THE LAW REFORM COMMISSION

AN COIMISIÚN UM ATHCHÓIRIÚ AN DLÍ

CONSULTATION PAPER

ON

PRIVACY: SURVEILLANCE AND THE INTERCEPTION OF COMMUNICATIONS

IRELAND
The Law Reform Commission
Ardilaun Centre, 111 St. Stephen's Green, Dublin 2

First Published September 1996

ISSN 1393-3140

THE LAW REFORM COMMISSION

The Law Reform Commission was established by section 3 of the *Law Reform Commission Act, 1975* on 20th October, 1975. It is an independent body consisting of a President and four other members appointed by the Government.

The Commissioners at present are:

The Hon. Anthony J. Hederman, former Judge of the Supreme Court, President;
John F. Buckley, Esq., Judge of the Circuit Court;
William R. Duncan, Esq., M.A., F.T.C.D., Barrister-at-Law, Professor of Law and Jurisprudence, University of Dublin, Trinity College;
Ms. Maureen Gaffney, B.A., M.A. (Univ. of Chicago), Senior Lecturer in Psychology, University of Dublin, Trinity College;
Simon P. O'Leary, Esq., B.A., Barrister-at-Law.

John Quirke is Secretary to the Commission.

The Commission's programme of law reform, prepared in consultation with the Attorney General, was approved by the Government and copies were laid before both Houses of the Oireachtas on 4th January, 1977. The Commission has formulated and submitted to the Taoiseach or the Attorney General fifty three Reports containing proposals for the reform of the law. It has also published eleven Working Papers, nine Consultation Papers and Annual Reports. Details will be found on pp.329-334.

The post of Research Counsellor to the Commission is vacant at present.

Ms. Deirdre Mulligan, LL.B., LL.M. (Edinburgh), Attorney-at-Law (State of New York), Ms. Lia O'Hegarty, B.C.L., LL.M. (Michigan), LL.M. (Harvard), Barrister-at-Law and Ms. Roisin Pillay, LL.B., LL.M (Cantab.) are Research Assistants.

Further information from:

The Secretary,
The Law Reform Commission,
Ardilaun Centre,
111 St. Stephen's Green,
Dublin 2.
Telephone: 671 5699.
Fax No: 671 5316.

CONTENTS *PAGES*

CONTENTS *PAGES*

CONTENTS *PAGES*

CONTENTS *PAGES*

PART 1: INTRODUCTION

CHAPTER 1: GENERAL

1.1 Privacy as a concept is notoriously resistant to definition.[1] It embraces a wide range of personal interests or claims which would place limits on the right of society and of its members to acquire knowledge of, and to take action regarding, another person. At its core lies the desire of the individual to maintain control over information, possessions and conduct of a personal kind, and, as a corollary, to deny or control access thereto by others. As such, it is now universally recognised as a human right,[2] and is to be distinguished from

---

1 See, e.g., E.J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser," (1964) *New York University Law Review* 962; Lord Chancellor's Department and the Scottish Office, *Consultation Paper on Infringement of Privacy*, July 1993, paras. 3.1-3.6; *Report of the Committee on Privacy* (the Younger Committee), Cmnd. 5012, 1972, ch.4; *Report of the Committee on Privacy and Related Matters* (Calcutt I), Cm 1102, 1990, paras. 3.1-3.8.; D.J. Seipp, "English Judicial Recognition of a Right to Privacy", (1983) *Oxford Journal of Legal Studies* 325 at 328-334; B. Walsh, "The Judicial Power and the Protection of the Right of Privacy," (1977) 1 D.U.L.J. 3; and *X v. Iceland*, admissibility decision of the European Commission of Human Rights, 18 May 1976, 5 D.& R. 86 at 87.

2 See Art. 12 of the *Universal Declaration of Human Rights*, Art. 17 of the *International Covenant on Civil and Political Rights*, and further below paras. 7.45-7.52.

other interests such as secrecy and confidentiality.[3]

1.2 The Commission noted in its *First Programme for Examination of Certain Branches of the Law with a View to their Reform*[4] that there appeared to be growing public concern in most countries, including Ireland, at the lack of legal protection for privacy, and indicated its intention to examine the whole area of the protection of privacy.

1.3 Public concern is justified. Technological developments of recent years mean that it is now possible to acquire, record and store vast amounts of the most detailed information about an individual. There is a real danger that such information may be acquired and used to the detriment not only of the individual concerned but also of society at large, and also that information which has been legitimately obtained may be used for a purpose other than the one for which it was acquired. The individual concerned may be completely unaware of the acquisition and storing of such information. Whether at home or in the workplace, one's behaviour may be monitored in ways and to an extent which was not possible a decade ago. Nor do the threats to privacy come only from the State or semi-state bodies. An individual's personal profile may be available to a large number of other persons. Private investigators have access to the most sophisticated devices for aural and visual surveillance, and there are few, if any,

---

3 The Law Reform Commission of Australia distinguished as follows between privacy interests and secrecy interests, at paras. 65 & 66, of its *Report on Privacy*, 1983:

> "The term 'secrecy' has been used in this report to describe the claim of public and private institutions to hide from others details of their organisation and operations, designs, ideas and other information pertaining to their experience, history, plans and activities, as organisations. Secrecy claims are made in the interests of the efficient running, profitability and competitiveness of the institution or in the public interest. Thus, this report speaks of trade secrets which a business wishes to keep from competitors and others who might wish to profit from them. It speaks also of duties of secrecy imposed on public servants not to disclose information which comes to them by virtue of their office. These interests contrast with individual interests in non-disclosure of personal information, i.e. privacy interests.
>
> Often, secrecy interests of institutions and privacy interests of individuals will be complementary. Thus, for example, both a government agency and the subjects of the records which it keeps might have a legitimate interest in their non-disclosure to unauthorised third parties. But these interests might be inconsistent. A person claiming protection of privacy interests might seek access to his personal information to check that it has been correctly recorded and is not being disclosed without his consent; but to grant his claim could intrude upon the secrecy interests of the institution. Further, it should be borne in mind that secret information (in the sense of information which it is in an institution's interest to keep secret) is not necessarily private information (in the sense that the privacy interests of a person would be invaded by its disclosure) and vice versa. But private information might be secret, and secret information might be private. And in formulating rights to privacy in certain areas of activity, one of the interests which must be thrown into the balance is that of a government agency, or of a private enterprise, in maintaining secrecy about its affairs."

We take a slightly different view of the distinction between privacy and secrecy interests. A secrecy interest is indeed an interest in the non-disclosure of information, in keeping information from persons other than those to whom one has no objection knowing it. In our view, however, there are two features which distinguish a secrecy interest from a privacy interest. First, the information which it is sought to keep from others may be of any kind. It is not limited, as is a privacy interest, to information of a personal kind. Secondly, both individuals and institutions have an interest in secrecy, but only individuals have an interest in privacy.

On the distinction between privacy and confidentiality, see below paras. 4.35-4.37.

4 Prl. 5984, laid by the Taoiseach before both Houses of the Oireachtas on 4 January 1977 pursuant to section 5(2) of the *Law Reform Commission Act, 1975*.

databases which are completely impervious to computer hacking.

1.4 There can be little doubt that in many areas technological capacity has outstripped the legal protection of privacy. In some areas, there is little or no protection. In other areas, some protection exists but, given the pace of technological change, there is always the danger that protection will become outmoded and inadequate. We are aware that any proposals which we may make for reform of the law on this matter may need revision and supplementing in the light of new technological developments. This is a field in which there is a need for continual vigilance and a proactive perspective on reform. But first it is necessary to document the extent to which privacy is protected under Irish law, to identify any gaps in this protection and to assess the adequacy of the law where it affords protection.

1.5 Given the breadth of the subject and the difficulty of definition, we decided to adopt an essentially pragmatic approach to our study of the legal issues involved in the protection of privacy, without altogether abandoning theoretical considerations.

1.6 When considering privacy in relation to computers in the early 1970s, a Canadian Task Force identified three categories of claims to privacy: territorial privacy, privacy of the person and privacy in the information context. These it described as follows:

> "*Territorial Privacy*. Claims to privacy advanced in a territorial or spatial sense are related historically, legally and conceptually to property. There is a physical domain within which a claim to be left in solitude and tranquillity is advanced and is recognized. A man's home is his castle. At home he may not be disturbed by trespassers, noxious odours, loud noises, or peeping Toms. No one may enter without his permission, except by lawful warrant.
>
> *Privacy of the Person*. In a second sense, a claim to privacy of one's person is protected by laws guaranteeing freedom of movement and expression, prohibiting physical assault, and restricting unwarranted search or seizure of the person. This notion, like the territorial one, is spatial in the sense that the physical person is deemed to be surrounded by a bubble or aura protecting him from physical harassment. But, unlike physical property, this 'personal space' is not bounded by real walls and fences, but by legal norms and social values. Furthermore, this sense of privacy transcends the physical and is aimed essentially at protecting the dignity of the human person. Our persons are protected not so much against the physical search (the law gives physical protection in other ways) as against the indignity of the search, its invasion of the person in the moral sense.
>
> *Privacy in the Information Context*. The third category of claims to privacy ... is based essentially on a notion of the dignity and integrity of

the individual, and on their relationship to information about him. This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit. And this is so whether or not the information is subsequently communicated accurately, and whether or not it is potentially damaging to his reputation, his pocket-book, or his prospects; the context is of course the controlling factor in determining whether or not particular information will be damaging. Competing social values may require that an individual disclose certain information to particular authorities under certain circumstances (e.g., census information). He may decide to make it available in order to obtain certain benefits (e.g., credit information or information imparted to his lawyer to win a lawsuit or to his confessor to win salvation). He may also share it quite willingly with his intimates. Nevertheless, he has a basic and continuing interest in what happens to this information, and in controlling access to it."[5]

1.7 These three categories were approved by the Australian Law Reform Commission in its research on privacy and it added a fourth category - "the interest in freedom from surveillance and from interception of one's communications", or 'communications and surveillance privacy'.[6] Although this category is related to the other three,[7] the Commission decided "for exactness"[8] to treat it separately.

1.8 We find such categorisation of the interests which it is sought to protect under the heading of privacy useful,[9] and *we decided, as the first stage of our research on this topic, to address the extent to which freedom from surveillance and from interception of communications is, and should be, guaranteed by the law in order to protect individual privacy.*[10] These freedoms are today under increasing threat as a result of the availability and ease of use of sophisticated surveillance devices, and a review of the extent to which they are protected, and not protected, by the law is timely.

1.9 *Since the protection of these privacy interests in specific contexts raises issues which are peculiar to those contexts, we furthermore decided to limit our first*

---

5 *Privacy and Computers*, Department of Communications and Department of Justice, Canada, 1972, pp.13-14. See also *Public Government for Private People*, vol. 3, *Protection of Privacy*, Commission on Freedom of Information and Individual Privacy, Ontario, Canada, 1980, p.499.

6 *Report on Privacy*, para. 46.

7 As the Commission noted, breaches of communications and surveillance privacy may, but will not necessarily, involve breaches of territorial privacy, privacy of the person and information privacy: *Ibid.*

8 *Ibid.*

9 We would however reiterate that privacy is a universally recognised human right. All categories of privacy are therefore concerned with the protection of the dignity of the human person. This core element of privacy is not adverted to in the description of territorial privacy provided by the Canadian Task Force and approved by the Australian Law Reform Commission.

10 Law regulating the interception of communications is more concerned with the protection of secrecy than of privacy in that the law has typically made no distinction between communications on the basis of their content or of the correspondents. The same rules apply irrespective of whether the content is personal or, e.g., commercial, and of whether the sender or recipient is an organisation or an individual human being. However, interference with correspondence has been treated internationally as a privacy matter (see below paras. 7.17-7.18 & 7.45), and although this may not be altogether conceptually accurate, it will also be so treated here.

study to the general interest in freedom from surveillance and from interception of one's communications. The particular issues arising in specific institutional contexts, such as the workplace, prison and hospital, will be considered in a separate study.

1.10 In the remainder of Part I of this Paper, we will look briefly at pertinent technological and economic developments and at the significance of these developments for privacy. Then, in Part 2, we will document the extent to which there presently exists in Ireland legal protection for the individual against surveillance and the interception of her or his communications. In this connection, we will examine in detail protection under the Constitution, civil remedies, criminal sanctions and legislation governing State interference with post and telecommunications. We are concerned that any recommendations we make should be consistent with Ireland's obligations under international law and, in Part III, we will therefore review the relevant international standards, in particular, Ireland's international obligations in relation to respect for privacy and regulation of the post and telecommunications. Having surveyed the existing legal protection against surveillance and the interception of communications and Ireland's international obligations in this regard, in Part IV, we will identify the main issues which need to be addressed if adequate legal protection is to be afforded the individual against invasion of her or his privacy by surveillance[11] whether it be by the State or non-state actors. We will first examine the desirability of additional civil remedies and then consider whether further criminal sanctions and regulation are also needed in the areas of visual surveillance, aural surveillance and the interception of communications. We will conclude with a summary of our provisional recommendations.

1.11 We would emphasise that our concern throughout is primarily with the protection of privacy. Some of our recommendations will, by virtue of the nature of the subject matter, afford protection to interests in addition to that of privacy. Thus, it would not generally be feasible to regulate the interception of communications by reference to the content of the communication. Any prohibition on the interception of letters or telephone conversations will protect business interests as well as intimate, personal information. Nevertheless, in other areas, our recommendations are clearly targeted at the protection of privacy and are not intended as prescriptions for a general legal régime. Thus, video cameras may be used for many legitimate purposes. Our task here is not to devise a scheme for the general regulation of the use of these cameras. Rather it is to ensure that their use does not impinge unacceptably on the privacy of the individual.

1.12 We are also concerned principally with methods of acquiring personal information, that is, with the interception of communications and various forms of surveillance. It would however be unduly narrow to limit our study to methods of acquiring information without also to some extent considering the use to which

---

11 For the sake of brevity, the expression "surveillance" will often be used in this Paper to include the interception of communications as well as aural and visual surveillance.

information acquired by these methods is put. Thus, for example, in our review of the present law, we will look at the existing legal protection against both the use of certain methods of acquiring information and disclosure of information acquired by these means. The interest of an individual in the non-disclosure of personal information obtained by surveillance or the interception of communications is often the same as in the case of information obtained in other ways. It is not our intention to deal specifically in this Paper with the protection of "privacy in the information context",[12] a study which would extend well beyond its scope. Rather we are concerned with the disclosure of information only in so far as the information has been obtained by means of surveillance or the interception of communications.

1.13 We invite written submissions from members of the public on our provisional recommendations. We would especially welcome comments on our proposals for the protection of privacy from the invasive use of video cameras, an area in which the law to date has been strangely silent. We would also appreciate observations on the appropriate balance to be drawn between competing interests in privacy and in freedom of expression since reconciling these interests can be particularly difficult. Submissions should be sent to the Commission at:

Ardilaun Centre,
111 St. Stephen's Green,
Dublin 2,

to arrive no later than 1 December 1996.

12 See above para. 1.6.

CHAPTER 2: TECHNOLOGICAL AND ECONOMIC DEVELOPMENTS

Technological Developments

> The telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everyone all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.
>
> ... in the past no government had the power to keep its citizens under constant surveillance. The invention of print, however, made it easier to manipulate public opinion, and the film and the radio carried the process further. With the development of television, and the technical advance which made it possible to receive and transmit simultaneously on the same instrument, private life came to an end. Every citizen, or at least every citizen important enough to be worth watching, could be kept for twenty-four hours a day under the eyes of the police and in the sound of official propaganda, with all other channels of communication closed. The possibility of enforcing not only complete obedience to the will of the State, but complete uniformity of opinion on all subjects, now existed for the first time. (George Orwell, *Nineteen Eighty-four.*)

2.1 The nightmare society envisaged by Orwell in which people's every action, word and even thought were monitored and controlled by an authoritarian

régime has not come to pass; but the surveillance technology which could be used to create such social conditions does exist. In a democracy which values individual human worth and dignity, the potential use of such technology for the invasion of privacy on a massive scale needs to be carefully monitored, and countermeasures taken where a real risk to privacy is identified.

2.2 In the Orwellian nightmare, the state exercised complete control over the individual by virtue of its ability to observe human conduct almost at will. The use of technology by the state to gain information about individuals undoubtedly poses one of the greatest risks to personal autonomy and well-being because of the extent and concentration of power wielded by the state. In the Ireland of today, however, as in many other societies, the threat to privacy from the use of surveillance technology stems not only from public authority. Private individuals and business concerns may also resort to surveillance for a variety of reasons. Optical surveillance, of both the overt and the covert kind, is now fairly common. Closed circuit TVs and video cameras are widely used by banks and shops in Ireland as elsewhere for security purposes. Employee theft is a problem in many areas of industry, trade and commerce, and a hidden video camera may be used to identify the culprits. For example, a video camera may be mounted in an unobtrusive location in a shop or public house to view and record sales. The camera may be linked to the cash register so that the amount which should have been rung up and deposited in the till is superimposed on the camera picture allowing a comparison to be made between the cash actually deposited and the amount which should have been deposited.[1] The use of such devices by private actors raises issues of privacy in relation not only to employees but also to customers who may have their behaviour electronically observed and recorded without their knowledge or consent. Similarly, a person may engage in eavesdropping for a variety of reasons ranging from a pastime to industrial espionage.

2.3 Although manufacturers and suppliers restrict the sale of some equipment to government sources, a wide range of optical and listening devices are available on the market to both public and private customers. Many may be purchased at a relatively low cost and even specialised equipment tailored to the needs of a customer is not necessarily very expensive.[2] Moreover, many devices require no special knowledge for either installation or use. The availability, low cost and ease of use of many devices mean that the use of surveillance technology is not limited to public authorities or commercial concerns but is within the reach of most individuals.

2.4 The precise extent to which surveillance occurs in Ireland is unknown, but media reports suggest that surveillance by both public and private actors is not uncommon. When the Gardaí received information that paramilitaries might

---

1 For example, the 'Tillscan' system uses microchip technology to monitor all transactions through a till and can be used with single or multiple till installations. All till transactions are overprinted on to the picture from a closed circuit television camera and displayed on a television monitor. All transactions can be recorded on any standard of video camera. Information supplied by Liam Brady, private investigator, Dublin.

2 For example, the 'Tillscan' system mentioned above may be purchased for under £2,000.

target suburban shopping centres in Dublin because they regarded them as easier to rob than premises in the city centre, the police contacted the management of several shopping centres to ensure that proper procedures were in place to monitor the shopping areas and themselves placed a few centres under constant surveillance.[3] In the autumn of 1993, in order to combat street crime, a specially adapted police vehicle containing sophisticated video and recording equipment which can be used at night as well as during the day was introduced onto the streets of Dublin;[4] and in the spring of 1995, a closed-circuit television system was installed as a pilot project in a city centre area of the capital city in an endeavour to reduce street crime.[5] In order to combat theft, security staff at a branch of a supermarket chain secretly placed a video camera behind an air-vent grill in a changing room for female staff.[6] In order to counter a claim for damages for personal injuries, a local authority hired a private detective to take photographs of the plaintiff,[7] and it has been estimated by one private investigator that 25-30% of his business now involves surveillance on behalf of defendants in public liability compensation claims.[8] Some stockbroking firms have a policy of recording telephone calls from their share dealing rooms. The recordings are used if there is a dispute over a transaction.[9] The leader of a political party has had his conversations on a mobile telephone intercepted by means of a radio scanning device and recorded, and the taped conversations subsequently used in a radio broadcast and newspaper articles. The conversations were monitored by a private citizen from his own home using a scanner to which a home-made aerial of brass welding rods had been attached and which was connected to a cassette tape recorder. The scanner was purportedly readily obtainable at a cost of about £450.[10]

2.5 In its Report on Privacy in 1983, the Australian Law Reform Commission gave a number of examples of the new, privacy-invasive technology. In relation to the post it mentioned:

> "... extremely long, thin pliers which enable letters to be rolled up and removed from envelopes via the corners, special sprays which turn envelopes temporarily translucent, special solvents to 'ungum' envelope flaps, and electronic scanning equipment which can detect the carbon used in most kinds of ink."[11]

As examples of listening and optical devices, they gave:

> "• parabolic microphones with ranges extending to more than 250

---

3 See 'The Irish Times', 14 December 1993.

4 See 'Public Sector Times', October 1993, and 'The Irish Times', 18 September 1993. At the time, the Minister for Justice stated, 'Experience with such equipment in cities abroad shows significant reductions in the levels of street crime following its introduction.'

5 See, e.g., 'The Irish Times', 18 April 1995.

6 See 'The Irish Times', 13 and 29 July 1993, and 'The Irish Press', 28 July 1993.

7 See further below paras. 3.21-3.22.

8 Liam Brady, interviewed for 'Tuesday File', broadcast on Network 2, 6 September 1994.

9 See 'The Irish Times', 24 May 1993.

10 See 'The Irish Times', 29 May 1993, and 'The Sunday Independent', 1 August 1993.

11 *Report No. 22*, para. 94.

metres;

- miniature tape recorders which can be concealed inside, for example, cigarette packets;
- binoculars having built-in cartridge cameras;
- listening devices laminated into business cards;
- brief-case cameras, activated by pressing a button on the brief-case;
- residual light image intensifiers with ranges of up to 10 kilometres for long-distance observation at night;
- day-and-night cameras connected to monitors and operated by remote control;
- long-range photographic flash devices enabling photographs to be taken at night without detection and from a range of 100 metres or more;
- microphones concealed in watches, buttonholes, pens and ties;
- sub-miniature transmitters, smaller than sugar cubes, which can record conversations from a distance of 10 metres and transmit them at high quality up to 150 metres;
- listening devices which through the use of laser beams can monitor and record conversations from positions outside the room in which they are occurring;
- electronic stethoscopes which, by picking up mechanical vibrations and amplifying them up to 10,000-fold, enable conversations to be monitored through windows, doors and walls;
- optical devices which permit continuous monitoring in complete darkness; and
- listening devices placed in telephones, which enable surveillance of conversations within a room even when the telephone is not in use."[12]

2.6 The range and sophistication of technological devices which can be used

---

12 *Ibid.*

for surveillance purposes have increased substantially since the Australian Law Reform Commisssion studied the topic of privacy, and technological innovation continues at an amazing rate. According to recent newpaper reports, the Japanese electronics company, Hitachi Ltd., has developed a small video camera which can be held comfortably in the palm of one's hand.[13] It is claimed to be the smallest video camera in the world, and the smallness of its size was made possible by the use of a semiconductor chip instead of tape to store the video data. The same company, together with researchers at Trinity College Dublin, have invented an artificial eye capable of recognising shapes and patterns in a way which mimics human sight.[14] Present automatic vision systems use television cameras to scan an image or an object, the shape of which is analysed by special software. The new "eye" was devised by combining two of the most advanced information processing technologies, optical or light-based computing and neural networking.[15] The result is a device which through the use of microprocessor chips attempts to replicate human brain functions and which can "learn" to recognise objects in a fashion far in advance of existing vision systems.

2.7 There have moreover been significant developments in recent years in the form and speed of personal communication. It is now possible for one person to send a message to another by electronic mail, commonly referred to as e-mail, that is, a paperless form of communication involving the transmission of computerised data from one computer user to another. Electronic mail has the potential to replace many of the traditional postal services and indeed use of the telephone. It is however inherently vulnerable to interception and oversight by others. It can be easily accessed and read by someone other than the intended recipient by using a networked computer terminal. It has been described by one data security expert as having "the same security level as a postcard".[16]

2.8 Technological developments have had a particularly profound impact on the field of telecommunications and can be expected to have a continuing significant impact for some years to come. The marriage of computer and communications technology has revolutionised telecommunications. As a result of digital technology, forms of communication now exist which could only be dreamed of in the recent past, and this technology is rapidly replacing the old analogue systems.[17] The carriage of voice telephony,[18] video images and data

---

13 See "The Irish Times", 29 August 1994.

14 See "The Financial Times", 13 May 1993; and P. Horan, A. Jennings, B. Kelly and J. Hegarty, "Optical implementation of a second-order translation-invariant network algorithm", *Applied Optics*, 10 March 1993.

15 On neural networks see, e.g., "The Irish Times", 5 September 1994. It is claimed that neural networks will enable breakthroughs in such areas as continuous speech recognition, handwritten character recognition, and autonomous vehicles or robots.

16 Ronald L. Rivest, Professor of Computer Science at the Massachusetts Institute of Technology, reported in *Technology Review*, August/September 1992, at p.11, and quoted in *Privacy Protection Principles for Electronic Mail Systems*, Information and Privacy Commissioner, Ontario, 1994.

17 See, e.g., Commission of the European Communities, *Towards the Personal Communications Environment: Green Paper on a common approach in the field of mobile and personal communications in the European Union*, pp.13 & 72f. As the Commission points out in this Paper, the European Union is now considered to be the world leader in digital cellular telecomunications systems. The digitisation of telecommunications in Ireland is at an advanced stage.

is now possible[19]; and all these functions may be available to a user on a single piece of terminal equipment connected to a digitised network.[20] To the traditional telecommunications services of voice telephony and telex have been added a wide range of new services, including, in addition to electronic mail, packet-switched data, circuit-switched data, facsimile, teletex and videotex. Indeed telex has to an appreciable extent been replaced by some of these new services. The quality and capacity of transmission are greatly enhanced by the medium of fibre optic cable.[21] Digital cordless telecommunications are available for use in the home and in the office. Carriage by satellite means that distance and location do not present the problems which they did heretofore.[22] Non-geostationary satellite systems and services have initiated a major shift towards personal mobile communications, away from fixed communications[23]; and it has been estimated that within the next five years a new generation of telecommunications satellites is likely to provide a truly global mobile communications service, using lightweight pocket-sized handsets,[24] and that within ten years twenty to thirty per cent of calls will terminate in, or originate from, mobile devices.[25] Many of these developments present new privacy problems. For example, a conversation on a mobile telephone can be easily

---

18 Voice telephony is defined in various European Union instruments to mean the commercial provision for the public of the direct transport and switching of speech in real-time between public switched network termination points, enabling any user to use equipment connected to such a network termination point in order to communicate with another termination point: see, e.g., Council Directive 90/387/EEC, 28 June 1990, Art 2(7) and Commission Directive 90/388/EEC, 28 June 1990, Art. 1(1). See also the definition of "voice telephone service" in s.2(1) of the *European Communities (Telecommunications Services) Regulations, 1992.*

19 The Integrated Services Digital Network (ISDN) is a new form of transmission technology which allows the full integration of voice and data services over a digital network. It is EU policy that ISDN be developed as a trans-European telecommunications infrastructure: see, e.g, Council Resolution 92/C 158/01, 5 June 1992, reproduced in Denton Hall, *EC Telecommunications Law* (henceforth *Denton Hall*), Chancery Law Publishing Ltd., Chichester, England, 1993, at pp.A243-A244.

20 See "The Irish Times", 22 August 1994, concerning a computer system costing under £200 that can answer the telephone, send and receive faxes, work as a modem and do the job of a soundcard. Using a Digital Signal Processor (DSP) chip instead of a typical central processing unit (CPU), the board can answer the telephone and send a fax concurrently, without affecting the work being done by the computer itself. It obviates the need for separate fax machines, modems, answering-machines and soundcards.

21 See "The Irish Times", 8 and 12 April 1994, concerning the laying of a fibre optic telephone cable between Wexford and Land's End in Cornwall in a joint venture between Telecom Éireann and British Telecom. According to these reports, six pairs of glass fibre, each thinner than a human hair, are contained within a reinforced casing; and each pair is capable of carrying 30,000 telephone conversations simultaneously.

22 Communication by satellite can be of various kinds: fixed service (point-to-point communication), multipoint (point- to-multipoint and multipoint-to-multipoint), one-way or two-way. See, e.g., the *European Commission Guidelines on the Application to EEC Competition Rules in the Telecommunications Sector*, 91/C233/02, para. 29(a). Satellites' uses can be broken down into the following categories: public switched voice and data transmission, business value-added services and broadcasting. See, e.g., *ibid.*, para. 29(c).

23 See *Denton Hall*, para. 5.42.

24 See "The Irish Times", 29 August 1994. On 9 September 1994, Sony Corporation started selling in Japan a cellular phone the size of a credit card: see "The Irish Times", 3 September 1994.

25 *Denton Hall*, para. 4.23. The Commission of the European Communities has pointed out that, by 1994, there were more than 8 million cellular mobile telephone users in Europe, more than double the number three years previously, and that there were also more than 8 million users of other mobile communications services, in particular, paging and private mobile radio systems. It forecast that by the year 2000, there could be nearly 40 million users in the European Union and, by the year 2010, up to 80 million users: see *Towards the Personal Communications Environment: Green Paper on a common approach in the field of mobile and personal communications in the European Union*, COM(94) 145 final, 27 April 1994, pp.4 & 72.

> In mobile communications distinct services seem presently to exist such as cellular telephone, paging, telepoint, cordless voice and cordless data communication. However, technical development permits providing each of these systems with more and more enhanced features, and a consequence of this is that the differences between these sytems are progressively blurring and their interchangeability increasing: see the *European Commission Guidelines on the Application of EEC Competition Rules in the Telecommunications Sector*, para. 30.

intercepted and recorded. All that is needed is a radio-scanning device linked to a recorder.[26]

2.9 In the past individual privacy was not vulnerable to such wide-ranging invasion. It is the development of new technology which, along with the many benefits it confers, has exposed individuals to this risk.

Economic Developments

(i) Competition and the open market economy

2.10 Ireland's membership of the European Union is of profound significance in relation to the law and policy pertaining to the provision of goods and services. The European Economic Community was founded in order to promote the creation of a common market among the Member States, and, in accordance with the Single European Act,[27] the internal market came into effect on 1 January

---

26 This risk can be minimised by using sophisticated encryption techniques. On technical countermeasures see further below para. 2.37.

The European Commission has said of the move from analogue to digital technologies in the telecommunications sector that it "will in general substantially reduce the possibilities for unauthorised interception of mobile communications through the use of highly sophisticated encryption techniques", but that "it also adds urgency to the need for a clear framework for effective data security, storage, processing and privacy.": see *Towards the Personal Communications Environment: Green Paper on a common approach in the field of mobile and personal communications in the European Union*, 1994, p.189. See also pp.131-132 of the *Green Paper* where, in considering new requirements for the protection of privacy, it is stated that:

> "The evolution in the industrialised countries towards the creation of information societies is closely connected to the increasing use, processing and exchange of personal data in all spheres of social and economic life. In the European Union these trends are reinforced by the establishment of the internal market, stimulating a rapid growth in trans-border flows of personal data. The increasing importance of data processing and data exchange demand new measures to ensure the effective protection of personal data and privacy.
>
> In the telecommunications sector, the digitalisation of the networks has led to specific new requirements.
>
> On the one hand, fully computer-based processing can offer a substantially higher degree of data security through, for example, the use of highly sophisticated encryption techniques.
>
> On the other hand, digital processing of both operational and call data within computerised exchanges, may make it easier to record and monitor systematically specific call-related data, such as origin of specific calls or the location of the calling or called party. Such monitoring was only feasible in "non-intelligent" analogue networks after substantial and costly adaptation of the network equipment and therefore was only implemented in very exceptional circumstances.
>
> At the same time, new intelligence communications functions, such as calling-line identification and itemised billing, offer substantial additional service features to the subscriber which enhance both service quality and which can contribute to the level of consumer protection.
>
> The new possibilities and service features presented by digital technology require specific new regulatory measures if the protection of privacy is to be guaranteed in the new environment, and the erection of barriers within the internal market based on national data processing rules is to be avoided."

In this Paper, we will only consider the risk to privacy arising from the computerisation of data in so far as the risk relates to the interception of communications and, in general terms, to the recording of information acquired as a result of surveillance. We will examine other privacy issues relating to the computerisation of data at a later stage.

27 Article 13, inserting a new Article 8a in the EEC Treaty which provided for the progressive establishment of the internal market over a period expiring on 31 December 1992.

1993. This "internal market shall comprise an area without internal frontiers in which the free movement of goods, persons, services and capital is ensured in accordance with the provisons of [the EEC] Treaty."[28] The principle of an open market economy with free competition lies at the heart of the economic policy of the European Union and its Member States[29]; and the EEC Treaty itself contains a number of competition rules designed to foster and maintain such an economy.[30]

2.11 Of particular relevance in the context of the present study are Articles 85, 86 and 90 of the EEC Treaty. Paragraph 1 of Article 85 prohibits as incompatible with the common market:

> "all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the common market".

The paragraph goes on to list a number of such agreements, decisions and practices which are in particular prohibited. They include those which limit or control production, markets, technical development, or investment, and those which apply dissimilar conditions to equivalent transactions with other trading parties, thereby placing them at a competitive disadvantage. Article 86 targets abuse by one or more undertakings of a dominant position within the common market in so far as it may affect trade between Member States. The Article does not prohibit the holding of a dominant position as such, but rather the abuse of such a position. The Article then goes on to give a list of such abuse very similar to that contained in Article 85 and which includes the two examples given above. Paragraph 1 of Article 90 deals with public undertakings and undertakings to which Member States grant special or exclusive rights, and provides that "Member States shall neither enact nor maintain in force any measure contrary to the rules contained in this Treaty", which rules of course include those provided for in Articles 85 and 86. Paragraph 2 of Article 90, however, qualifies this obligation somewhat. It provides:

> "Undertakings entrusted with the operation of services of general economic interest or having the character of a revenue-producing monopoly shall be subject to the rules contained in this Treaty, in particular to the rules on competition, in so far as the application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned to them. The development of trade must not be affected to such an extent as would be contrary to the interests of the Community."

---

28 Art 7a of the EEC Treaty, as inserted by Art. 13 of the Single European Act and renumbered by Art. G(9) of the Maastricht Treaty.

29 See, e.g., Articles 3a, 102a & 105(1) of the EEC Treaty as amended by the Maastricht Treaty.

30 Arts. 85-94.

(ii) Deregulation of postal and telecommunications services

2.12 Historically postal and telecommunications services have usually been provided in Europe by the state or by state-controlled bodies and there has often been a national monopoly of these services. This situation is however in the process of dramatic change, a change encouraged and promoted in Ireland by the European Union, but discernible globally.

2.13 In 1987, the European Commission published a Green Paper in which it proposed a more liberal and flexible competitive environment for telecommunications services and equipment.[31] The creation of this environment would entail, *inter alia*, the break up of monopolies and the provision of open access to the telecommunications infrastructure with a consequent proliferation in the number of suppliers of goods and services. The Commission followed this up in 1988 with a Directive on competition in the markets in telecommunications terminal equipment[32] and in 1990 with a Directive on competition in the markets for telecommunications services.[33] In the former Directive, the Commission expressed the view that the special or exclusive rights relating to terminal equipment enjoyed by national telecommunications monopolies brought about a situation whereby competition in the common market was distorted and that this situation infringed the Community's competition rules. It therefore required Member States which had granted a public or private body special or exclusive rights for the importation, marketing, connection, bringing into service of and/or maintenance of such telecommunications terminal equipment to ensure that these rights were withdrawn[34] and that economic operators have the right to import, market, connect, bring into service and maintain terminal equipment.[35] As a result, there is now a free market in terminal equipment both within and between Member States. In the latter Directive, the Commission reiterated its view, this time with respect to telecommunications services, that special or exclusive rights conflict with the Community's competition rules, and required "Member States [to] withdraw all special or exclusive rights for the supply of telecommunications services other than voice telephony and [to] take the measures necessary to ensure that any operator is entitled to supply such telecommunications services."[36]

2.14 It is accepted that the development of the common market for telecommunications services and equipment requires that capacity on fixed public telecommunications networks be afforded any applicant, in direct competition with telecommunications administrations, subject only to fair conditions of access; and the Union is gradually moving towards open network provision (ONP). In

---

31 Reproduced in *Denton Hall*, at pp.A43-A55.

32 Directive 88/301/EEC, 16 May 1988, reproduced in *Denton Hall*, at pp.A65-A71.

33 Directive 90/388/EEC, 28 June 1990, reproduced in *Denton Hall*, pp.A91-A100. See also Council Directive 90/387/EEC on the establishment of the internal market for telecommunications services through the implementation of open network provision, *ibid.*, pp.A81-A90.

34 Article 2.

35 Article 3. The right is subject to technical specifications and the use of qualified personnel.

36 Article 2. The Directive does not apply to telex, mobile radiotelephony, paging and satellite services: see Article 1(2). In addition, in 1991, the Commission issued Guidelines on the Application of EEC Competition Rules in the Telecommunications Sector: see *Denton Hall*, at pp.A179-A207.

1990, the Council issued a Directive on the establishment of the internal market for telecommunications services through the implementation of ONP.[37] This Directive was intended to lay the basis for such provision.

> "The vision was ... clear; the existing public fixed networks were to become a kind of pan-European motorway system over which any operator, TA[38] or TO[39], British, French, German or American, could run telecommunications services - just as anyone can run trucks on a motorway - in the knowledge that the tolls and the conditions of access and use were to be the same for all users.
>
> Network infrastructure providers were effectively to become "common carriers", with no right to give special favours to anyone, even divisions within their own companies."[40]

The Directive specifies that ONP provision conditions must comply with a number of basic principles, namely, they must be based on objective criteria, they must be transparent and published in an appropriate manner, and they must guarantee equality of access and be non-discriminatory, in accordance with Community law.[41] Furthermore, the conditions must not restrict access to public telecommunications networks or public telecommunications services, except for reasons of general public interest, otherwise referred to as "essential requirements".[42] Since "situations differ and technical and administrative constraints exist in Member States",[43] it is proposed that ONP will be realised in stages.[44]

2.15 In the same year as the Commission's Green Paper on the development of the common market for telecommunications services and equipment was issued, the Council adopted a Recommendation on the co-ordinated introduction of public pan-European cellular digital land-based mobile communications in the

---

37 Directive 90/387/EEC, 28 June 1990, reproduced in *Denton Hall*, at pp.A81-A90.

38 Telecommunications administration. This term is used to indicate a government agency or a corporate body wholly or partly owned by the government of a Member State and which supplies telecommunications infrastructure and services under special or exclusive rights.

39 Telecommunications operator.

40 *Denton Hall*, pp.3-13.

41 Art. 3(1).

42 "Essential requirements" are defined in the Directive. The term means the non-economic reasons in the general interest which may cause a Member State to restrict access to the public telecommunications network or public telecommunications services. These reasons are security of network operations, maintenance of network integrity and, in justified cases, interoperability of services and data protection. Data protection may include protection of personal data, the confidentiality of information transmitted or stored as well as the protection of privacy: see Art. 2(6). In addition, the conditions generally applicable to the connection of terminal equipment to the network shall apply: see Art. 3(2).

43 Preamble of the Directive.

44 See, e.g., Council Directive 92/44/EEC on the application of open network provision to leased lines, 5 June 1992, reproduced in *Denton Hall*, at pp.A231-A242; Council Recommendations 92/382/EEC on the harmonised provision of a minimum set of packet-switched data services in accordance with open network provision principles and 92/383/EEC on the provision of harmonised integrated services digital network access arrangements and a minimum set of ISDN offerings in accordance with open network provision principles, also of 5 June 1992, reproduced in *Denton Hall*, at pp.A245-A252 and A253-262 respectively; and Council Resolution 94/C379/03 on the principles and timetable for the liberalization of telecommunications infrastructures, reproduced in *Denton Hall*, at pp.A377-A378.

Community[45] and a Directive on the frequency bands to be reserved for their introduction.[46] It followed this, in 1990, with a Recommendation on the co-ordinated introduction of pan-European land based public radio paging in the Community[47] and a Directive on the frequency bands to be allocated for this purpose[48]; and, in 1991, with a Recommendation on the introduction of digital European cordless telecommunications[49] and a Directive on the frequency band to be designated for the introduction of these telecommunications.[50] In the latter Recommendation, the Council urged the Commission, *inter alia*, to prepare "a long-term strategy ... for the evolution of the soon to be introduced pan-European digital cellular and paging systems, and digital cordless systems, taking account of the general development towards a future universal personal communications system".[51] Following on this recommendation and a Council Resolution of 1993 which identified as one of the major short-term goals for the Community's telecommunications policy "the development of future Community policy in the field of mobile and personal communications",[52] the Commission

---

45 Recommendation 87/371/EEC, 25 June 1987, reproduced in *Denton Hall*, at pp.A57-A61. The transmission mode for the pan-European mobile system is digital; and the Recommendation provides, *inter alia*,

> 'that the telecommunications administrations plan for a gradual evolution from any existing public mobile radio systems to the pan-European cellular digital mobile communications system so as to ensure a transition which meets the needs of users, telecommunications administrations and undertakings established within Community countries'.

46 Directive 87/372/EEC, reproduced in *Denton Hall*, at pp.A63-A64.

47 Council Recommendation 90/543/EEC, 9 October 1990, reproduced in *Denton Hall*, at pp.A129-A133.

48 Council Directive 90/544/EEC, 9 October 1990, reproduced in *Denton Hall*, at pp.A135-A136.

Paging services are provided in Ireland through a joint venture by Telecom Éireann and Motorola, Eirpage.

49 Recommendation 91/288/EEC, 3 June 1991, reproduced in *Denton Hall*, at pp.A175-A178.

50 Directive 91/287/EEC, reproduced in *Denton Hall*, at pp.A173-A174.

51 Para. 4.

52 Resolution 93/C 213/01 on the review of the situation in the telecommunications sector and the need for further development in that market, 22 July 1993, reproduced in *Denton Hall*, at pp.A265-A268.

produced a Green Paper on the subject.[53] In the Paper, it advocated, *inter alia*, the abolition of remaining exclusive and special rights in the mobile communications sector, subject where required to the establishment of

---

53 *Towards the Personal Communications Environment: Green Paper on a common approach in the field of mobile and personal communications in the European Union*, COM(94) 145 final, 27 April 1994. At p.50 of this *Green Paper*, the Commission states:

> "Personal communications services must be seen as services which ultimately will allow person-to-person calling, independent of location, the terminal used, the means of transmission (wired or wireless) and/or of the choice of technology.
>
> Personal communications services will be based on a combination of fixed and wireless/mobile services to form a seamless end-to-end service for the user."

See also p.119, where it is stated, with specific reference to the European Union, that:

> "The twin forces of market demand and technological innovation are both pointing towards the same long-term goal - full mobility for the telecommunications user, who will make use of mobile and/or fixed networks as appropriate, and in most cases will be unaware of the underlying network technology. Achieving such interoperability at a European level will be a powerful cohesive influence within the Union.
>
> The European citizen will be able to travel throughout the EU, and by inserting his or her smart card in a fixed or portable telephone will be able to make and receive calls anywhere in the Union.";

and p. 206, where the Commission expresses the view that:

> "In the future evolution towards personal communications, priority should be given to personal, portable numbers, independent of the network provider, the individual service type, the location (nationally or internationally) and the individual terminal equipment."

Universal personal telecommunication (UPT) has been described by the European Telecommunications Standards Institute as:

> "... a service that enables improved access to telecommunication services by allowing personal mobility. It enables each UPT user to participate in a user defined set of subscribed services, and to initiate and receive calls on the basis of a unique, personal, network independent UPT number across multiple networks at any terminal, fixed, movable or mobile. Such participation is irrespective of geographic location, limited only by terminal or network capabilities and restrictions imposed by the network provider."

See ETSI Technical Report 083, *Universal Personal Telecommunication (UPT); General UPT security architecture*, July 1993, p.11.

appropriate licensing conditions[54]; the removal of all restrictions on the provision of mobile services both by independent service providers and on direct service provision by mobile network operators; and the removal of restrictions on the combined offering of services via the fixed and mobile networks within the overall time schedule set by the 1993 Council Resolution for the full liberalisation of public voice telephony services via the fixed network. The latter would mean that, from 1 January 1998, mobile operators would be allowed to transport voice traffic between any combination of fixed and mobile destinations in most Member States of the Union.[55]

---

54 With respect to limiting the number of licensed operators, the Commission commented, at pp.197-198 of the *Green Paper*:

> "Whilst efficient frequency planning will maximise the number of potential operators, the technical limitations which the frequency spectrum imposes on the number of mobile networks means that in most cases Member States currently have to set up procedures in order to determine to whom frequency spectrum will be allocated. This involves a choice both of individual operators for a particular service, but also a more general choice between technologies as to how much spectrum each technology should be allocated.
>
> Whilst it is accepted that frequency considerations will continue to limit competition between mobile networks, the removal of exclusive and special rights in the mobile sector requires the application of existing Union principles to the licensing award procedures. This will overcome the barriers to greater competition and to the development of the internal market which result from current discretionary and nationally-focused award procedures for licences and frequencies.
>
> Licence awards must respect the competition rules and must be based on open, non-discriminatory, and transparent procedures. Where this is not the case, or where there are arbitrary restrictions on the range of undertakings from whom applications can be received, the award procedure can have a detrimental impact on the market structure in that Member State and in the European Union.
>
> In particular, the automatic grant of licences to certain public operators or restrictions on licence applications from operators active in other telecommunications sectors or in other Member States may distort competition.
>
> Unless such restrictions are justified, for example, in order to prevent the extension of market dominance on one market to a neighbouring market or service, inappropriate restrictions should not be applied. Such restrictions on the range of applicants can reduce efficiency and limit consumer benefits, which would normally be derived from the resulting economies of scope and scale, as well as commercial experience in other markets.
>
> Where the number of operators is limited by a Member State, this limit is a potential restriction on the freedom to provide services and must be justified under European law. In particular, any limitation on numbers must normally be justified on the basis of either the essential requirements, such as the efficient use of frequency spectrum, and/or public service requirements in the form of trade regulations, and must be consistent with the Community competition rules.
>
> Any limitation should respect the principle of proportionality, by imposing the solution which is least limiting and must give priority to competitive provision."

See also pp.198-199, where the Commission considers the principles for licensing award procedures and specifies what measures are necesary to ensure that licensing procedures are open, non-discriminatory and transparent. The Commission points out, at p.199, that "Licence numbers may not ... be restricted on the basis of a subjective economic assessment of the awarding body of the number of operators a specific market can hold", and that:

> "In general, market forces rather than regulatory authorities at a national or Community level, should decide future market structures, subject always to the application of the Community competition rules and the overall safeguards found in the Treaty."

55 In recognition of its less developed network, Ireland, along with Greece, Portugal and Spain, was granted an additional transition period of up to five years to achieve the necessary structural adjustments, in particular of tariffs, for the liberalization of voice telephony services. The deadline for these four countries is therefore 1 January 2003. Luxembourg was allowed an additional transition period of up to two years. In its Resolution, the Council noted the intention of the Commission to work closely with these Member States in order to achieve the adjustments as soon as possible and in the best possible way within the period.

2.16 The 1987 Commission Green Paper expressly excluded from its scope satellite communications. These were the subject of a Green Paper in 1990.[56] The Paper proposed the extension of existing Community telecommunications policy to satellite communications, and was followed by a Council Resolution in 1991 on the development of the common market for satellite communication services and equipment.[57] In the Resolution, Council confirmed, without prejudice to future decisions, four major goals in satellite telecommunications policy identified in the Green Paper. These are:

> "1. harmonization and liberalization for appropriate satellite earth stations,including where applicable the abolition of exclusive or special rights in this area, subject in particular to conditions necessary for compliance with essential requirements;
> 2. harmonization and liberalization as far as required to facilitate the provision and use of Europe-wide satellite telecommunications services subject, where applicable, to conditions necessary for compliance with essential requirements and special or exclusive rights;
> 3. separation in all Member States of regulatory and operational functions in the field of satellite communications;
> 4. improved access to the space segment and access to the space capacity of intergovernmental organizations operating satellite systems and effective and accelerated procedures for the establishment of the access to separate satellite systems".

In December 1993, Council passed a resolution recognizing "the importance of the planned use of satellites for personal communications, and of the opportunities this may offer for European industry, service providers, and users", and invited Member States "to make efforts towards developing as soon as possible a Community policy concerning satellite personal communications".[58] Then, in October 1994, the Commission adopted a Draft Directive extending the scope of earlier Directives on telecommunications terminal equipment and telecommunications services[59] to cover satellite communications.[60] This Directive allows private operators in Member States to offer satellite-based services directly in competition with the telecommunications administrations and, subject to certain conditions, aims to abolish exclusive or special rights in this area.

2.17 In its 1987 Green Paper, the Commission proposed that it carry out a continuous review of the compatibility of operations within the telecommunications industry with the Community's competition rules; and in 1991

---

56 COM(90) 490 *final, Green Paper, Towards Europe-wide systems and services: a common approach in the field of satellite communications in the European Community*, 20 November 1990, reproduced in *Denton Hall*, at pp.A137-A151.

57 Council Resolution 92/C 8/01, 19 December 1991, reproduced in *Denton Hall*, at pp.A209-A211.

58 Resolution on the introduction of satellite personal communication services in the Community, reproduced in *Denton Hall*, at pp.A339-A341.

59 Directives 88/301/EEC and 90/388/EEC.

60 Directive 94/46, reproduced in *Denton Hall*, at pp.A360-A368.

it published Guidelines on the application of the competition rules to the telecommunications sector.[61] In the Introduction to the Guidelines, the Commission noted that:

> "The fundamental technological development worldwide in the telecommunications sector has caused considerable changes in the competition conditions. The traditional monopolistic administrations cannot alone take up the challenge of the technological revolution. New economic forces have appeared on the telecoms scene which are capable of offering users the numerous enhanced services generated by the new technologies. This has given rise to and stimulated a wide deregulation process propagated in the Community with various degrees of intensity. This move is progressively changing the face of the European market structure. New private suppliers have penetrated the market with more and more transnational value-added services and equipment. The telecommunications administrations, although keeping a central role as public services providers, have acquired a business-like way of thinking. They have started competing dynamically with private operators in services and equipment. Wide restructuring, through mergers and joint ventures, is taking place in order to compete more effectively on the deregulated market through economies of scale and rationalization. All these events have a multiplier effect on technological progress."[62]

Given these market developments, the Commission was of the opinion that there is a need for more certainty as to the application of the Community's competition rules.[63] The Guidelines essentially concern the direct application of competition rules to undertakings.[64] Articles 85 and 86 of the EEC Treaty deal with "undertakings", and for some time there was doubt as to whether telecommunications administrations were included in this term. The Commission's view that they are was upheld by the European Court of Justice in a case involving British Telecommunications, which at the time held a statutory monopoly of the operation of telecommunications systems in the United Kingdom.[65] In the Guidelines, the Commission reiterated its view that:

> "... Articles 85 and 86 apply both to private enterprises and public telecommunications operators embracing telecommunications administrations and recognized private operating agencies, hereinafter called 'telecommunications organizations' (TOs).
>
> TOs are undertakings within the meaning of Articles 85 and 86 to the extent that they exert an economic activity, for the manufacturing and/or sale of telecommunications equipment and/or for the provision of

---

61 These are reproduced in *Denton Hall*, at pp.A179-A207.
62 Para. 3 of the Guidelines.
63 *Ibid.*, para. 6.
64 *Ibid.*, para. 12. They do not concern those applicable to the Member States, in particular Articles 5 and 90(1) and (3).
65 Case 41/83, *Italy v. Commission*, [1985] E.C.R. 873.

telecommunications services, regardless of other facts such as, for example, whether their nature is economic or not and whether they are legally distinct entities or form part of the State organization."[66]

As regards paragraph 2 of Article 90 of the EEC Treaty,[67] it inferred from the case law of the European Court of Justice[68] that the Commission itself:

> "... has exclusive competence, under the control of the Court, to decide that the exception of Article 90(2) applies. The national authorities including judicial authorities can assess that this exception does not apply, when they find that the competition rules clearly do not obstruct the performance of the task of general economic interest assigned to undertakings. When those authorities cannot make a clear assessment in this sense they should suspend their decision in order to enable the Commission to find that the conditions for the application of that provision are fulfilled."[69]

2.18 In 1992 the Commission submitted to the Council a communication on the situation in the market for telecommunications services.[70] This initiated a wide-ranging debate in the Community on the future of telecommunications, and in 1993 the Council adopted a Resolution on the review of the situation in the telecommunications sector and the need for further development in that market.[71] The Council noted in the Resolution that there is a general acceptance that liberalization of telecommunications services markets is the inevitable result of technological and market developments and identified a number of major goals for the Community's telecommunications policy in both the short and the longer term. Among the short term goals are the extension of

---

66 Para. 20 of the Guidelines. The paragraph further provides that:

> "Articles 85 and 86 apply also to undertakings located outside the EEC when restrictive agreements are implemented or intended to be implemented or abuses are committed by those undertakings within the common market to the extent that trade between Member States is affected."

67 See above para. 2.11.

68 Case 10/71, *Mueller-Hein*, [1971] E.C.R. 723; and Case 66/86, *Ahmed Saeed*, [1989] E.C.R. 803.

69 Para. 23 of the *Guidelines*.

70 EEC (92) 1048 final, 21 October 1992.

71 Resolution 93/C 213/01, 22 July 1993, reproduced in *Denton Hall*, at pp.A265-A268.

open network provision,[72] and among the longer term the liberalization of all public voice telephony services.[73]

2.19 Similarly, postal services are also undergoing a radical transformation as a result of developments in technology and market demand. One example of this change is the development of postal electronic mail which is provided by all the postal administrations in the European Union.[74] There are three main forms of such mail:

(i) Individual message delivery[75];
(ii) Bulk distribution of one message[76];
(iii) Electronic Data Interchange (EDI).[77]

The future demand for postal electronic mail is uncertain since it competes in the market with private fax, telex and express mail services. All electronic mail operators (both postal and non-postal) are free to establish their own networks using leased lines, equipment which they choose for their own needs and their

---

72 The major goals for the Community's telecommunications policy in the short term are:

1. the adoption of legislative proposals in the field of ONP and satellites, together with rapid and effective implementation of existing Community legislation in the field of telecommunications services and ONP;
2. the application throughout the Community and, where necessary, the adaptation, in the light of further liberalization, of ONP principles in respect of the entities covered and of such issues as universal service, interconnection questions connected with licensing conditions;
3. the development of future Community policy in the field of mobile and personal communications;
4. the development of future Community policy in the field of telecommunications infrastructure and cable TV networks;
5. the working-out of arrangements for suitable measures in relation to specific difficulties encountered by the peripheral regions with less developed networks. Such measures, as a complement to national funding, should where appropriate, and taking into account the priorities set at national level, make full use of appropriate Community support frameworks to assist network development and universal service in peripheral regions;
6. the taking into account by the Commission, in the preparation of the steps to implement the goals of this Resolution, of the specific situation of small networks.

73 The longer term goals are:

1. the liberalization of all public voice telephony services, whilst maintaining universal service;
2. ensuring the balance between liberalization and harmonization in an evolving market;
3. the examination, prior to full liberalization of all public voice telephony services, of progress on structural adjustment, in particular of tariffs, in those countries experiencing specific difficulties, in order to take account of the situation of the peripheral regions with less developed networks and of very small networks, including the fixing of additional transition periods, where justified;
4. the working out of a future policy for telecommunications infrastructure, on the basis of the result of a broad consultation process following the publication of the Green Paper on infrastructure.

74 For a description of postal electronic mail services, see Annex 12, Commission of the European Communities, *Green Paper on the Development of the Single Market for Postal Services*, COM(91) 476 final, 11 June 1992, p.339.

75 This involves the transmission of text and/or images to a postal administration operated fax machine close to the addressee. The transmitted message is then converted into "hard copy", placed in an envelope and delivered as a postal item to the addressee.

76 This involves a customer supplying the postal administration with an address list together with the message to be sent to each address. Both the list and the message are transmitted to the relevant office, which then prints out the message in individually addressed letters. The letters are placed in envelopes and delivered as postal items to the addressees.

77 This is an electronic method for transmitting quantitative information. It relies on information being input in strictly formatted fashion, and is particularly interesting to large companies exchanging large amounts of quantitative information. It can also be used by postal operators to communicate with their customers. See the 1992 Commission *Green Paper*, p.365.

own access protocols.[78] Moreover, individuals may now acquire their own fax machines for private and business purposes, and if both sender and recipient possess such machines, there may be no need to use the services of the postal administration, at least for individual message delivery.

2.20 EU policy in the area of postal services mirrors that in the telecommunications sector, but is at a somewhat less advanced stage. The Commission produced a Green Paper on the Development of the Single Market for Postal Services in 1992,[79] and will make its final proposals and, if appropriate, draw up draft directives in the light of the views and information it receives during the following consultation process.

2.21 In the Paper, the Commission identified the maintenance of a universal postal service which would provide collection and delivery facilities throughout the European Union, at prices affordable to all and with a satisfactory quality of service, as the fundamental principle governing the postal services. Subject to this overriding objective, it was of the view that there should be as much freedom of choice as possible for customers of these services. It pointed out that the sector was already significantly liberalised. In no Member State was there any longer a monopoly of parcel services and express services were monopolised in only three of the twelve Member States, one of them being Ireland.[80] These two markets, the parcel and the express, have been growing significantly and the practical effect of them being non-reserved was that approximately 43% of the postal sector's revenue was generated at the time by private operators.[81] The Commission suggested that express services and publications should be completely removed from the reserved sector, but recognised that in order to ensure a universal service national postal administrations should continue to enjoy some special and exclusive rights, principally with respect to personal and business correspondence. These rights should however be strictly proportional to the need to secure a universal service, and clear limits should be established indicating the precise scope of the reserved area. These limits would be defined in terms of weight and price.

2.22 The dismantling of postal and telecommunication monopolies and the increased deregulation and privatisation of postal and telecommunications services is a universal phenomenon. When the International Telecommunication Union,[82] an intergovernmental organisation, was being restructured in 1992, provision was made in the ITU Convention for the participation of entities and organizations other than administrations[83] in the Union's activities. Under Article 19(1) of the Convention, the Secretary-General and the Directors of the

---

78 *Ibid.*, p.341.
79 COM(91) 476 final, 11 June 1992.
80 The other two were France and Portugal.
81 See p.33 of the *Green Paper*.
82 See below paras. 7.63-7.67.
83 'Administration' is defined in an Annex to the ITU Constitution as 'any governmental department or service responsible for discharging the obligations undertaken in the Constitution of the International Telecommunication Union, in the Convention of the International Telecommunication Union and in the Administrative Regulations.'

Bureaux of the ITU shall encourage the enhanced participation in the activities of the Union of the following entities and organizations:

> "a) recognised operating agencies, scientific or industrial organizations and financial or development institutions which are approved by the Member concerned;
>
> b) other entities dealing with telecommunication matters which are approved by the Member concerned;
>
> c) regional and other international telecommunication, standardization, financial or development organizations."

An "operating agency" is:

> "any individual, company, corporation or governmental agency which operates a telecommunication installation intended for an international telecommunication service or capable of causing harmful interference with such a service"[84];

and a "recognized operating agency" is any operating agency, as defined above:

> "which operates a public correspondence or broadcasting service and upon which the obligations provided for in Article 6 of [the ITU] Constitution[85] are imposed by the Member in whose territory the head office of the agency is situated, or by the Member which has authorized this operating agency to establish and operate a telecommunication service on its territory."[86]

The Directors of the various ITU Bureaux are required to:

> "maintain close working relations with those entities and organizations which are authorized to participate in the activities of one or more of

---

84 Annex to the ITU Constitution, *Definition of Certain Terms Used in this Constitution, the Convention and the Administrative Regulations of the International Telecommunication Union.*

85 Article 6 is headed, 'Execution of the Instruments of the Union', and provides:

> '1. The Members are bound to abide by the provisions of this Constitution, the Convention and the Administrative Regulations in all telecommunication offices and stations established or operated by them which engage in international services or which are capable of causing harmful interference to radio services of other countries, except in regard to services exempted from these obligations in accordance with the provisions of Article 48 of this Constitution.
>
> 2. The Members are also bound to take the necessary steps to impose the observance of the provisions of this Constitution, the Convention and the Administrative Regulations upon operating agencies authorized by them to establish and operate telecommunications and which engage in international services or which operate stations capable of causing harmful interference to the radio services of other countries.'

86 *Ibid.* A recognized operating agency may act on behalf of the Member which has recognized it, provided that Member informs the Director of the ITU Bureau concerned that it is authorized to do so: Art. 19(9) of the Convention.

the Sectors[87] of the Union."[88]

Lists of these entities and organizations are compiled and maintained by the Secretary-General of the Union.[89] Bord Telecom Éireann is a recognized operating agency and participates as such in the activities of the ITU.

2.23 In contrast, participation in the activities of the Universal Postal Union[90] has been limited to date to member countries and their postal administrations. Postal administrations around the world have been concerned at the major inroads being made by private companies into their traditional markets. The range of products offered by these companies has often been better suited to market needs and their rates more reasonable than those charged by the administrations. The UPU has sought to propose and to coordinate joint action by postal administrations aimed at counteracting the effect of competition from private companies.[91]

(iii) Deregulation of postal and telecommunications services in Ireland

2.24 In 1983, many functions exercised by the Minister for Posts and Telegraphs in respect of postal and telecommunications services in Ireland were assigned by legislation to two new companies: An Post and Bord Telecom

---

87 There are three Sectors: Radiocommunication, Telecommunication Standardization and Telecommunication Development. See Chapters II-IV of the ITU Constitution.

88 Art. 19(2). The importance of encouraging more participants with appropriate rights and obligations to contribute to the success of the Union was also addressed in a resolution passed by the Additional Plenipotentiary Conference of the ITU in Geneva in 1992: Resolution 4, Participation of Entities and Organizations Other than Administrations in the Activities of the Union. The Resolution recognised that the procedures and conditions for participation and the rights and obligations of participants may differ among the categories of participants, and instructed the Council of the ITU to study the criteria and procedures to govern participation in Union activities by entities and organizations specified in Art. 19(1)(b) & (c) of the Convention and to make recommendations accordingly to the Plenipotentiary Conference to be held in Kyoto in 1994.

89 Art. 19(7).

90 See below paras. 7.54-7.62.

91 See, e.g., Resolution C 27/1989 of the 1989 Congress of the UPU in Washington, reproduced in Vol. 3 of the *UPU Annotated Code*, International Bureau of the UPU, Berne, 1991, at pp.189-190.

Éireann.[92] Exclusive privileges were conferred on each company in relation to the provision of services in their respective fields[93]; but the Minister for Transport, Energy and Communications[94] owns shares in the companies and retains a certain amount of control over them.[95]

2.25 This legislation, the *Postal and Telecommunications Services Act, 1983*,[96] is the principal statute governing the provision of postal and telecommunications services in the State. Under it, An Post has "the exclusive privilege in respect of the conveyance of postal packets within, to and from the State and the offering and performance of the services of receiving, collecting, despatching and delivering postal packets"[97]; and Bord Telecom Éireann has "the exclusive privilege of offering, providing and maintaining telecommunications services for transmitting, receiving, collecting and delivering telecommunications messages within the State up to (and including) a connection point in the premises of a subscriber for any such service."[98] It is to be noted that the exclusive privilege of An Post applies to the conveyance of postal packets not only within the State

---

92 Under s.12(1) of the Postal and Telecommunications Services Act, 1983, the principal objects of An Post are stated in its memorandum of association to be:

> "(a) to provide a national postal service within the State and between the State and places outside the State,
>
> (b) to meet the industrial, commercial, social and household needs of the State for comprehensive and efficient postal services and, so far as the company considers reasonably practicable, to satisfy all reasonable demands for such services throughout the State,
>
> (c) to provide services by which money may be remitted (whether by means of money orders, postal orders or otherwise) as the company thinks fit,
>
> (d) to provide counter services for the company's own and Government business and, provided that they are compatible with those services and with the other principal objects set out in this subsection, for others as the company thinks fit, and
>
> (e) to provide such consultancy, advisory, training and contract services inside and outside the State as the company thinks fit."

Under s.14(1) of the Act, the principal objects of Bord Telecom Éireann are stated in its memorandum of association to be:

> "(a) to provide a national telecommunications service within the State and between the State and places outside the State,
>
> (b) to meet the industrial, commercial, social and household needs of the State for comprehensive and efficient telecommunications services and, as far as the company considers reasonably practicable, to satisfy all reasonable demands for such services throughout the State, and
>
> (c) to provide such consultancy, advisory, training and contract services inside and outside the State as the company thinks fit."

93 *Postal and Telecommunications Services Act, 1983*, ss.63(1) & 87(1). It is an offence to breach the exclusive privileges of An Post and Bord Telecom Éireann: see ss.63(6) & 87(4). See also s.6 of the *Telegraph Act, 1869* and s.4(1)(b) of the 1983 Act.

94 Originally the Minister for Posts and Telegraphs.

95 Other Ministers, notably the Minister for Finance, also play a role under the legislation in relation to the operation of the companies.

96 Hereafter "the 1983 Act".

97 Section 63(1).

98 Section 87(1). In the *Broadcasting and Wireless Telegraphy Act, 1988*, the expression "telecommunications service" is defined as meaning "a telecommunications service described in section 87(1) of the *Postal and Telecommunications Services Act, 1983*": see section 1.

but also to and from the State, whereas the privilege of Bord Telecom Éireann applies only to the provision of telecommunications services within the State.

2.26 These exclusive privileges are not truly exclusive in that licences may be granted to other bodies to provide services within the privileges. First, the Minister for Transport, Energy and Communications may, with the consent of the Minister for Finance, by order provide for the grant of a licence by the Minister to any person to provide a postal service or a telecommunications service of a class or description specified in the order to which an exclusive privilege granted to either An Post or Bord Telecom Éireann under the Act relates.[99] Any such licence may be subject to such terms and conditions as the Minister may think fit to impose.[100] Before providing for the grant of a licence, the Minister must consult with the relevant company, that is either An Post or Bord Telecom Éireann, and a licence may only be granted if, in the opinion of the Minister, the grant of the licence is in the public interest and is consistent with the reasons given in the Act[101] for the grant of the exclusive privilege.[102] Secondly, both An Post and Bord Telecom Éireann may, with the consent of the Minister for Transport, Energy and Communications and subject to such terms and conditions as the Minister may approve, grant, upon application, a licence to a person to provide a service within the exclusive privilege granted to it.[103] In both cases, where a licence is refused by the company, appeal may be made by the unsuccessful applicant to the Minister with whom the ultimate power of decision lies to grant or refuse a licence.[104]

2.27 Moreover, the statute provides that the above and certain other services are not to be regarded as a breach of the exclusive privileges granted to An Post and Bord Telecom Éireann. In respect of An Post, these other services are:

(i) the conveyance and delivery of a postal packet personally by the sender,

(ii) the sending, conveyance and delivery of a postal packet by means of a private individual otherwise than for hire or reward where that individual herself or himself delivers the packet to the addressee,

(iii) the sending, conveyance and delivery of a postal packet concerning the private affairs of the sender or the addressee by means of a messenger sent for the purpose by the sender or receiver of the packet provided that the messenger is either a member of the family or an employee of the sender or receiver thereof,

(iv) the sending, conveyance and delivery otherwise than by post of

---

99 Section 111(a).

100 *Ibid.*

101 See sections 63(2) and 87(2).

102 Section 111(1)(a).

103 Sections 73(1) and 89(1) respectively. Sections 73 and 89 may in fact now be regarded as effectively obsolete in that EU policy requires the separation of regulatory and operational functions. It would be incompatible with this policy for a national postal or telecommunications administration to grant licences to competitors.

104 Sections 73(4) and 89(4).

any document issuing out of a court or of any return or answer thereto,

(v) the sending, conveyance and delivery of a postal packet of the owner of a merchant ship or commercial aircraft or of goods carried in such a ship or aircraft by means of that ship or aircraft and its delivery to the addressee by any person employed for the purpose by the owner provided that no payment or reward, profit or advantage of any kind is given or received for the conveyance or delivery of the packet,

(vi) the sending, conveyance and delivery by means of a common carrier of postal packets concerning and for delivery with goods carried by the carrier, provided that no payment or reward, profit or advantage of any kind is given or received for the conveyance or delivery of those packets.[105]

In respect of Bord Telecom Éireann, the other services are:

(i) services provided and maintained by a person solely for the domestic use of that person,

(ii) services provided and maintained by a business for use between employees for the purposes of the business and not rendering a service to any other person,

(iii) services provided and maintained by a person by means of apparatus situated wholly in a single set of premises occupied by that person,

(iv) the operation of a broadcasting station under licence granted by the Minister for Transport, Energy and Communications,

(v) radio communications systems provided under licences granted under the *Wireless Telegraphy Acts, 1926* to *1972*,

(vi) cable television systems licensed under the *Wireless Telegraphy Acts, 1926* to *1972*.[106]

---

105 Section 63(3). See also s.63(4). The equivalent list in section 34(2) of the *Post Office Act, 1908*, which conferred exclusive privileges on the Postmaster-General with respect to the conveyance of letters, read:

> "(a) Letters sent by a private friend in his way, journey, or travel, so as those letters be delivered by that friend to the person to whom they are directed:
>
> (b) Letters sent by a messenger on purpose, concerning the private affairs of the sender or receiver thereof:
>
> (c) Commissions or returns thereof, and affidavits and writs, process or proceedings, or returns thereof, issuing out of a court of justice:
>
> (d) Letters sent out of the British Islands by a private vessel (not being a vessel carrying postal packets under contract):
>
> (e) Letters of merchants, owners of vessels of merchandise, or the cargo or loading therein, sent by those vessels of merchandise or by any person employed by those owners for the carriage of those letters, according to their respective directions, and delivered to the respective persons to whom they are directed, without paying or receiving hire or reward, advantage, or profit for the same in anywise:
>
> (f) Letters concerning goods or merchandise sent by common known carriers, to be delivered with the goods which those letters concern, without hire or reward or other profit or advantage for receiving or delivering those letters".

For the purposes of section 34, the expression "letter" included "packet": s.34(7). This section was repealed by the 1983 Act.

106 Section 87(3).

2.28 With respect to postal and telecommunications services outside the exclusive privilege of each company, no licence is required to provide a postal service, but a licence is generally required for the commercial provision of telecommunications services. Under s.111(2) of the 1983 Act, the Minister for Transport, Energy and Communications may, after consultation with Bord Telecom Éireann, grant a licence to any person to provide a telecommunications service of a kind not within the exclusive privilege granted to the Bord.[107] This licence requirement does not apply however to the first three exempted services listed above, that is services provided and maintained for domestic, business or occupiers' purposes.[108]

2.29 The exclusive privilege granted to Bord Telecom Éireann by the 1983 Act was radically modified by Regulations made in 1992 to give effect to European Council Directive No. 90/387/EEC of 28 June 1990[109] and Commission Directive No. 90/388/EEC of the same date.[110] Under paragraph (1) of Regulation 3 of the European Communities (Telecommunications Services) Regulations, 1992,[111] the exclusive privilege granted under the 1983 Act:

> "... shall, subject to paragraph (2) of this Regulation, be restricted to offering, providing and maintaining the public telecommunications network and offering, providing and maintaining voice telephony services."

The "public telecommunications network" is defined in the Regulations as meaning:

> "the public telecommunications infrastructure which permits the conveyance of signals between network termination points by wire, microwave, optical means or other electromagnetic means";[112]

and "voice telephone service" as meaning:

> "the commercial provision for the public of the direct transport and switching of speech in real-time between public switched network termination points, enabling any user to use equipment connected to such a network termination point in order to communicate with another termination point."[113]

Paragraph (2) of Regulation 3 provides that:

> "Nothing in paragraph (1) ... shall be construed as affecting the offer,

---

107 Section 111(2). See also s.111(3) & (4) concerning the conditions which may be attached to such a licence.
108 *Ibid.*
109 See above para. 2.14.
110 See above para. 2.13.
111 S.I. No. 45 of 1992.
112 Regulation 2, paragraph (1).
113 *Ibid.*

provision or maintenance by the Company within the State of telex services, mobile radio telephony services, paging services and satellite services which are within the exclusive privilege of the Company by virtue of section 87 of the Act of 1983."[114]

The exclusive privilege of Bord Telecom Éireann now therefore relates only to the following services:

(i) voice telephony;
(ii) telex;
(iii) mobile radio telephony;
(iv) paging[115]; and
(v) satellite communications.

Regulation 4 gives effect to the relevant paragraphs of the specified Council and Commission Directives with regard to open network provision conditions; and Regulation 5 makes the Minister for Transport, Energy and Communications[116] responsible "for surveillance of the Company's usage conditions".

2.30 With specific regard to licences, Regulation 7 inserts new procedural provisions into s.111 of the 1983 Act. Under a new subsection (2A), the Minister may grant a licence on the basis of a declaration by the applicant that the telecommunications service in respect of which the licence is being sought shall, at all times, comply, in all respects, with service conditions prescribed by the Minister as being applicable to the provision of a telecommunications service of the kind for which the licence is being sought. This provision was needed to implement the State's obligations under the Commission Directive with respect to the liberalisation of the markets for telecommunications services in the value added and data transmission areas. It is not altogether clear whether it stands alone or should be read together with the previous subsections (1) and (2) of s.111, but it appears that it was intended to be an entirely independent provision, and it is so treated for administrative purposes by the Department of Transport, Energy and Communications.[117] A new subsection (7) itemises the procedure to be followed if the Minister refuses to grant a licence under the new subsection (2A), or proposes to revoke or suspend a licence granted under the subsection, and includes provision for appeal by the applicant in case of refusal, revocation

---

114 The Directives did not cover these services: see above n. 35.

Section 87(1) of the 1983 Act, as amended by Regulation 3, reads:

> "(1) The Company shall, subject to the provisions of this section and Regulation 3 of the European Communities (Telecommunications Services) Regulations, 1992, have the exclusive privilege of offering, providing and maintaining telecommunications services for transmitting, receiving, collecting and delivering telecommunications messages within the State up to (and including) a connection point in the premises of a subscriber for any such service."

115 It should however be noted that, by virtue of s.87(3)(e) of the 1983 Act, radio communications systems provided under licences granted under the *Wireless Telegraphy Acts, 1926* to *1972* are not to be regarded as a breach of the Bord's exclusive privilege. A number of different types of licence, including paging licences, have been granted under these Acts: see further below paras. 5.31-5.35.

116 Originally the Minister for Tourism, Transport and Communications.

117 Information supplied by the Department, 19 October 1994.

or suspension to the District Court and for further appeal on a question of law to the High Court.

2.31 No licence has been granted under the 1983 Act by either the Minister or An Post in respect of postal services within the exclusive privilege of the latter.[118] Clearly a number of private couriers are operating in the Irish market. In so far as they convey and deliver parcels, they do not fall within the exclusive privilege of An Post with respect to postal packets.[119] It would seem, however, that some of the items they carry do come within the privilege. Their services do not feature on the statutory list of services which are not to be regarded as a breach of An Post's exclusive privilege,[120] and some of the items they carry undoubtedly fall within the definition of postal packets.[121] These apparent breaches of An Post's statutory privilege appear to be tolerated by both An Post and the Minister. This tolerance may be due in large part to the fact that Ireland is one of the few remaining EU states to maintain a monopoly in respect of express services, and that the European Commission has explicitly recommended that these services be taken out of the area reserved to national postal administrations.[122]

2.32 The law with respect to the licensing of telecommunications services is also somewhat outdated due to EU developments. Bord Telecom Éireann has itself been issued with a licence by the Minister to provide international services (which are outside its exclusive privilege). At present, the Bord alone provides a GSM service,[123] but it is expected that the Minister will licence a second GSM service provider in order to bring Ireland into line with other EU countries in this field,[124] and this licence will include the provision of services within the exclusive privilege of the Bord.[125] Most licences for the provision of telecommunications services have been granted under the new subsection (2A) of s.111 of the 1983 Act, as inserted by the European Communities Regulations of 1992. As of 29 January 1995, twenty-eight licences had been granted under this subsection. Essentially they cover any telecommunications service other than voice telephony or other services within the exclusive privilege of Bord Telecom Éireann. The licensed services include video-conferencing,[126] facsimile and data transmission. In applying for a licence, an applicant undertakes to comply with a number of service conditions and these conditions are recited in any licence granted. They include a condition that the telecommunications services

---

118 Information supplied by the Department of Transport, Energy and Communications, 7 September 1994.

119 Unless a communication is contained in the parcel: see s.63(7) of the 1983 Act, and further below para. 5.49.

120 Section 63(3) of the 1983 Act.

121 See below paras. 5.45-5.52.

122 See above para. 2.21.

123 Global System for Mobile Communications. This is a second generation digital mobile system which enables a person to use radio telephone equipment to roam among other telecommunications networks both domestically and internationally (provided the necessary roaming agreements have been concluded).

124 See the Tables reproduced at pp.121 and 156 of *Towards the Personal Communications Environment: Green Paper on a common approach in the field of mobile and personal communications in the European Union*, Commission of the European Communities, COM(94) 145 final, 27 April 1994.

125 The company, ESAT Digifone, was the successful bidder in a tender competition in 1994 for the licence to provide a second GSM service.

126 This involves the transmission of pictures whereby telephone users may see one another as well as talk to one another.

provided shall utilise telecommunications links provided by Bord Telecom Éireann under its exclusive privilege and also a condition that the services shall utilise international telecommunications links provided by Bord Telecom Éireann or other network operators licensed by the Minister for Transport, Energy and Communications for the international conveyance of telecommunications messages.[127]

Conclusion

2.33 Recent technological and economic developments are of enormous social significance. They confer many benefits on society and the individual, but they also bring some problems in their train. One of the areas in which the latter are evident is that of privacy.

2.34 The scope and pace of technological change is such that individuals are exposed to the risk of surveillance to an extent that was not possible in the past; and there is no indication that the scope and pace of this change will decelerate in the near future. Technological developments have contributed to the risk of surveillance and the attendant erosion of privacy in a number of ways.

2.35 First, the devices which may be used for surveillance have become increasingly sophisticated and are often easy to conceal by virtue of miniaturisation or through careful placing or disguise as an article commonly in use such as a pen. Surveillance is therefore easier to carry out and less easy to detect than formerly was the case.

2.36 Secondly, the forms of personal communication are being revolutionised by developments in the fields of telecommunications and computer technology. Messages sent by some of these new forms of communication are intrinsically vulnerable to interception and to being read either deliberately or inadvertently by persons other than the intended recipient. Electronic mail can be read by another person with computer access to the mailing network. A conversation on a mobile telephone may be accidentally intercepted by a radio ham as well as deliberately eavesdropped without difficulty.

2.37 Technology itself may provide a means of counteracting these risks, particularly the risk of being overheard by a listening device. A scrambler may be used to render a telephone conversation unintelligible to the human ear.[128] A jammer or a radio noise generator may be used to interfere with the radio signals emitted by electronic audio surveillance equipment. Or resort may be had to a "squealer" (also known as a "howler" or "screamer") which causes feedback when positioned near a transmitter. Detectors and sweeping devices may be used

---

127 See the standard application form and licence reproduced in Appendices A and B respectively.

128 Scramblers are speech-inversion and/or frequency-inversion devices that code audio frequencies so that they are not intelligible to the human ear. They are also sophisticated digital devices which change voice into a digital form upon transmission and/or reconvert it into intelligible voice at its intended destination.

to minimise the risk from clandestine bugging.[129] Highly sophisticated encryption techniques offer a solution to the inherent susceptibility of mobile communications to interception. No comparable range of countermeasures exists in respect of optical surveillance; but a form of encryption may be used for electronic mail and for fax messages, coupled with a form of decryption at the receiving end. As well as security measures which may be taken by individuals to counteract the risk of an invasion of their privacy, the providers of postal and telecommunications services may be expected to take certain measures to maintain the confidentiality of communications sent via their services and to afford certain security options to their customers.[130]

2.38 Where counter surveillance equipment is available, and particularly where it is also inexpensive, it may be reasonable to expect persons who wish to secure their privacy to have recourse to them at least as a first line of defence. A prudent individual will not confide intimate secrets to another person in a loud voice in a crowded room. That individual will realise that there is a high risk that such behaviour will result in the information not remaining secret. Rather she or he will seek out a quiet spot to communicate the information, that is, the person will tailor their behaviour to protect their privacy. Similarly, in the case of overt video surveillance, a person who wishes to conceal something from the prying eye of the camera will conduct herself or himself accordingly. Likewise, if a person can reasonably be expected to be aware of a risk to their privacy from covert surveillance equipment, particularly if the risk is a high one, then that person can also be expected to take reasonable countermeasures to protect their own privacy.

2.39 The fact that counter surveillance equipment exists and is readily obtainable or that other countermeasures could easily have been taken does not however necessarily mean that the law has no role to play in affording protection against the particular surveillance. Not only may the law act as a deterrent to snoopers. It may also provide primary protection in the form of an injunction when surveillance is apprehended and subsidiary protection in the form of a remedy where countermeasures have failed. Moreover, it may not be possible or reasonable for countermeasures to be taken. It may however be appropriate, in formulating and in interpreting any protection afforded by the law, to pay some regard to the feasibility of countermeasures and to whether a person could reasonably be expected to have recourse to them or not.

2.40 Furthermore, the fast pace of technological change means that existing rules and procedures may become outdated. The more narrowly framed and

---

129 Detection of an ultra high frequency listening device is however difficult, even when bug-sweeping equipment is used.

130 The European Telecommunications Standards Institute has considered security in relation to telecommunications systems: see, e.g., ETSI Technical Report 083, *Universal Personal Telecommunication (UPT); General UPT security architecture*, July 1993, and the Bibliography at Annex A of the Report. The Report mentions that fraud levels in the U.S. system of analogue mobile phones were as high as 30% in the mid 1980s because the system did not have built into it strong security and fraudsters exploited this. When anti-fraud mechanisms were introduced, the level of fraud fell to 2%-5%, but as fraudsters found new technical holes in a structurally weak mechanism, the level of fraud increased again: see para. 2.3.4 of the Report.

precisely targetted they are, the greater the risk of obsolescence. Rules regulating the interception of telephone conversations will not cover communication by fax. Rules governing telephone tapping will not apply to covert recording of what is said at a meeting. Also, lists of surveillance devices which may not lawfully be imported or sold in a country invite evasion by technological innovation.[131] It is desirable that the law be phrased with a sufficient degree of generality that the courts and other bodies entrusted with the interpretation and application of the law are not precluded from taking new developments into account. At the same time, if individual liberty is to be respected, the rules must not be so general that the ordinary citizen has little idea what they cover and what they do not.[132] This is particularly important if criminal sanctions are to be employed for breach of the rules.

2.41 Technological developments coupled with market forces have the further consequence that the risk to privacy is more broadly based than heretofore. Both audio and optical equipment is readily available on the Irish market. The extent of audio surveillance is difficult to assess given that much of it is covert and probably illegal.[133] Optical surveillance, on the other hand, is often quite visible. It is widely used in banks, department stores, etc. for security and other legitimate purposes. A degree of such surveillance is now an inherent feature of certain aspects of social intercourse and appears to be generally accepted. While covert surveillance poses an obvious risk to privacy, a risk also arises in respect of overt surveillance. The fact than surveillance is known to the person being observed is no guarantee of that person's privacy. A person may know that a press photographer is using a powerful telephoto lens to get pictures of the person at home, but not agree to the taking of the pictures and feel intruded upon. A video camera installed for a legitimate purpose may be used for illegitimate purposes, such as the invasion of a person's privacy. The wide availability of such equipment means that there has been a proliferation in the number of potential violators of privacy by means of surveillance.

2.42 More generally, the current economic climate with its emphasis on competition, fostered regionally by the European Union but evident globally, has added to the complexity of regulating surveillance in that monopolies and special or exclusive rights in the supply of goods and services are being increasingly abolished. It is no longer sufficient, for example, for the lawful interception of post and telecommunications for legitimate public interests such as the detection of crime and the protection of national security to be based solely on a procedure involving the personnel of a semi-state monopoly in either of these fields. As communications equipment and services are liberalised, the legal framework for both legitimate state intervention and for the protection of the privacy of the users of a communications system must take account of the multiplicity of private suppliers.

---

131 See below paras. 11.46-11.49.
132 See further below paras. 5.12 & 7.21.
133 See below paras. 11.1-11.4.

2.43 Furthermore, operational requirements as, for example, when checking a suspected fault on a telecommunications system, may entail the overhearing of a private conversation. Whereas formerly, when there was a monopoly of telecommunications, the risk of being overheard as a result of such requirements was localised in a specific organisation, now the risk is spread over a greater number of operators; and the rules to protect a user's privacy need to take account of the disseminated nature of the risk.

2.44 The liberalisation of postal services is underway; and although liberalisation of the telecommunications sector may be delayed until 2003 following the derogation granted Ireland in this regard in EU Council Resolution of 22 July 1993 on the review of the situation in the telecommunications sector and the need for further development in the market, it is also in train. The consequences of the liberalisation of both postal and telecommunications services need to be faced. Even in the area of satellite services which have traditionally been provided by government-owned domestic, regional or international satellite service providers there has, over the last few years, been a significant increase in the number of privately owned and operated satellite systems. The ASTRA Satellite System, which is based in Luxembourg and owned by Société Européenne des Satellites, is an example. As the European Commission has predicted, not only will competition between operators of public networks and systems be a key feature of the future personal communications environment, a major consequence of an open environment for service provision could be the emergence of new telecommunications players to exploit the opportunities of personal communications and synergies with activities in other sectors.[134] Any measures designed to protect the privacy of users of these services must take account of both the multiplicity of players and the diversity of the services provided.

2.45 As regards the multiplicity of players in the provision of postal and telecommunications services, it is worthy of note that the licence provisions of the 1983 Act to some extent recognise the need for the extension of legislative regulation to the providers of these services other than An Post and Bord Telecom Éireann. Where a licence is granted by the Minister under s.111 of the Act:

> "... to any person to perform any function every provision of this Act or any other enactment relating to the appropriate company which is specified in regulations made by the Minister under this section shall in respect of that function and subject to such conditions, limitations or modifications as may be prescribed in such regulations, apply to the licensee as it applies to the company."[135]

However, while this provision covers licensed commercial services in the

---

134 See *Towards the Personal Communications Environment: Green Paper on a common approach in the field of mobile and personal communications in the European Union*, pp.95 & 96.

135 Section 111(5).

telecommunications sector whether or not the service falls within the exclusive privilege of Bord Telecom Éireann, in the postal sector, it applies only to the licensing of any service within the exclusive privilege of An Post. No licence is required for the provision of a postal service falling outside the exclusive privilege of An Post.

2.46 Clearly, the participation of many private actors in the surveillance field means that it is not only protection against overly invasive public authority which is needed. As important today is protection against the invasion of privacy by an increasing array of private individuals. The kind and degree of protection needed against privacy-invasive surveillance by private actors will of course often, but not invariably, be different to those required in respect of public authority and may even differ between private actors. Whereas, in the case of private surveillance, a balance has to be drawn between the private interests of the observed and the observer, in the case of surveillance by a public authority, the balance is between the individual interest in privacy and the public interest in surveillance. The law may need to take account of the different interests to be balanced depending on whether the surveillance is conducted by a public authority or a private individual; but legal protection is required irrespective of the source of the threat to privacy. To leave threats to privacy from private sources entirely to market forces and individual initiative is unacceptable in a society which values individual human dignity and worth.

PART 2: THE LAW IN IRELAND

CHAPTER 3: THE CONSTITUTION

The Constitutional Basis Of The Protection of Privacy[1]

3.1 The Constitution does not afford any explicit protection to a right of privacy. However, over the last twenty years, the High and the Supreme Courts have so construed the provisions of the Constitution, in particular, the fundamental rights provisions, as to afford a degree of protection to privacy interests. Some judges have identified specific provisions as guaranteeing particular aspects of privacy, while others have examined any claim to privacy solely in the context of the personal rights which the State guarantees to defend and vindicate under Article 40.3.1°.[2]

3.2 In *McGee v. The Attorney General*,[3] Walsh J. identified the "sexual life of a husband and wife [as] of necessity and by its nature an area of particular privacy."[4] In his view, this area is screened from unjustified invasion by the State by virtue of Article 41 which protects the institution of the family.[5] More generally, Henchy J. stated in *Norris v. The Attorney General*[6] that among the basic personal rights enjoyed by the citizen under the Constitution:

> "... is a complex of rights which vary in nature, purpose and range (each

---

1 See, in general, J. P. Casey, *Constitutional Law in Ireland*, 2nd ed., Sweet & Maxwell, London, 1992, pp.317-320; R. Clark, *Data Protection Law in Ireland.*, Round Hall Press, Dublin, 1990, pp.6-10; M. Forde, *Constitutional Law of Ireland*, Mercier Press, Cork and Dublin, 1987, ch. XX; and J. M. Kelly, *The Irish Constitution*, 3rd ed. (by G. Hogan and G. Whyte), Butterworths, Dublin, 1994, pp.767-770. See also our *Consultation Paper on the Civil Law of Defamation*, 1991, Appendix A, where we briefly considered the constitutional right to privacy in the context of our examination of civil liability for defamation.

2 Article 40.3.1° provides:

> "The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen."

3 [1974] I.R. 284.

4 At p.312.

5 At pp.311-314.

6 [1984] I.R. 36.

necessarily being a facet of the citizen's core of individuality within the constitutional order) and which may be compendiously referred to as the right of privacy. An express recognition of such a right is the guarantee in Article 16, s.1, sub-s.4, that voting in elections for Dáil Éireann shall be by secret ballot. A constitutional right to marital privacy was recognized and implemented by this Court in *McGee v. The Attorney General*[7]: the right there claimed and recognized being, in effect, the right of a married woman to use contraceptives ... There are many other aspects of the right of privacy, some yet to be given judicial recognition ... they would all appear to fall within a secluded area of activity or non-activity which may be claimed as necessary for the expression of an individual personality, for purposes not always necessarily moral or commendable, but meriting recognition in circumstances which do not engender considerations such as State security, public order or morality, or other essential components of the common good."[8]

McCarthy J. elaborated even further in the same case on those constitutional provisions which, in his view, afford protection to aspects of privacy:

> "... there is a guarantee of privacy in voting under Article 16, s.1, sub-s.4 - the secret ballot; a limited right of privacy given to certain litigants under laws made under Article 34; the limited freedom from arrest and detention under Article 40, s.4; the inviolability of the dwelling of every citizen under Article 40, s.5; the rights of the citizens to express freely their convictions and opinions, to assemble peaceably and without arms, and to form associations and unions - all conferred by Article 40, s.6, sub-s.1; the rights of the family under Article 41; the rights of the family with regard to education under Article 42; the right of private property under Article 43; freedom of conscience and the free expression and practice of religion under Article 44. All these may properly be described as different facets of the right of privacy..."[9]

In addition, both these judges regarded the personal rights comprehended by Article 40, s.3 as including a more general right of privacy.[10]

3.3 In contrast, some judges, rather than identifying aspects of privacy which are guaranteed by various provisions of the Constitution, have distinguished between the right of privacy itself and other constitutionally guaranteed rights of a personal kind. In *Murray v. Ireland*,[11] in the High Court, Costello J. regarded the right of a spouse to beget children as an unspecified personal right protected by Article 40.3.1° of the Constitution and as distinct from "the right to marry, the right to marital privacy and the right to resolve matters relating to the

---

7 [1974] I.R. 284.
8 [1984] I.R. 36 at 71-72.
9 At p.100.
10 At pp.71 (Henchy J.) and 100-101 (McCarthy J.).
11 [1985] I.R. 532.

procreation of children"[12] which are likewise protected by Article 40.3.1°.[13] The Supreme Court agreed that the right of each spouse in marriage to beget children is protected by Article 40.3.1°. Four Justices were of the opinion that:

> "... the fact that the Constitution so clearly protects the institution of marriage necessarily involves a constitutional protection of certain marital rights. They include the right of cohabitation, the right to take responsibility for and actively participate in the education of any children born of the marriage, the right to beget children or further children of the marriage, the right to privacy within the marriage: privacy of communication and of association."[14]

These judges were however silent as to the precise constitutional basis of the rights other than the right to beget children, and it is therefore unclear whether these rights also obtain their protection from Article 40.3.1° or from other Articles such as Articles 41 (The Family) and 42 (Education). The fifth judge, McCarthy J., after identifying the right to procreate children within marriage as one of the unenumerated rights guaranteed by Article 40 gave as one of a number of examples of other rights (the enjoyment of which is also suspended while a person is deprived of liberty according to law) the right to be let alone, a description which he had accepted in an earlier case as pertaining to the right of privacy guaranteed by Article 40.3.1°.[15]

3.4 There is therefore considerable uncertainty over the particular constitutional basis of the protection of various aspects of privacy and over whether certain interests are properly classified under the heading of privacy or are to be treated as distinct matters. It now seems to be established however that at least certain privacy interests are included among the unspecified personal rights guaranteed by Article 40.3.1° of the Constitution.

The Unspecified Right Of Privacy

3.5 The Supreme Court first accepted that Article 40.3.1° of the Constitution affords some protection to privacy interests in 1973 in the case of *McGee v. The Attorney General*.[16] This case concerned a challenge to the constitutional

---

12 At p.537.

13 Citing *Ryan v. The Attorney General* [1965] I.R. 294 and *McGee v. The Attorney General* [1974] I.R. 284 as "strong and persuasive authority".

14 Finlay C.J., at p.472, Hamilton P., O'Flaherty and Keane JJ. concurring. They added that it was:

> "an inevitable practical and legal consequence of imprisonment as a convicted person that a great many of these constitutional rights arising from the married status are for the period of imprisonment suspended or placed in abeyance";

and that, in their opinion, of the rights listed:

> "only a right of communication, and that without privacy, and a right by communication to take some part in the education of children of the marriage would ordinarily survive a sentence of imprisonment as a convicted prisoner."

15 In *Norris v. The Attorney General* [1984] I.R.36 at 101. Hamilton P., O'Flaherty and Keane JJ. also concurred with this view as to the suspension of the enjoyment of certain rights during a period of lawful detention.

16 [1974] I.R. 284.

validity of a statutory provision which prohibited the importation into Ireland of contraceptives. A majority of the Court held that the statutory prohibition on the importation of contraceptives constituted an illegitimate intervention by the State in the sexual relations between a husband and wife, there being no sufficient justification grounded in the common good for such intervention.

3.6 Three of the judges in the majority were of the view that privacy was among the personal rights which the State guarantees in Article 40.3.1° to respect, defend and vindicate, as far as practicable. Two of the three, Griffin and Henchy JJ., specifically limited their treatment of privacy to the field of marital relations. Budd J., however, placed the marital relationship within a larger context of privacy:

> "... it is scarcely to be doubted in our society that the right to privacy is universally recognized and accepted with possibly the rarest of exceptions, and that the matter of marital relationship must rank as one of the most important of matters in the realm of privacy."[17]

3.7 Although this was a landmark case in that it established that Article 40.3.1° affords some protection to privacy, it left many questions unanswered. Most importantly, with the exception of Budd J., the judges gave no indication of the extent to which, if at all, Article 40.3.1° protects privacy interests other than those within a marital context.

3.8 Subsequent case law has made it clear that Article 40.3.1° does protect other privacy interests but the range of these interests is as yet ill-defined. It has only been successfully pleaded on one other occasion to date - in relation to telephone tapping.[18] It has been pleaded unsuccessfully in relation to sexual relations between a husband and wife in prison,[19] publicity given to the adulterous sexual relations of a wife,[20] distress which would be caused to minor children by publication of details of parental infidelity,[21] homosexual relations between consenting adult males,[22] tax matters,[23] financial transactions,[24] intensive garda surveillance[25] and the admission of certain evidence in court.[26]

---

17 At p.322. As we have seen, the fourth judge in the majority, Walsh J., identified the "sexual life of a husband and wife" as being "of necessity and by its nature an area of particular privacy", and stated that in his view this area was protected not by Article 40.3.1° of the Constitution, but by Article 41 which deals with the family. In so far as the legislation unreasonably restricted the availability of contraceptives for use within marriage, it was "inconsistent with the provisions of Article 41 for being an unjustified invasion of the privacy of husband and wife in their sexual relations with one another": see above para. 3.2.

18 *Kennedy and Arnold v. Ireland* [1987] I.R. 587, [1988] I.L.R.M. 472. It was also successfully pleaded to gain interlocutory relief in respect of the reporting of legal proceedings and publication in the media of information pertaining to private and family life: *X. v. Independent Star Ltd. and others*, High Court, unreported, 19 May 1994 (Costello J.).

19 *Murray v. Ireland* [1985] I.R. 532 (H.C.); [1991] I.L.R.M. 465 (S.C.).

20 *Maguire v. Drury and Others*, High Court, unreported, 8 June 1994.

21 *Ibid.*

22 *Norris v. Attorney General* [1984] I.R. 36.

23 *Murphy v. The Attorney General* [1982] I.R. 241; *Madigan and Gallagher v. The Attorney General* [1986] I.L.R.M. 136.

24 *Desmond v. Glackin (No. 2)* [1993] 3 I.R. 67 (H.C.); and *Probets v. Glackin* [1993] 3 I.R. 134 (H.C.). The right of privacy (as opposed to confidentiality) was not considered, on appeal, by the Supreme Court in these cases.

25 *Kane v. Governor of Mountjoy Prison* [1988] I.R. 757.

Where the claim to protection of one's privacy has been unsuccessful, it is not always clear whether the court was rejecting that the matter before it was one of privacy or whether it viewed other interests as overriding any individual interest in privacy.[27] Moreover, where the claim has been raised by a collective or corporate entity such as a company rather than an individual, the courts have not distinguished between the nature of such claims, and seem indeed to have equated privacy and secrecy or privacy and confidentiality.[28]

3.9 A full analysis of the content, scope and basis of the constitutional right of privacy is beyond the confines of this Paper. Rather of relevance in the context of our study of the threat to privacy posed by the interception of communications and surveillance is the fact that the courts have accepted that Article 40.3.1° affords some protection against such threats; and the few cases in which the courts have considered the existence and the scope of this protection will be examined below.

Privacy And Competing Interests

3.10 Even when a matter is recognised as pertaining to the realm of privacy, the individual interest in privacy will not invariably take priority over all other considerations. In framing the rules to govern any society, certainly any democratic society, account must be taken of any countervailing interests, both those of other individuals and those of society in general, and a balance must be drawn between any competing interests. These other interests to which consideration may properly be given in determining the personal right of privacy under Article 40.3.1° of the Constitution have been variously identified in the case law as:

---

26 *D.P.P. v. Kenny* [1992] 2 I.R. 141 and *Nason v. Cork Corporation*, High Court, unreported, 12 April 1991. See further below paras. 3.20-3.22 on these cases.

27 For example, in *Murphy v. The Attorney General* [1982] I.R. 241, the plaintiffs, a married couple, claimed that a system of tax returns which obliged one spouse to disclose particulars of his or her income to the other was unconstitutional in that it infringed the former's constitutional right to privacy. In the High Court, Hamilton P. held that "the Constitution does not guarantee any such privacy to either the husband or the wife" (at p.266), and that:

> "[t]he common good of ... society requires that revenue be raised for the purposes of that society by taxation and that information be made available for the purposes of determining the amount payable by any individual. The Constitution does not guarantee the right to either spouse not to disclose to his or her spouse the source or amount of his or her income for the purpose of making such returns." (*Ibid.*)

This may mean either that (i) as between spouses, individual income is not a matter of privacy; (ii) for taxation purposes, individual income is not a matter of privacy between spouses; or (iii) while an individual's income is a matter of privacy, for the purpose of tax returns, the interest of society in raising revenue overrides any interest of a spouse in not disclosing to the other his or her income. The Supreme Court did not address the issue of privacy. Cf. *Madigan and Gallagher v. The Attorney General* [1986] I.L.R.M. 136.

28 For example, the applicants in *Desmond v. Glackin (No. 2)* [1993] 3 I.R. 67 and in *Probets v. Glackin* [1993] 3 I.R. 134 claimed that information which they were required by statute to furnish to the Central Bank had been passed on to Mr. Glackin - an inspector appointed by the Minister under s.14 of the Companies Act, 1990 - in breach, *inter alia*, of their constitutional right of privacy. For the distinction between privacy and secrecy, see above p.1, n.3 and for that between privacy and confidentiality, see below paras. 4.35-4.37.

See also, *Attorney General v. Open Door Counselling Ltd.* [1988] I.R. 593, in which one of the plaintiffs, a family planning clinic, sought to rely, *inter alia*, on a constitutional right of privacy.

- the common (or public) good;[29]
- the maintenance of public order;[30]
- the attainment of true social order;[31]
- the protection of public morality;[32]
- the protection of human life (including the life of the unborn);[33]
- the protection of health;[34]
- the implementation of the principles of social policy directed by Article 45;[35]
- the protection of the institution of marriage;[36]
- State security;[37]
- the protection of "those who may readily be subject to undue influence", such as the young or the weak-willed;[38]
- the protection of persons under incapacity of one kind or another;[39]
- the protection of "those who should be deemed to be in need of protection";[40]
- the protection of the family as the natural primary and fundamental unit of society;[41]
- the preservation of decency;[42]
- the preservation of discipline in the armed forces or the security forces;[43]
- the investigation or detection of crime;[44]
- the execution of an extradition warrant;[45]
- the implementation of a term of imprisonment upon conviction of a criminal offence;[46]

---

29 *Per* Walsh J. in *McGee v. Attorney General* [1974] I.R. 284 at 315; Henchy J. in *Norris v. Attorney General* [1984] I.R. 36 at 72, 78 & 79; and Hamilton P. in *Murphy v. Attorney General* [1982] I.R. 241 at 266 and in *Kennedy and Arnold v. Ireland* [1987] I.R. 587 at 592, [1988] I.L.R.M. 472 at 476.

30 *Per* McWilliam J. in *Norris v. Attorney General* [1984] I.R. 36 at 48 and Henchy J. *ibid.* at 72 & 79; and Hamilton P. in *Kennedy and Arnold v. Ireland* [1987] I.R. 587 at 592 & 593.

31 *Per* McWilliam J. in *Norris v. Attorney General* [1984] I.R. 36 at 48.

32 *Per* Griffin J. in *McGee v. Attorney General* [1974] I.R. 284 at 334; McWilliam J. in *Norris v. Attorney General* [1984] I.R. 36 at 48, O'Higgins C.J., *ibid.*, at 64 (Finlay P. and Griffin J. concurring) and Henchy J., *ibid.*, at 72 & 79; and Hamilton P. in *Kennedy and Arnold v. Ireland* [1987] I.R. 587 at 592, [1988] I.L.R.M. 472 at 476.

33 *Per* Walsh J. in *McGee v. Attorney General* [1974] I.R. 284 at 315; McCarthy J. in *Norris v. Attorney General* [1984] I.R. 36 at 103; Hamilton P. in *Murphy v. Attorney General* [1982] I.R. 241 at 266 and in *Open Door Counselling Ltd. and Dublin Well Woman Centre Ltd.* [1988] I.R. 593 at 617.

34 *Per* McWilliam J. in *Norris v. Attorney General* [1984] I.R. 36 at 48, O'Higgins C.J., *ibid.*, at 62, 63 & 65 (Finlay P. and Griffin J. concurring) and Henchy J., *ibid.* at 79.

35 *Per* McWilliam J. in *Norris v. Attorney General* [1984] I.R. 36 at 48.

36 *Per* O'Higgins C.J. in *Norris v. Attorney General* [1984] I.R. 36 at 63 & 65 (Finlay P. and Griffin J. concurring) and Henchy J., *ibid.*, at 79.

37 *Per* Henchy J. in *Norris v. Attorney General* [1984] I.R. 36 at 72. See also McCarthy J. in *Murray v. Ireland and the Attorney General* [1991] I.L.R.M. 465 at 476 (the requirements of prison security).

38 *Per* Henchy J. in *Norris v. Attorney General* [1984] I.R. 36 at 79 and McCarthy J., *ibid.*, at 101.

39 *Per* McCarthy J. in *Norris v. Attorney General* [1984] I.R. 36 at 101.

40 *Per* Henchy J. in *Norris v. Attorney General* [1984] I.R. 36 at 79.

41 *Ibid.*

42 *Per* Henchy J. in *Norris v. Attorney General* [1984] I.R. 36 at 79 and McCarthy J., *ibid.*, at 101.

43 *Per* McCarthy J. in *Norris v. Attorney General* [1984] I.R. 36 at 101.

44 *Per* Griffin J. in *McGee v. Attorney General* [1974] I.R. 284 at 334; McWilliam J. in *Norris v. Attorney General* [1984] I.R. 36 at 45; Finlay C.J. in *Kane v. Governor of Mountjoy Prison* [1988] I.R. 757 at 769 (Henchy and Griffin JJ. concurring) and McCarthy J., *ibid.*, at 770-771 (Hederman J. concurring).

45 *Per* Finlay C.J. in *Kane v. Governor of Mountjoy Prison* [1988] I.R. 757 at 769 (Henchy and Griffin JJ. concurring) and McCarthy J., *ibid.*, at 770-771 (Hederman J. concurring).

46 *Per* Finlay C.J. in *Murray v. Ireland* [1991] I.L.R.M. 465 at 472 (Hamilton P., O'Flaherty and Keane JJ. concurring) and McCarthy J., *ibid.*, at 476 & 477 (Hamilton P., O'Flaherty and Keane JJ. concurring).

- detention for contempt of court;[47]
- detention pursuant to mental treatment procedures;[48]
- the conduct of an official inquiry into possible financial irregularities;[49]
- the determination of tax liability;[50]
- the admission of evidence in a criminal trial;[51]
- the admission of evidence in civil proceedings;[52]
- the constitutional rights of others;[53]
- the right of journalists to communicate and to carry on their profession;[54]
- other and more generalised considerations (than privacy) expressed in or postulated by the Constitution.[55]

3.11 This list, comprising both community and individual interests, should probably not be regarded as exhaustive of the grounds on which an invasion of privacy may be justified. Other cases may throw up other acceptable grounds. The Irish courts do not appear to have given any indication of when a ground advanced will be rejected since the legitimacy of the grounds advanced to date have not been challenged.[56] They have however indicated that, in balancing the individual's interest in privacy with a countervailing interest, all interests do not carry the same weight, that some interests, such as an interest in the preservation of human life, carry a greater weight than others.[57] Nevertheless, while some interests may be regarded as intrinsically of greater value than others, it is doubtful whether all interests can be hierarchically arranged. For example, is privacy in itself of greater value than freedom of expression? Is it of greater value than the public interest in the due administration of justice? Often the answer will depend upon the particular circumstances in which the interests collide and resort must be had to criteria other than the intrinsic worth of each interest in determining which is to prevail.[58] The particular criteria which the

---

47 *Per* McCarthy J. in *Murray v. Ireland* [1991] I.L.R.M. 465 at 477 (Hamilton P, O'Flaherty and Keane JJ. concurring).

48 *Ibid.*

49 *Per* O'Hanlon J. in *Desmond v. Glackin (No. 2)* [1993] 3 I.R. 67 at 97-102 and in *Probets v. Glackin* [1993] 3 I.R. 134 at 139.

50 *Per* Hamilton P. in *Murphy v. Attorney General* [1982] I.R. 241 at 266, and O'Hanlon J. in *Madigan v. Attorney General and others* [1986] I.L.R.M. 136 at 156.

51 *D.P.P. v. Kenny* [1992] 2 I.R. 141 at 144.

52 *Nason v. Cork Corporation*, High Court, unreported, 10 April 1991.

53 *Kennedy v. Ireland* [1987] I.R. 587 at 592, [1988] I.L.R.M. 472 at 476.

54 *X. v. Independent Star Ltd. and others*, High Court, unreported, 19 May 1994, at pp.1 & 4 of the Judgment.

55 *Per* Henchy J. in *Norris v. Attorney General* [1984] I.R. 36 at 68.

56 Cf. also Article 8(2) of the European Convention on Human Rights: see below para. 7.19.

57 See, e.g., *Attorney General (SPUC) v. Open Door Counselling Ltd.* [1988] I.R. 593 at 617, [1987] I.L.R.M. 477 at 500 (H.C.).

58 In dealing with a conflict between the right to one's personality and the freedom of broadcasting stations to provide information, both of which are guaranteed by the Constitution, the German Federal Constitutional Court said in a 1973 case:

> "In solving this conflict it must be remembered that according to the intention of the Constitution both constitutional concerns are essential aspects of the liberal-democratic order of the Constitution with the result that neither can claim precedence in principle."

BVerfGE 35, 202, translated by F.H. Lawson and B.S. Markesinis and reproduced in B.S. Markesinis, *The German Law of Torts*, 3rd ed., Clarendon Press, Oxford, 1994, p.390 at p.394. Privacy and freedom of information are described in the *Consultation Paper on Infringement of Privacy*, published by the Lord Chancellor's Department and the Scottish Office, July 1993, as "values of apparently equal weight": para. 5.57.

courts have used in balancing a privacy interest with the ground or grounds advanced to justify surveillance will be considered below.

Privacy And Surveillance

3.12 Surveillance has came under court scrutiny five times in the context of an alleged invasion of privacy. Two involved allegations that the behaviour of public officials infringed the constitutional right to privacy of the plaintiffs. One of these cases concerned overt garda surveillance of a person whose whereabouts the guards wished to keep known to themselves; and the other concerned the tapping of telephones by post office officials on the instructions of a Government Minister. In the former, the applicant sought his release from custody on the ground that he was being unlawfully detained; in the latter, the plaintiffs sought damages for the invasion of their constitutional rights. In the other three cases, a challenge was made to the admissibility of certain evidence, in one case on the ground that its admission would infringe the constitutional right to privacy of the defendant, in the other two, on the ground that the evidence had been obtained in breach of the constitutional right to privacy of the plaintiff. In only one of the five cases, that dealing with overt garda surveillance, was the privacy issue decided by the Supreme Court. In the other four, the issue was determined by the High Court. Three of the cases involved the use of technology. In the other two, the subject was observed by using the normal human senses, unassisted by technological means.

3.13 **First** case: In the one case decided by the Supreme Court, *Kane v. Governor of Mountjoy Prison*,[59] the Court accepted that overt police surveillance is lawful provided adequate justification exists for it. Kane was arrested under s.30 of the *Offences Against the State Act, 1939*, during a nationwide search for unlawful supplies of arms and ammunition, on suspicion of being a member of the I.R.A. While he was being detained some arms were found in a location near where he had been staying and there was reason to believe that he was associated with these arms. For some time he refused to give his name or address or to answer any questions, and only after being visited by a solicitor did he give his name and state that his address was Belfast, without supplying any more details. Upon release, he was subjected for a period of a little more than five hours by gardaí to surveillance which was variously described by the High Court as "intense",[60] "most thorough"[61] and "open and extremely obvious".[62] After a dramatic car chase, Kane attempted to elude garda surveillance on foot, but was pursued and arrested for causing a breach of the peace and assaulting a member of the gardaí. He applied to the High Court for his release on the ground that he was being unlawfully detained. Egan J. found that he had been lawfully arrested and that the close surveillance to which he had been subjected was justified either by way of attempting to find evidence of his association with

---

59 [1988] I.R. 757. For general comment on the case see R. Humphries, "Constitutional Law - Surveillance and Subversion. A Tangled Judicial Maze", (1989) 11 D.U.L.J. 138-149.

60 At p.761.

61 *Ibid.*

62 At p.763.

the arms which had been discovered or in the expectation of a provisional extradition warrant, the latter being the more likely reason for the surveillance.

3.14 On appeal by Kane, three members of the Supreme Court were of the opinion that:

> "... if overt surveillance of the general type proved in this case were applied to an individual without a basis to justify it, it would be objectionable, and ... would be clearly unlawful. Overt surveillance including a number of gardai on foot closely following a pedestrian, and a number of garda cars, marked as well as unmarked, tailing a driver or passenger in a motor car would, it seems to me, require a specific justification arising from all the circumstances of a particular case and the nature and importance of the particular police duty being discharged.
>
> Such surveillance is capable of gravely affecting the peace of mind and public reputation of any individual and the courts could not ... accept any general application of such a procedure by the police, but should require where it is put into operation and challenged, a specific adequate justification for it."[63]

The issue raised by the applicant's submission that the surveillance infringed his constitutional right of privacy involved:

> "a consideration of all the proven circumstances, background and facts of the case, as well as a consideration of the duty being discharged by the police and the nature of the surveillance which was proved to have occurred."[64]

Given that Kane had been arrested in the course of a countrywide search for arms, believed by the authorities to represent a major danger to the security of the State and that, when released, he was most likely to go into hiding as he had done before and to be assisted in this by the I.R.A., they thought it most unlikely that covert surveillance or even overt surveillance by a very limited number of people following him at a discreet distance would suffice to keep his whereabouts known. Bearing in mind also the nature of the duty which the Garda Síochána were carrying out, they regarded the surveillance as justified. Regarding the nature of the duty which the gardaí were carrying out, they found that the view of the trial judge as to the more likely reason for the surveillance being the expectation of an extradition warrant rather than the search for evidence of association with the arms was "supported by the evidence".[65] This however did not affect the question of justification. The surveillance was justified on either ground. Moreover, they rejected the distinction sought to be drawn by the

---

63 Finlay C.J., at p.767, Griffin and Henchy JJ. concurring.
64 *Ibid.*
65 At p.769.

applicant's counsel between the duty of investigating or detecting crime and the duty of executing an extradition warrant.[66]

3.15 The other two members of the Court regarded the issue as being:

> "whether or not the gardai, who may lawfully "stake-out" a premises which they believe will be burgled, or who may lawfully and overtly or otherwise follow a suspect with a view to investigating or detecting crime may lawfully do the same in the reasonable expectation of the arrival of a valid extradition warrant."[67]

They were concerned about the limitation imposed by overt as opposed to covert surveillance on the freedom of movement of a person, and stated that the issue narrowed further if one concluded, as they did:

> "... that covert surveillance, which by definition, does not impede the freedom of choice of movement, is a lawful invasion of privacy, to whether or not the overt nature of the surveillance can be equally so justified."[68]

In their view, the duty of the guards in investigating or detecting crime was not the same as providing for the execution of an extradition warrant, and whereas surveillance in the former circumstances was generally lawful, in the latter it was ordinarily not. However, given the fact that in the instant case the extradition process had advanced to a stage where it was "reaching finality",[69] in the circumstances the surveillance was not excessive and, therefore, not unlawful.

3.16 The case provides authority for the proposition that the matters properly to be taken into account in determining whether or not overt police surveillance infringes upon the constitutional right of privacy of the person observed are (i) the proven circumstances, background and facts of the case, (ii) the duty being discharged by the police, and (iii) the extent and nature of the surveillance. In addition, a criterion of proportionality is implied both by the view of the majority that less intrusive forms of surveillance would not have sufficed to keep Kane's whereabouts known to the gardaí and by the view of the minority that in the

---

66 As to the latter they stated:

> "The State has a very clear interest in the expeditious and efficient discharge of the obligations reciprocally undertaken between it and other States for the apprehension of fugitive offenders. A member of the Garda Síochána aware of the intended issue and backing of an extradition warrant has a clear duty to take reasonable steps to ascertain where it probably can be speedily executed, when it is obtained."

[1988] I.R. 757 at 769.

67 McCarthy J, at p.770, Hederman J. concurring.

68 *Ibid.* The reference to covert surveillance is *obiter*. If what is meant here is that covert surveillance is a lawful invasion of privacy because it does not impede upon a person's freedom of movement, the statement is surely wrong as a general proposition and needs to be qualified. The majority did not regard the police surveillance as having curtailed Kane's freedom of movement.

69 At p.771.

circumstances the surveillance was not excessive.[70]

3.17 This authority is however subject to an important qualification. The case proceeded on the assumption that a person enjoys a right of privacy even while in a public place,[71] and since the Court found the invasion of Kane's assumed privacy to be justified in the circumstances, it was not necessary for it to decide whether this assumption was valid or not. The case therefore does not provide authority for the view that the scope of the right of privacy extends to conduct in a public place such as a highway or public street. Indeed the case was concerned at least as much, if not more, with the applicant's freedom of movement as with his privacy, and affords no indication of the scope and content of the interests embraced by the right of privacy.

3.18 **Second** case: The constitutionality of the covert interception of communications has not to date been considered by the Supreme Court. It has however been considered by the High Court in proceedings for damages for the unlawful tapping of telephones: *Kennedy and Arnold v. Ireland*.[72] The Court was presented with evidence of the tapping of the home telephones of two journalists under warrant issued by the Minister for Justice. No attempt was made in court to justify the tapping on the grounds of the detection of crime or of the protection of the security of the State or indeed on any other ground. Hamilton P. categorised the right of privacy as "one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State",[73] and stated that the "nature of the right to privacy must be such as to ensure the dignity and freedom of an individual in the type of society envisaged by the Constitution, namely, a sovereign, independent and democratic society."[74] Recognising that there "are many aspects to the right to privacy",[75] he identified the question to be determined in the case before him as being:

> "... whether the right to privacy includes the right to privacy in respect of telephonic conversations and the right to hold such conversations without deliberate, conscious and unjustified interference therewith and intrusion thereon by servants of the State, who listen to such conversations, record them, transcribe them and make the transcriptions thereof available to other persons."[76]

He had no doubt that it does.

---

70 The case also provides authority for the proposition that when a person makes a journey and the person's route and journey are observed by the police but the person is not impeded in any way from making the journey, that person is not in law being detained: [1988] I.R. 757 at 768-769.

71 With respect to the applicant's submission that his privacy had been infringed, Finlay C.J. stated, at p.769, Griffin and Henchy JJ. concurring:

> "I would be prepared to assume, without deciding, for the purpose of dealing with this submission that a right of privacy may exist in an individual, even while travelling in the public streets and roads."

72 [1987] I.R. 587, [1988] I.L.R.M. 472.

73 [1987] I.R. 587 at 592, [1988] I.L.R.M. 472 at 476.

74 [1987] I.R. 587 at 593, [1988] I.L.R.M. 472 at 477.

75 [1987] I.R. 587 at 592, [1988] I.L.R.M. 472 at 476.

76 [1987] I.R. 587 at 592, [1988] I.L.R.M. 472 at 476-477.

> "The dignity and freedom of an individual in a democratic society cannot be ensured if his communications of a private nature, be they written or telephonic, are deliberately, consciously and unjustifiably intruded upon and interfered with."[77]

The State through its executive organ had deliberately and consciously interfered with the telephonic communications of the plaintiffs and had offered no justification for the interference. There had therefore been an infringement of the constitutional right to privacy of each plaintiff.[78]

3.19 This decision, while establishing that a person enjoys a constitutional right of privacy in respect of telephone conversations and that the right is breached by deliberate, conscious and unjustifiable interference with such communications, is unfortunately unclear as to whether the right covers all telephone conversations or merely those "of a private nature". While it is likely that the former was intended since no distinction was made in the decision between telephone conversations on the basis of their content or nature but the tapped conversations were treated as a whole, the issue was not specifically addressed.[79] Moreover, while accidental interference with communications was recognised as not in general constituting an infringement of a person's right of privacy, it is questionable whether all continued interference should be regarded as immune from constitutional challenge merely because the interference was accidental in origin. The decision does however show that enjoyment of the right is not dependent upon citizenship. One of the plaintiffs was not an Irish citizen, and the Court held that he was "entitled to the same personal rights as if he were".[80] It also shows that the right of privacy was infringed not merely by the tapping of the telephones, but also by the recording, the transcription and the making available of the transcriptions to other persons. The decision further provides a clear guide as to the grounds on which the interception of telephone conversations may be justified, namely, the protection of the constitutional rights of other persons, the common good and public order and morality.[81] Since no

---

77 [1987] I.R. 587 at 593, [1988] I.L.R.M. 472 at 477.

78 The Court held that the plaintiffs were entitled to substantial damages, and awarded £20,000 damages to each of the journalists, and £10,000 to the third plaintiff, the wife of one of the journalists. It was of the opinion that, in the circumstances of the case, it was irrelevant whether they be described as "aggravated" or "exemplary" damages. It further held that the plaintiffs were not entitled to punitive damages:

> "… because of the action of the then Minister for Justice, in the course of the statement made by him on 20th January, 1983…in openly acknowledging that both the telephones referred to in this case were in fact "tapped", that the system of safeguards which successive Ministers for Justice have publicly declared in Dáil Éireann to be an integral part of the system was either disregarded or, what amounted to the same thing, was operated in such a way as to be rendered meaningless and that the facts showed that there was no justification for the tapping of either of the two telephones and that what occurred went beyond what could be explained as just an error of judgment. In doing so he, though belatedly, vindicated the good names of the plaintiffs herein, in particular the first and second plaintiffs." ([1987] I.R. 587 at 594, [1988] I.L.R.M. 472 at 478.)

The Court also directed the defendants to return to the plaintiffs all transcripts of the conversations recorded on their respective telephone lines.

79 The plaintiffs had pleaded that the tapping failed to respect their privacy both in the exercise of their profession as political journalists and in the living of their private lives.

80 [1987] I.R. 587 at 593, [1988] I.L.R.M. 472 at 477.

81 [1987] I.R. 587 at 592, [1988] I.L.R.M. 472 at 476.

justification was offered in the case for the interference with the plaintiffs' privacy, little indication was given of how these other interests were to be balanced in a specific case against the individual's interest in privacy other than that the right of privacy might legitimately be restricted when this was *required* by these other interests and that the balancing should be made by reference to the sovereign, independent, democratic and Christian nature of the State.

3.20 The **third** case concerned observation by a medical practitioner of a person who had been arrested under road traffic legislation and brought to a garda station for the purpose of taking from him a sample of blood or urine. He consented to the taking of a blood sample, but at his subsequent trial for drunken driving it was submitted that the doctor who took the sample could not give evidence either of his observation of the accused or as to his opinion on the fitness of the accused to drive a mechanically propelled vehicle. It was argued that the admission of such evidence would breach the accused's constitutional right to privacy. Appropriate questions as to the existence and scope of the alleged right were referred by the trial court by way of case stated to the High Court for determination.[82] The High Court held that the accused did have a right to privacy in the circumstances, but that it was "perfectly permissible for the doctor to give evidence of his observation of the defendant incidental to the taking of [the blood] sample".[83] The right to privacy was "not breached by observation of the accused by persons who are lawfully required to deal with him while in custody."[84] As the Court added, "[w]hether it would be breached by observation of the accused by persons in any other category and, if so, in what circumstances"[85] did not arise for decision in the particular case.

3.21 In the **fourth** case, the High Court held that the admission of photographic evidence on behalf of the defendant, a local authority, in a personal injuries claim would not breach the plaintiff's constitutional right to privacy.[86] The photographs had been taken by a private investigator on behalf of the local authority. Some of them were of the plaintiff in the street, but others were of her in the living room of her own home. The Court took the view that, provided no trespass was committed in the taking of the photographs, they were:

> "... simply a record, a photographic record of what anyone walking down the street presumably could observe and that is no violation of the right to privacy or, it is a violation of the right of privacy no different from the covert surveillance of the same person in the street because if people elect to walk to and fro in their drawing room, without the curtains drawn, then, of course, they are visible from the street and anybody who would pass and glance in their direction is not in any sensible way violating their privacy.

---

82 *D.P.P. v. Kenny* [1992] 2 I.R. 141.
83 *Ibid.*
84 *Ibid.*
85 *Ibid.*
86 *Nason v. Cork Corporation*, unreported, 12 April 1991 (Keane J.).

> But if somebody covertly photographs them, whilst that is obviously a distasteful operation, viewed from the legal point of view, it is no different than if they are equally covertly photographed while out in the public gaze because essentially in most cases they are in the public gaze ...."[87]

3.22 This passage, read on its own, may be interpreted to mean that what is visible to members of the public is not to be regarded as falling within the realm of privacy. Only if a person seeks to keep their behaviour from the public gaze as, in this case, by drawing the curtains, is it to be regarded as a matter of privacy. Other passages in the Court's Judgment suggest however that any interest of the plaintiff in the exclusion of such evidence was outweighed by the interest of the defendants in receiving a fair trial:

> "... every litigant who invokes the aid of the court against another party, of necessity, subjects himself or herself to certain violations of their right to privacy ... [T]here was - in a sense - a far more significant violation of the plaintiff's privacy when she had to give intimate details concerning herself in her evidence, which naturally were not objected to ... [I]t was not suggested that they were not relevant to the inquiry that the court has to conduct, no matter how embarrassing and unpleasant, as undoubtedly they were for the plaintiff.
>
> Now, similarly here we have, I would have thought, from that point of view, a far less intrusive invasion of the plaintiff's privacy ... to hold that the court is not entitled to evidence which might, in a particular case, indicate that the plaintiff's evidence, that he or she has been incapacitated or disabled to a particular extent, is not borne out by the manner in which they are conducting their daily lives, if it meant that a court was without that evidence, that could result in a significant injustice to the other parties ... the right of privacy is ... most certainly not absolute because the plaintiff is to an extent, in seeking relief from the court in personal injuries actions such as this, where there were medical examinations by doctors not of their own choice, there is a necessary invasion of their privacy as a necessary consequence of the litigation and to exclude that could be to do injustice to another party and to prevent the court from having evidence it should have."[88]

3.23 The **fifth** case[89] concerned the use of a tape recording in disciplinary proceedings against a local authority workman. The recording showed the workman being abusive to a foreman and had been made secretly, in view of the workman's earlier denial of such conduct. The workman sought a series of declarations from the High Court, including a declaration that in deciding to

---

87 At p.6 of the transcript of the proceedings of 10 April 1991.

88 At pp.4-5 of the transcript of the proceedings of 10 April 1991.

89 *Devoy v. The Right Honourable Lord Mayor, Aldermen & Burgesses of Dublin, Beattie, Heavey & Brooks*, The High Court, unreported, 18 October 1995.

suspend him from work for two weeks without pay pursuant to the disciplinary hearing the local authority had relied on evidence obtained in breach of his constitutional right to privacy. The High Court disposed quickly of this argument. The playing of the recording for thirty to fifty seconds did not vitiate the proceedings. It could be compared to the production of photographs by a defendant showing a plaintiff with an allegedly bad back lifting concrete blocks.

3.24 The brief treatment of the privacy issue in this case throws little light on the content, scope and relative weight to be afforded privacy. Although the analogy with the production of photographic evidence suggests that the administration of justice would take precedence in such circumstances over any privacy interest, the Court did not address the logically prior questions of whether the recording infringed any privacy interest of the plaintiff, and if so, what interest.

Conclusion

3.25 It is now established by case law that the personal rights of the citizen guaranteed by Article 40.3.1° of the Constitution include a right of privacy. The scope and content of this right are however as yet ill-defined. The subsection provides some protection against surveillance and the interception of communications, though the individual interest in privacy must often cede place to other private and public interests such as the public interest in the detection of crime and the interest of a litigant, whether public or private, in a fair trial. As *Kane*[90] illustrates, however, there may be no acceptable countervailing interest in a specific case.

3.26 In resolving a conflict between a person's interest in privacy and other interests, there is authority to the effect that some interests carry greater weight than others, notably that the right to life of the unborn takes priority over any interest in privacy. There is also Supreme Court authority for resort to a criterion of proportionality in balancing the interests concerned. More generally, there is High Court authority that the nature of the right to privacy should be determined by reference to the type of society envisaged by the Constitution, namely, a sovereign, independent and democratic society.

3.27 The case law does therefore provide some guidance as to how the courts will approach the determination of an allegation that particular surveillance has breached an individual's constitutional right to privacy. This guidance is however, on the present state of the case law, of a rather general kind. There have been few cases; and many types of surveillance have not as yet given rise to complaints of an invasion of the constitutional right to privacy. Thus, the courts have had little occasion to examine the constitutionality of the use of various listening and optical devices. In and of itself the Constitution therefore affords only patchy and uncertain protection for privacy in respect of surveillance. The Constitution

---

90 *Kane v. Governor of Mountjoy Prison* [1988] I.R. 757.

does not however stand alone. The protection it affords is supplemented by a range of civil remedies and criminal sanctions, of which account must also be taken in determining the scope of the legal protection afforded privacy against invasive surveillance and in assessing the adequacy of this protection.

CHAPTER 4: CIVIL LIABILITY

Introduction

4.1 Unlike the situation in several other jurisdictions,[1] there is in Ireland no cause of action for breach of privacy as such either in equity or under statute. Nor have the Irish courts explicitly recognised a right to privacy at common law. Whether or not such a right exists may perhaps not yet have been definitively decided since an argument for the existence of such a right was recently put to the High Court and was not rejected.[2] Mention should also be made in this context of an earlier High Court decision in which it was held that an insured person had a natural right, flowing from the rules of natural justice and separate from the Constitution, to confidentiality in respect of personal information supplied by him to insurers and that there was a corresponding obligation on the insurers not to divulge this information.[3] These cases however concerned information privacy,[4] and their value as precedent for recognition of a common law right to privacy in respect of one's communications and freedom from surveillance is consequently limited.

4.2 While the existence of a general right to privacy apart from the Constitution is therefore uncertain, various aspects of privacy are protected by a range of civil actions. The remedies available include an injunction to restrain a prospective invasion of privacy, damages for actual invasion, and delivery up

---

1 See below paras. 9.2-9.13. It was recently affirmed by the English Court of Appeal that there is no general right to privacy in English law, and that accordingly there is no right of action for breach of a person's privacy: see *Kaye v. Robertson and Another* [1991] F.S.R. 62 at 66 (*per* Lord Justice Glidewell), 70 (*per* Lord Justice Bingham) & 71 (*per* Lord Justice Leggatt, contrasting the position in England with that in the U.S.A.). See also the earlier case, *Malone v. Metropolitan Police Commissioner* [1979] 1 Ch. 344 at 372-375.

2 Indeed, as regards the situation before it, the Court took the view that the protection afforded by the common law and by the Constitution are probably co-extensive: *Desmond and Dedeir v. Glackin and others*, unreported, 25 February 1992 (O'Hanlon J.).

3 *Murphy v. P.M.P.A.* [1978] I.L.R.M. 25 (Doyle J.).

4 On this category of privacy interests, see above para. 1.6.

or destruction of relevant material. In general, all these actions and remedies apply to invasion of privacy by surveillance as they do to invasion by other means, but the fact that surveillance was used may be relevant to the scope of the protection afforded.

4.3 Some of the actions afford remedies in respect of the surveillance activity itself, others in respect of the use of information obtained by means of surveillance. Among the former are the actions in tort for trespass to land, private nuisance, trespass to the person and trespass to goods. Among the latter are the actions in tort for defamation, malicious falsehood and breach of statutory duty and in equity (and probably tort) for breach of confidence. In addition, an action for breach of contract or copyright may be available.

Torts

(i) Trespass to land[5]

4.4 Where surveillance involves physical intrusion by the observer upon another person's land, the common law tort of trespass to land may afford a remedy in respect of the invasion of privacy concerned. No damage or loss as a result of the intrusion need be shown; and anyone in possession of the land may sue.

4.5 The interest protected by this tort is of course not privacy as such, but an interest in property - in the possession and use of property with the ancillary right to exclude possession and use by others. In the context of freedom from surveillance, it may afford a remedy against the overenthusiastic press photographer who trespasses on a person's land to take photographs or against the private investigator who enters a person's property to instal a bugging device. Leading commentators on the Irish law of torts have noted the potential of this tort to afford protection to an individual's privacy interests in such circumstances. In their view, it is open to the courts to find that "a secret purpose on the part of the entrant unknown to the person who has invited him onto the property vitiates permission to be there"[6] and that entry therefore constitutes a trespass. Any protection afforded by this tort would not extend however to surveillance of persons and property on the land where the surveillance activities are conducted outside the boundaries of the land. Thus, if the press photographer was taking the pictures from a public highway or the private investigator, using a sophisticated listening device, was listening in to conversations on the property while sitting in a van parked some distance away, an action for trespass to land would not be available to the owner or occupier of the land.

---

5 On this tort in general see, e.g., J.G. Fleming, *The Law of Torts*, 8th ed., The Law Book Company Ltd., 1992, pp.39-48; R.F.V. Heuston and R.A. Buckley, *Salmond and Heuston on the Law of Torts*, 12th ed., Sweet & Maxwell, London, 1992, ch. 4; B.S. Markesinis and S.F. Deakin, *Tort Law*, 3rd ed., Clarendon Press, Oxford, 1994, pp.411-418; W.V.H. Rogers, *Winfield& Jolowicz on Tort.*, 14th ed., Sweet & Maxwell, London, 1994, ch. 13; and, with specific reference to Ireland, B.M.E. McMahon and W. Binchy, *Irish Law of Torts*, 2nd ed., Butterworth (Ireland), Dublin, 1990, ch. 23.

6 B.M.E. McMahon and W. Binchy, *op. cit.*, p.685.

4.6 An English case of the turn of the century illustrates the scope and some of the limitations of this tort as a vehicle of protection against unwelcome surveillance. In *Hickman v. Maisey*,[7] the plaintiff had entered into an agreement with a trainer of race-horses whereby the latter could use some of his land for the training and trial of race-horses. The land was crossed by a highway, and the defendant was in the habit of walking backwards and forwards along a fifteen-yard section of the highway observing the horse-trials through binoculars and taking notes. His purpose in so doing was to use the information gained in a publication of which he was a proprietor and which gave accounts of the performance of race-horses in training. When the trainer objected to the defendant's activity, the plaintiff gave the defendant notice that he should desist from using the highway for the purpose of observing the horses. When the defendant refused, the plaintiff brought an action against him for trespass to land, claiming damages and an injunction to restrain him from using the highway for this purpose. The Court of Appeal upheld the judgment of the lower court in favour of the plaintiff. The principal right of the public in relation to the use of a highway is to pass and repass along it. By extension, the public may also make such ordinary and reasonable use of the highway as is incidental to passage. All three judges had no difficulty in finding that the use made of the highway by the defendant - not for passage as such but "for the purpose of carrying on his business as a racing tout"[8] - was outside the ordinary and reasonable user of a highway for passage.[9] One judge also mentioned that it was crucial to the plaintiff's claim that the soil of the highway belonged to him, and that "if what the defendant did had been done by him on soil which was not vested in the plaintiff, the latter would have had no legal right to complain."[10]

4.7 Moreover, that trespass may not be successfully invoked to stop the broadcasting of material which has been obtained by the covert use of recording equipment was indicated in a recent case before the English Court of Appeal.[11] In making a programme about the police investigation of an alleged paedophile, the makers of the programme, with the agreement of the police, brought a concealed camera and sound-recording equipment into the home of the man's former wife. The issue of trespass was not before the court. All the material obtained by trespass was in fact excluded from the broadcast programme, but without admission of any legal liability to do so by the television company concerned. In the course of his decision, one judge stated that the company was "entitled to publish the programme in full, and...there was no legal bar to prevent them from including pictures of the place of arrest",[12] that is, the house of the former wife. Another said that although he was glad that the television company

---

7 [1900] 1 Q.B. 752.

8 *Per* A.L. Smith L.J., at p.756.

9 In *Hubbard and Others v. Pitt and Others*, Forbes J. defined the right of the public to use a highway as "a right to use it reasonably for passage and repassage and for any other purpose reasonably incidental thereto": [1976] 1 Q.B. 142 at 150.

10 Romer L.J., at p.759.

11 *R v. Central Independent Television Plc.* [1994] 3 W.L.R. 20. See the comment on this case by J. Gardiner, Another step towards a right of privacy?", (1995) 145 *New Law Journal* 225.

12 Neill L.J., at p.29.

had excluded the material, "it was not obliged to do so."[13]

4.8 The question whether intrusion by aircraft into the air space above land may constitute a trespass was considered in another English case, *Bernstein of Leigh (Baron) v. Skyviews & General Ltd.*[14] The defendants in this case ran a business taking aerial photographs of properties and then offering them for sale to the owners of the properties. Lord Bernstein took exception to the taking of an aerial photograph of his country house and sought damages claiming, *inter alia*, that by entering the air space above his property in order to take aerial photographs the defendants were guilty of trespass. After reviewing relevant case law, the Court concluded that it could find no support therein for the view that a landowner's rights in the air space above his or her property extend to an unlimited height. Indeed it described this view as "a fanciful notion leading to the absurdity of a trespass at common law being committed by a satellite every time it passes over a suburban garden."[15] It then turned to the academic literature which unanimously rejected such a view and, accepting it as correct, identified the problem in a case such as the one before it as being:

> "... to balance the rights of an owner to enjoy the use of his land against the rights of the general public to take advantage of all that science now offers in the use of air space."[16]

This balance was best struck at the present day:

> "... by restricting the rights of an owner in the air space above his land to such height as is necessary for the ordinary use and enjoyment of his land and the structures upon it, and declaring that above that height he has no greater rights in the air space than any other member of the public."[17]

The aircraft in question had flown many hundreds of feet above the ground, and it was not suggested that it had caused any interference with any use to which the plaintiff put or might wish to put his land. There was therefore no trespass. It would thus appear that in general flying above a person's land for the purpose of aerial photography does not constitute a trespass; but the situation may be different if a low-flying aircraft were to disturb the person's peaceful enjoyment or use of the land.

---

13 Hoffmann L.J., at p.32. See also the approval of Hoffmann L.J.'s general approach to balancing freedom of speech against other interests by O'Hanlon J. in *Maguire v. Drury and Others*, High Court, unreported, 8 June 1994, at pp.8-9 of the Judgment.

14 [1978] 1 Q.B. 479.

15 At p.487.

16 At p.488.

17 *Ibid.*

(ii) **Private nuisance**[18]

4.9 According to a former Chief Justice of Ireland:

> "The term nuisance contemplates an act or omission which amounts to an unreasonable interference with, disturbance of, or annoyance to another person in the exercise of his rights. If the rights so interfered with belong to the person as a member of the public, the act or omission is a public nuisance. If these rights relate to the ownership or occupation of land, or of some easement, profit, or other right enjoyed in connection with land, then the acts or omissions amount to a private nuisance."[19]

4.10 As in the case of trespass to land, then, the tort of private nuisance is concerned with protection of the use and enjoyment of land. Unlike trespass to land, however, a private nuisance is not usually actionable *per se*. Actual damage must be shown; and the damage may consist of either (a) physical injury to land, (b) a substantial interference with the enjoyment of land, or (c) an interference with servitudes.[20]

4.11 In so far as surveillance activity may come within the scope of this tort, any damage is most likely to fall under the second of these headings - a substantial interference with the enjoyment of land. Thus, for example, the tort may catch press photographers who gather at the front gate of a house and seriously obstruct the occupant's ingress and egress from the property. Watching and besetting premises have been held by an English court to be capable of constituting a private nuisance.[21] As we have seen,[22] aerial photography has also come under scrutiny in the English courts. In the *Bernstein* case, it was stated *obiter* that:

> "... no court would regard the taking of a single photograph as an actionable nuisance. But if the circumstances were such that a plaintiff was subjected to the harassment of constant surveillance of his house from the air, accompanied by the photographing of his every activity, I am far from saying that the court would not regard such a monstrous invasion of his privacy as an actionable nuisance for which they would give relief."[23]

4.12 The tort clearly requires a substantial degree of interference with a

---

18 On this tort in general see, e.g., F.G. Fleming, *op. cit.*, pp.416-426; R.F.V. Heuston and R.A. Buckley, *op. cit.*, pp.57-85; B.S. Markesinis and S.F. Deakin, *op. cit.*, pp.418-448; B.M.E. McMahon and W. Binchy, *op. cit.*, pp.454-479; and W.V.H. Rogers, *op. cit.*, pp.404-433.

19 O'Higgins C.J. in *Connolly v. South of Ireland Asphalt Co.* [1977] I.R. 99 at 103.

20 B.M.E. McMahon and W. Binchy, *op. cit.*, p.454.

21 Court of Appeal in *Hubbard and Others v. Pitt and Others* [1976] 1 Q.B. 142 at 175-177, 179-183 & 188-189. Citing this case, the British Home Office Committee on Privacy and Related Matters thought that the tort of nuisance might provide a remedy against harassment by identifiable journalists pestering for information but not necessarily a crowd of reporters and photographers on the pavement. No action may be brought unless the individuals concerned can be identified. See the *Report* of the Committee, Cm 1102, 1990, para. 6.15.

22 See above para. 4.8.

23 *Bernstein of Leigh (Baron) v. Skyviews & General Ltd.* [1978] 1 Q.B. 479 at 489.

person's use or enjoyment of land; and while Irish commentators have expressed the view that it has "considerable potential in relation to the protection of privacy",[24] other commentators have been less optimistic, seeing it as providing little protection "against the privacy of one's home being violated by curious onlookers",[25] and pointing to case law which shows that it provides "no redress against opening new windows which command a view over neighbouring premises."[26]

(iii) Trespass to the person[27]

4.13 In the course of surveillance a person may commit the tort of assault, battery or other trespass to the person. Thus, it has been held in an English case that the taking of photographs with a flashbulb may in certain circumstances constitute a battery.[28] "The essence of trespass is that wrongful conduct should cause a direct injury to the plaintiff."[29] If the plaintiff proves direct injury, then to escape liability, the defendant must show that she or he did not act either intentionally or negligently.

4.14 Torts of trespass to the person afford remedies in respect of the infringement of personal privacy.[30] In most cases of surveillance, any trespass to the person will be merely incidental to the conduct of the surveillance. One such form of trespass, as yet undeveloped in Ireland, does however appear to apply to conduct which is more integral to the surveillance itself. This is the tort of the infliction of emotional or mental suffering.

4.15 A person who intentionally or recklessly or, perhaps, negligently causes emotional suffering to another may thereby commit a tort. Most of the cases concern the causing of shock, fear or other psychological harm to another. The scope of the tort is uncertain, as is the relationship between it and a claim for damages for emotional distress resulting from other distinct torts. It has been most developed to date in the United States of America, where the emotional distress caused must be substantial and the conduct leading to the suffering 'extreme and outrageous'.[31]

4.16 Much surveillance occurs without the knowledge or consent of the subject of surveillance, and as long as it remains unknown to the subject, it is unlikely to inflict on that person emotional suffering. Where, however, surveillance is overt and known to the subject, it may cause that person distress.

---

24 B.M.E. McMahon and W. Binchy, *op. cit.*, p.686. It has been held in other common law jurisdictions that harassment by telephone may constitute a nuisance: see, e.g., *Stoakes v. Brydges* [1958] A.L.J. 205; *Motherwell v. Motherwell* [1976] 73 D.L.R. (3d) 62; and *Khorasandjian v. Bush* (1993) 143 *New Law Journal* 329.

25 J.G. Fleming, *op. cit.*, p.603.

26 *Ibid.*

27 On this category of tort in general see, e.g., F.G. Fleming, *op. cit.*, pp.23-26 & 30-33; R.F.V. Heuston and R.A. Buckley, *op. cit.*, ch. 7; B.S. Markesinis and S.F. Deaton, *op. cit.*, pp.353-363; B.M.E. McMahon and W. Binchy, *op. cit.*, pp.399-409; and W.V.H. Rogers, *op. cit.*, ch. 4.

28 *Kaye v. Robertson and Another* [1991] F.S.R. 62 at 68 (C.A.).

29 B.M.E. McMahon and W. Binchy, *op. cit.*, p.399.

30 On this category of privacy see above para. 1.6.

31 *Restatement of the Law of Torts*, 2nd ed., 1965, §.46.

Where the distress is severe and the surveillance activity is especially offensive, the conduct may fall within the scope of this tort. The tort would therefore seem to have the potential to afford some protection in the most egregious cases of overt surveillance; and, in principle, there would seem to be no good reason why it should not also afford protection where the distress is caused by the use or disclosure of information obtained by surveillance, whether covert or overt, if use or disclosure is especially reprehensible in the circumstances. It does not however appear so far to have been successfully pleaded in any common law jurisdiction in relation to surveillance or to the disclosure or other use of information obtained by means of surveillance.

(iv) Trespass to goods[32]

4.17 As with trespass to the person, in conducting surveillance a person may incidentally commit a trespass to goods. The authors of the leading Irish textbook on torts, while observing that the law on this topic lacks clarity and consistency, define this form of trespass as wrongfully and directly interfering with the possession of chattels.[33] It would seem that it is actionable *per se* and that no actual damage to property need be shown, though there is judicial authority in other jurisdictions to the contrary.[34] This tort is clearly concerned with the protection of property and provides only incidental protection in cases of invasion of privacy.

4.18 There are however two types of surveillance in which trespass will be integral to the surveillance itself. One is telephone tapping. The process of tapping involves breaking into a telephone line or wire and attaching a device thereto. Where the line belongs to the person who is the subject of the tap, this tort may afford that person a remedy.[35] The drawback from a privacy perspective is that, in many cases, the tapped line will belong to a telephone company or to a person other than the one who wishes to complain of the invasion of their privacy, and in such cases, this tort is not available to the aggrieved individual. The other type of surveillance is bugging where a listening device is placed in a telephone receiver or other object which is in the possession of the person whose conversations are being monitored. Again, an action for trespass will only be available to the latter and not to other persons whose conversations have been eavesdropped.

(v) Defamation[36]

4.19 An invasion of privacy comprising the disclosure of personal information

---

32 On this tort in general see, e.g., F.G. Fleming, *op. cit.*, pp.52-54; R.F.V. Heuston and R.A. Buckley, *op. cit.*, pp.97-100; B.S. Markesinis and S.F. Deaton, *op. cit.*, pp.403-406; B.M.E. McMahon and W. Binchy, *op. cit.*, ch. 28; and W.V.H. Rogers, *op. cit.*, pp.487-489.

33 B.M.E. McMahon and W. Binchy, *op. cit.*, p.522.

34 See, e.g., the New Zealand case, *Everitt v. Martin* [1953] N.Z.L.R. 298.

35 The tort is founded on possession, not ownership.

36 On this tort in general see, e.g., F.G. Fleming, *op. cit.*, ch. 25; R.F.V. Heuston and R.A. Buckley, *op. cit.*, ch. 8; B.S. Markesinis and S.F. Deaton, *op. cit.*, pp.565-605; B.M.E. McMahon and W. Binchy, *op. cit.*, ch. 34; and W.V.H. Rogers, *op. cit.*, ch. 12.

usually involves the revelation of information which is true, and the truth of a statement affords a defence in an action for defamation. Nonetheless, as we remarked in our Consultation Paper on the Civil Law of Defamation:

> "There is an overlap between the law on privacy and the law on defamation. If defamation seeks to protect reputation, and privacy law seeks to protect matters which are personal to the individual and should not be regulated or revealed without his or her consent, it is clear that some invasions of privacy will also constitute an attack on reputation."[37]

4.20 With specific regard to surveillance activities, the tort of libel may afford protection in cases where personal information or a photograph acquired by surveillance are published without the consent of the subject in doctored form or alongside other information in such a way that the reputation of the person concerned is damaged. That a defamatory innuendo may be drawn from the circumstances of a publication rather than from the published words or published picture as such is illustrated by the English House of Lords decision, *Tolley v. J.S. Fry and Sons Ltd.*[38] The plaintiff in this case was a well-known amateur golfer, and the defendants, a firm of chocolate manufacturers, included a caricature of the plaintiff together with a caddie in an advertisement for their chocolates. The plaintiff was depicted in golfing costume as just having completed a drive and had a packet of the defendant's chocolate protruding from his pocket. The caddie was holding up packets of the defendants' chocolate. Below the caricature was the following limerick:

> "The caddie to Tolley said, Oh, Sir,
> Good shot, Sir! That ball, see it go, Sir,
> My word how it flies,
> Like a cartet of Frys,
> They're handy, they're good, and priced low, Sir'."

The caricature and the limerick were surrounded with descriptions of the merits of the defendants' chocolates. This advertisement was published without the knowledge or consent of the plaintiff who brought an action claiming damages for libel. He alleged that the advertisement would be understood to mean that he had agreed or permitted his likeness to be exhibited in this way for reward or notoriety and that he had thereby prostituted his reputation as an amateur golfer.

---

37 *Consultation Paper on the Civil Law of Defamation*, March 1991, para. 539. We also identified as an essential difference between defamation law and privacy law that the former looks to the quality of the statement (its truth, its negative effect) whereas the latter looks to the content of the statement (whether it concerns a person's private life: *Ibid.* See Part I of that Consultation Paper for a review of the civil law of defamation in Ireland; and for a further distinction between the law of defamation and that relating to privacy, S.D. Warren and L.D. Brandeis, "The Right to Privacy", (1890) 4 *Harvard Law Review* 193 at 197. That there is a degree of overlap between intrusions into individual privacy and defamation was also recognised by the British Home Office Committee on Privacy and Related Matters, *op. cit.*, para. 7.1; and by the Law Reform Commission of New South Wales in its *Report on Defamation*, Report 75, 1995, paras. 1.22-24 & 2.32-36.

Some international human rights instruments treat privacy and reputation together in that, although there is separate mention of each, they are protected by the same provision: see. e.g. Art. 12 of the Universal Declaration of Human Rights and Art. 17 of the International Covenant on Civil and Political Rights.

38 [1931] A.C. 333. See also *Kaye v. Robertson and Another* [1991] F.S.R. 62 at 66-67.

Uncontested evidence was called on the plaintiff's behalf to show that if the advertisement had been issued with his consent it would have seriously injured his position in golf clubs and his status as an amateur player; and the Court held that an inference of consent could be drawn by the ordinary man or woman from the facts of the publication. The advertisement was therefore capable of being regarded as defamatory of the plaintiff. By analogy with this case, if a photograph were to be taken of a person and used without that person's consent for advertising purposes, or perhaps for any purpose, in some circumstances such publication might be defamatory of the person.

4.21 Indeed the photograph need not be of the plaintiff. The crucial question is whether or not publication thereof is defamatory of the plaintiff. A defamatory inference may be drawn from a publication even though the plaintiff is neither depicted nor described therein. In the English case of *Cassidy v. Daily Mirror Newspapers Ltd.*,[39] a woman successfully sued a newspaper for libel arising from the publication of a photograph of her husband together with another woman. The photograph was accompanied by words stating that the persons in the photograph had announced their engagement. The Court held that the publication was capable of conveying a meaning defamatory of the plaintiff. Readers might understand from it that she was not married to the man in the photograph and was living with him as his mistress, thereby casting an aspersion on her moral character.

(vi) Malicious falsehood[40]

4.22 Publication of personal information may in certain circumstances constitute the tort of malicious or injurious falsehood.[41] The essentials of this tort are that the defendant has maliciously published about the plaintiff words which are false, and that special damage has followed as the direct and natural result of their publication.[42] The damage must be of a monetary character, and the requirement that special damage must be shown has been modified by the *Defamation Act, 1961*.[43] Malice will be inferred if it be proved that the words were calculated to produce damage and that the defendant knew when she or he

---

39 [1929] 2 K.B. 331.

40 On this tort in general see, e.g., F.G. Fleming, *op. cit.*, pp.709-714; R.F.V. Heuston and R.A. Buckley, *op. cit.*, pp.392-395 & 399-401; B.M.E. McMahon and W. Binchy, *op. cit.*, pp.673-675; and W.V.H. Rogers, *op. cit.*, pp.306-311: and for the distinction between this tort and defamation, *Joyce v. Sengupta* [1993] 1 W.L.R.337 at 341 (*per* Sir Donald Nicholls V.-C.); M. McDonald, *Irish Law of Defamation*, Round Hall Press, Dublin, 1987, pp.23-26; and B.S. Markesinis and S.F. Deaton. *op. cit.*, p.637.

41 On a preference for the latter term see B.M.E. McMahon and W. Binchy, *op. cit.*, p.673, n.50.

42 *Per* Lord Justice Glidewell in *Kaye v. Robertson and Another* [1991] F.S.R. 62 at 67.

43 Section 20(1) of the Act provides:

> "In an action for slander of title, slander of goods or other malicious falsehood, it shall not be necessary to allege or prove special damage -
>
> (a) if the words upon which the action is founded are calculated to cause pecuniary damage to the plaintiff and are published in writing or other permanent form; or
>
> (b) if the said words are calculated to cause pecuniary damage to the plaintiff in respect of any office, profession, calling, trade or business held or carried on by him at the time of the publication."

published the words that they were false or was reckless as to whether they were false or not.[44] Irish commentators have described the essence of the tort as being "that the falsehood deceives *others* about the plaintiff so as to cause loss to the plaintiff."[45]

4.23 The ingredients of this tort were found to be present by the English Court of Appeal in the case of *Kaye v. Robertson and Another*.[46] The plaintiff, a well-known actor, who had suffered severe head injuries, successfully sought an interlocutory injunction to prevent the defendants from publishing in "The Sunday Sport" an article based on an interview with him. The journalists who conducted the interview had gained access to the plaintiff in his hospital room, ignoring notices on the doors of the ward and of his private room asking visitors to see a member of the hospital staff before visiting. A number of photographs of the plaintiff were also taken at the time, and it was intended that one or more of these would be published with the article. The article clearly implied that the plaintiff had agreed to be interviewed and to be photographed. However, the medical evidence showed that the actor was in no fit condition to be interviewed or to give any informed consent to the interview or the taking of the photographs; and because the defendants were aware of this, any subsequent publication of the article would be malicious. Also, damage resulted from the undermining of the plaintiff's right to sell the story of his accident and of his recovery when he was fit enough to do so. If the defendants were allowed to publish the proposed article, the monetary value to the plaintiff of the later publication of his story would be much less.

4.24 As with defamation, it would only be in the rarest of circumstances that the publication of personal information gleaned by surveillance would constitute this tort since the element of falsehood would be absent.

---

44 *Per* Lord Justice Glidewell in *Kaye v. Robertson and Another* [1991] F.S.R. 62 at 67.

45 B.M.E. McMahon and W. Binchy, *op. cit.*, p.674.

46 [1991] F.S.R. 62. Glidewell L.J., with whom the other members of the Court agreed, at p.67, described the 'essentials' of the tort as being:

> '...that the defendant has published about the plaintiff words which are false, that were published maliciously, and that special damage has followed as the direct and natural result of their publication.'

'As to special damage', he stated that, by virtue of s.3(1) of the *Defamation Act 1952*:

> '...it is sufficient if the words published in writing are calculated to cause pecuniary damage to the plaintiff.'

Also:

> 'Malice will be inferred if it be proved that the words were calculated to produce damage and that the defendant knew when he published the words that they were false or was reckless as to whether they were false or not.'

(vii) Passing Off[47]

4.25 The tort of passing off has been described by the High Court in the following terms:

> "The essence of passing off is the adoption by the defendant of some element in the manner in which the plaintiff's goods are marketed in a manner calculated to deceive persons intending to buy the plaintiff's product into thinking that they have bought it when in fact they have bought the defendant's product. The element so adopted must be one for which the plaintiff can establish a reputation in the sense that those purchasing goods involving such element do so because of their awareness of the connection between that element and the plaintiff. The element may *inter alia* be the name, the particular mark or design attached to the goods or its get up. In each case, it indicates a badge of origin."[48]

The tort applies to the marketing of services as well as goods, and among the forms other than name, mark or design that the adopted element may take is a likeness (which would include a photograph).

4.26 Irish commentators have remarked that the present limitations of the tort are in some respects arbitrary and have expressed the opinion that the action for passing off could be developed to afford protection in respect of invasions of dignatory and privacy interests.[49]

4.27 Rights to one's name, one's image and one's personality are recognised in a number of civil law jurisdictions.[50] Also, in the United States of America, a remedy in tort is available in respect of the commercial exploitation of a person's name or likeness[51]; and some U.S. commentators have challenged the view that the interest protected thereby is a proprietary one. Thus, Bloustein has argued that in some of the cases the courts were concerned to protect not a proprietary interest, but an interest in preserving human dignity. In his view, the use of a personal photograph or a name for advertising purposes without the person's consent has the same tendency to degrade and humiliate as has

---

47 On this tort in general see, e.g., F.G. Fleming, *op. cit.*, pp.714-720; R.F.V. Heuston and R.A. Buckley, *op. cit.*, pp.395-399; B.M.E. McMahon and W. Binchy, *op. cit.*, ch. 31; and W.V.H. Rogers, *op. cit.*, pp.562-571. Fleming says of the difference between this tort and that of injurious falsehood, "While it is injurious falsehood for a defendant to claim that your goods are his, it is passing off for him to claim that his goods are yours" (p.714).

48 *Player & Wills (Ireland) Ltd. v. Gallagher (Dublin) Ltd.*, High Court, unreported, 26 September 1983, pp.1-2 (Barron J.). See also *Private Research Ltd. v. Brosnan and Network Financial Services Ltd.*, High Court, unreported, 1 June 1995, p.5: "...the essence of the action is that there must be a misrepresentation which would lead a third party to believe that the Defendant's business was that of the Plaintiff." (McCracken J.).

49 B.M.E. McMahon and W. Binchy, *op. cit.*, p.553.

50 See further below paras. 9.63-9.64.

51 See, e.g., D.B. Dobbs, R.E. Keeton and D.G. Owen, *Prosser and Keeton on Torts*, 5th ed., West Publishing Co., St. Paul, Minnesota, 1984, pp. 851-854, and the many cases cited thereat. The publication of a photograph in which the plaintiff incidentally appears is not a tortious invasion of privacy: *Dallessandro v. Henry Holt & Co.*, 1957, 4 A.D.2d 470, 166 N.Y.S.2d 805, appeal dismissed 7 N.Y.2d 7356, 193 N.Y.S.2d 635, 162 N.E.2d 726. Privacy legislation in some Canadian provinces also affords a remedy in tort for such exploitation: see below para. 9.60.

publishing details of personal life to the world at large.[52] This view obviously needs to be tempered somewhat in that the particular circumstances of a case need to be taken into account. The appropriation, to one's advantage, of the name or likeness of another person will not always be humiliating to the other person. While in some cases the other person may suffer a loss of dignity, in other cases any disadvantage will be essentally proprietary or commercial. However, the fact that the law of torts has been extended to afford protection to a person in situations where the person's name or likeness has only nominal value[53] is an interesting development.

4.28 Interesting as such a development may be in comparing the Irish law of torts with that in other jurisdictions, it is highly unlikely that the tort of passing off would in the foreseeable future be extended by the Irish courts to cover the publication of a person's likeness for commercial purposes, without the person's consent, where the essence of the disadvantage suffered by the plaintiff was an affront to human dignity. The tort has to date been treated by the courts as addressing the infringement of a proprietary interest.[54] Whether a common law right to privacy which embraces an interest in the use by another of one's name or likeness will in the future be recognised by the Irish courts is a separate question and one for which, as we have mentioned,[55] there would seem to be no Irish precedent.

(viii) Breach of statutory duty[56]

4.29 Occasionally a statute imposes civil liability for breach of one of its provisions, and it may even do so with explicit reference to the law of torts. An example in the area of information privacy is s.7 of the *Data Protection Act, 1988* which imposes a duty of care on a data controller or a data processor in respect

---

52 E.J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", (1964) 39 *New York University Law Review* 962 at 986.

53 *Ibid.*, p.987.

54 The High Court has said of passing off that:

> "It injures the complaining party's right of property in his business and injures the goodwill of his business. A person who passes off the goods of another acquires to some extent the benefit of the business reputation of the rival trader and gets the advantage of his advertising."

Polycell Products Ltd. v. O'Carroll and Others t/a Dillon, O'Carroll [1959] Ir.Jur.Rep. 34 at 36 (Budd J.).

55 See above para. 4.1.

56 On this type of tort see in general, e.g., R.F.V. Heuton and R.A. Buckley, *op. cit.*, ch. 10; B.S. Markesinis and S.F. Deakin, *op. cit.*, pp.307-324; B.M.E. McMahon and W. Binchy, *op. cit.*, pp.373-395; and W.V.H. Rogers, *op. cit.*, ch. 7.

of the collection of personal data or information and dealing with such data.[57] This section may provide some protection in respect of the unauthorised use or disclosure of personal electronic mail; but it should be noted that personal data kept by an individual and concerned only with the management of the individual's personal, family or household affairs is excluded from the protection afforded by the Act,[58] and of course the section does not specifically address the question of liability for the unauthorised interception of electronic mail.

4.30 A statute may also limit or seek to exclude altogether civil liability arising from breach of a statutory duty or failure to observe the conditions attaching to the exercise of a statutory power. Examples from the field of communications are sections 64 and 88 of the *Postal and Telecommunications Services Act, 1983* with respect to certain loss or damage suffered by a person in the use of a postal

---

57 Section 7 reads:

> "For the purposes of the law of torts and to the extent that that law does not so provide, a person, being a data controller or a data processor, shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned:
>
> Provided that, for the purposes only of this section, a data controller shall be deemed to have complied with the provisions of *section 2(1)(b)* of this Act if and so long as the personal data concerned accurately record data or other information received or obtained by him from the data subject or a third party and include (and, if the data are disclosed, the disclosure is accompanied by) -
>
> (a) an indication that the information constituting the data was received or obtained as aforesaid,
>
> (b) if appropriate, an indication that the data subject has informed the data controller that he regards the information as accurate or not kept up to date, and
>
> (c) any statement with which, pursuant to this Act, the data are supplemented."

Section 2(1)(b) requires a data controller to ensure that personal data kept by her or him is accurate and, where necessary, kept up to date.

58 Section 1(4)(c).

or telecommunications service.[59] An example relating specifically to the interception of communications is the scheme established by the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. This Act placed on a statutory basis and subjected to strict conditions the former administrative practice whereby post and telecommunications were intercepted in the interests of national security and the investigation of crime. It provides that a contravention of many of its provisions or a failure to fulfil conditions laid down in the Act in respect of the authorisation of interceptions shall not "constitute a cause of action at the suit of a person affected by the authorisation."[60] Instead the Act created a special complaints procedure in respect of such contraventions.[61]

4.31 The 1993 Act regulating State interception of communications is however a special case. Statutes which regulate surveillance and the interception of communications typically provide criminal sanctions for failure to comply with their regulatory provisions,[62] and are silent as to whether or not civil liability

---

59 Section 64 provides:

> "(1) Subject to *subsection (3)*, the company shall be immune from all liability in respect of any loss or damage suffered by a person in the use of a postal service by reason of -
>
> (a) failure or delay in providing, operating or maintaining a postal service,
>
> (b) failure, interruption, suspension or restriction of a postal service.
>
> (2) The members of the staff of the company shall be immune from civil liability except at the suit of the company in respect of any loss or damage referred to in *subsection (1)*.
>
> (3) (a) Section 39 of the *Sale of Goods and Supply of Services Act, 1980*, shall not apply to the provision of international services by the company.
>
> (b) The said section 39 shall not apply to the provision of postal services within the State until such date as the Minister for Trade, Commerce and Tourism, after consultation with the Minister, by order provides, whether in relation to such services generally or in relation to services of a class defined in the order in such manner and by reference to such matters as the Minister for Trade, Commerce and Tourism, after such consultation, thinks proper."

Subsection (1) of section 88 provides:

> "Subject to *subsection (3)*, the company shall be immune from all liability in respect of any loss or damage suffered by a person in the use of a service referred to in *paragraph (a)*, *(b)* or *(c)* by reason of:
>
> (a) failure or delay in providing, operating or maintaining a telecommunications service,
>
> (b) failure, interruption, suspension or restriction of a telecommunications service,
>
> (c) any error or omission in a directory published by the company or any telegrams or telex messages transmitted by the company."

Subsections (2) and (3) are the same, *mutatis mutandis*, as subsections (2) and (3) of s.64.

See also ss. 15(2) and 105.

60 Section 9(1).

61 On this procedure see below paras. 6.21-6.26. Section 9(1) explicitly states that the new complaints procedure shall not affect a cause of action for the infringement of a constitutional right.

62 See below ch. 5.

attaches to such failure.[63]

4.32 In cases where there has been a breach of a statutory duty and the statute does not address the issue of civil liability for such breach, the courts have sought to determine whether it was the legislative intent that there should be a civil remedy and have enunciated a number of guidelines they will follow in resolving the issue. The application of these guidelines in cases of surveillance and the interception of communications is however uncertain and much may depend upon the facts of a particular case. Thus, if the user of a postal or telecommunications service has suffered loss as a result of the unlawful interception of her or his communications, the success or otherwise of a civil action for damages resulting from the loss may well depend upon whether the user can be regarded as coming within a particular group or class of persons which it was the legislative intention to protect or whether the statutory provision was enacted solely for the benefit of the public at large. In the former case, the plaintiff may be successful, in the latter the plaintiff generally will not.[64] On the present state of the case law, therefore, an answer to whether civil liability exists for breach of a particular statutory provision regulating surveillance is speculative, since most of the relevant statutes do not specifically address the question.[65]

Equity

(i) The doctrine of confidentiality

4.33 The equitable doctrine of confidentiality affords some protection to a person in respect of the disclosure or use by another of information relating to that person.[66] An action for breach of confidence has been described as, broadly speaking, a civil remedy affording protection against the disclosure or use of information which is not publicly known and which has been entrusted to a person in circumstances imposing an obligation not to disclose or use that information without the authority of the person who has imparted it. There is however considerable uncertainty as to the precise nature and scope of this remedy. Of particular relevance in relation to surveillance is the uncertainty surrounding the relationship between liability and the means by which information is acquired. Moreover, there has been little attempt until recent

---

63 Three statutory provisions relating to broadcasting require respect for privacy in the making and transmission of programmes but do not impose either civil or criminal liability for breach of the requirement. These provisions are considered below at paras. 8.9-8.12.

64 One commentator has expressed the view that there may be a civil right of action for breach of statutory duty against persons who unlawfully open mail since s.66(1) of the *Postal and Telecommunications Services Act, 1983* provides, "Postal packets and mail bags in course of post shall be immune from examination, detention or seizure except as provided under this Act or any other enactment": see M. Forde, *Constitutional Law of Ireland*, Mercier Press, Cork, 1987, p.547.

65 E.G. Hall is of the view, citing the High Court decision, *Cosgrave v. Ireland* [1982] I.L.R.M. 48, that although the Broadcasting Authority Act, 1960 does not expressly provide that a person may sue RTE in damages for breach of its statutory duty to respect privacy, such a person could do so under the general law: *The electronic age*, p.271.

66 On this doctrine generally see Law Commission for England and Wales, *Report on Breach of Confidence*, Law Com. No. 110, Cmnd. 8388, 1981, and M. McDonald, "Some Aspects of the Law on Disclosure of Information", (1979) 14 (n.s.) *Irish Jurist* 229 at 239-242: and, with particular reference to Ireland, R. Keane, *Equity and the Law of Trusts in the Republic of Ireland*, Butterworths, London & Edinburgh, 1988, ch. 30; M. McDonald, *Irish Law of Defamation*, pp.244-251: and B. M. E. McMahon and W. Binchy, *op. cit.*, pp.687-690.

times to distinguish between notions of confidentiality, secrecy and privacy and to identify the relationship between them.[67]

4.34 Where the doctrine does operate to afford protection, the principal remedy is the grant of an injunction to prevent disclosure of the confidence, but other equitable relief such as the delivery up of documents or tapes and damages may be available.[68] Moreover, although the doctrine has its origins in equity, breach of confidence may now have been judicially recognised as a tort.[69]

(ii) The distinction and relationship between confidentiality and privacy

4.35 In its Report on Breach of Confidence, the Law Commission for England and Wales distinguished between privacy and confidence[70] and stressed the essentially different nature of a right based on privacy and one based on confidentiality:

> "... the ... right of action for breach of confidence ... is based on an obligation of confidence owed to another ... once information has been entrusted in circumstances giving rise to an obligation of confidence, that information is in effect impressed with a duty of confidence owed to the person who has entrusted it.
>
> By contrast, a right of privacy in respect of information would arise from the nature of the information itself: it would be based on the principle that certain kinds of information are categorised as private and for that reason alone ought not to be disclosed."[71]

4.36 By way of illustrating the difference, the Commission gave the following example in the context of its consideration of whether the category of persons who can sue for breach of confidence should be widened:

> "Suppose that a newspaper commissioned a journalist to write a candid assessment of a man's life on the understanding that it would be kept confidential until after the man's death and that the journalist furnished an article to the newspaper exposing details of the man's life which were true but likely to cause him distress, or even pecuniary loss; if the article was in fact published by the newspaper before the man's death in breach of their duty of confidence to the journalist, should the man also have a right of action against the newspaper based on their breach

---

67 On the conceptual confusion as to the basis of the action for breach of confidence see, e.g., G. Jones, "Restitution of Benefits Obtained in Breach of Another's Confidence", (1970) 86 L.Q.R. 463 at 463-466. On the distinction between privacy and secrecy, see above p.1, n.3.

68 The damages may be substantial: see *House of Spring Gardens Ltd. and others v. Point Blank Ltd. and others* [1984] I.R. 611 at 683-688 & 705-708, in which the issue of damages for misuse of confidential information was considered together with that for infringement of copyright and the sum of £2,843,857.64 sterling was awarded under this head.

69 See, e.g., *Malone v. Metropolitan Police Commissioner* [1979] Ch. 344; and M. McDonald, *Irish Law of Defamation*, pp.244-246.

70 At paras. 2.1-2.7.

71 See paras. 2.2 and 2.3. See also the *Report of the Committee on Privacy and Related Matters*, para. 8.6.

of confidence?"[72]

While accepting that in this situation the wrong to the man concerned might be regarded as far greater than that to the journalist, the Commission recommended against extending title to sue for breach of confidence to a person in the man's position on the ground that such a person

> "has a complaint not because his confidence has been abused but because his privacy has been infringed and ... to admit an action by him for breach of confidence would amount to using the law of confidence merely as a peg on which to hang a right of privacy in his favour."[73]

4.37 The Australian Law Reform Commission has commented on the distinction and the relationship between an interest in privacy and an interest in confidentiality as follows:

> "Interests in maintenance of confidences differ from privacy interests. Employers want to ensure that referees' confidences are respected so that they might continue to benefit from referees' frank assessments of candidates for employment. Referees have an interest in ensuring respect for their confidences, because of the embarrassment and other injury which might follow disclosure to the subject and others. The subject also has an interest in non-publication. The interests of the employer and referee are interests in confidentiality; the subject of it has a privacy interest. The interests are complementary in this case. But whilst most often complementary, confidences and privacy interests might sometimes be in competition. For example, an individual might seek access to a confidential referee's report to check its accuracy or currency. His privacy interests would be advanced by access. His referee's confidentiality would be destroyed."[74]

---

72 *Working Paper No. 58 on Breach of Confidence*, para. 75, quoted in the *Report* at para. 5.9.

73 *Ibid.* See also paras. 2.4 and 6.60 of the *Report*. In contrast, the Scottish Law Commission did not at first distinguish so sharply in its *Consultative Memorandum on Breach of Confidence* between breaches of confidence and breaches of privacy and proposed the extension of the delict of *injuria* and the creation of new delicts and criminal offences as protection for certain privacy interests: see Provisional Proposals 10-13 & 17-18. However, in its *Report*, the Commission resiled from this broad approach and stated that it was not dealing with the possibility of introducing a law protecting personal privacy in Scotland but only with the circumstances in which, in its view, the law should recognise civil obligations of confidentiality; the defences which should be available in an action for breach of confidence; and the provision of appropriate remedies: see para. 1.10 of the *Report*, Scot. Law Com. No. 90, 1984.

74 The Commission continued:

> "This body of law [i.e. that protecting confidentiality] does not hold the potential for effective protection of all the categories of interests classed by the Commission as 'privacy interests', for example, intrusions by physical or electronic means into the physical domain of a person ('territorial privacy'). Nor is the law relating to confidential relationships equipped to cope with invasions of 'privacy of the person', such as harassment of persons, unwarranted search or seizure, and other conduct threatening indignity, distress and upset to an individual. It does, however, go some way towards controlling the flow of information about a person and thus protecting information privacy."

Report No. 22 on Privacy, 1983, paras. 68 & 69.

4.38 As that Commission has correctly identified, although the distinction between privacy and confidentiality is important,[75] the two concepts may overlap in their application to particular facts. Thus, for example, if information of a private and personal kind is communicated in confidence by A to B, and if B discloses the information to C without A's consent, then B has breached both A's confidence and A's privacy. To the extent that the two concepts overlap, the law on breach of confidence may afford a remedy for what is also a breach of privacy.

4.39 The overlap is well illustrated by the facts of the celebrated case, *Duchess of Argyll v. Duke of Argyll and Others*.[76] The "others" in the case were the editor and proprietors of a Sunday newpaper to whom the Duke had supplied information obtained from the Duchess during their marriage. The Duchess sought an injunction to restrain publication of

> "... secrets of the plaintiff relating to her private life, personal affairs or private conduct, communicated to the first defendant in confidence during the subsistence of his marriage to the plaintiff and not hitherto made public property."[77]

The Court held that it was the policy of the law that communications between husband and wife should be protected against breaches of confidence and that the communications which would be protected are not limited to business matters.[78] Once a court recognised that the communications were confidential and that there was a danger of their publication within the mischief which the law as its policy sought to avoid, then the court would act to protect them. In the instant case the Court had no hesitation in concluding that publication of some of the passages complained of would be in breach of marital confidence and granted the injunction.[79]

(iii) Breach of confidence

4.40 The Younger Committee on Privacy recognised that the law relating to breach of confidence imposes important restrictions on persons' freedom to disclose information in their possession, and its survey of the law on this topic in England and Wales led it to two conclusions: first, that the action for breach of confidence affords, or at least is potentially capable of affording, much greater protection of privacy than is generally realised; and, secondly, that it would not be satisfactory, given the many uncertainties in the law on confidentiality, simply

---

75 It was described as "of fundamental importance" by the Law Commission for England and Wales: see its *Report*, para. 6.6.

76 [1967] 1 Ch. 302.

77 Words in the notice of motion, quoted by the Court at p.317.

78 At p.329.

79 See p.330.

to leave the further development and clarification of the law to the courts.[80] The Committee therefore recommended that the law relating to breach of confidence be referred to the Law Commission for England and Wales and to the Scottish Law Commission with a view to its clarification and statement in legislative form.[81]

4.41 These recommendations were accepted by the British Government and the referrals were duly made. A Working Paper setting out the provisional conclusions of the Law Commission for England and Wales was published in 1974,[82] and a Report containing the Commission's final recommendations was published in 1981.[83] A Consultative Memorandum of the Scottish Law Commission setting out its provisional proposals was published in 1977,[84] and the Report containing its final recommendations in 1984.[85]

4.42 There has been no in-depth study of the law on breach of confidence in Ireland comparable to that undertaken by the Law Commission for England and Wales and the Scottish Law Commission, and it is therefore difficult to identify with any degree of certainty the extent to which the law on the topic in Ireland differs from that in England, Wales and Scotland. Indeed it is the view of one commentator that it "is almost axiomatic that a party claiming relief before an Irish court in respect of the wrongful disclosure of confidential information would seek to rely on the English equitable doctrine of breach of confidence",[86] but, as the same commentator notes, "there exist indigenous legal principles of which an Irish court could be expected to make use, including those which are to be found in constitutional texts."[87]

4.43 That the Constitution may have a significant impact on the application of the doctrine in Ireland is illustrated by the recent High Court decision, *The Attorney General for England and Wales v. Brandon Book Publishers Ltd.*[88] In this case, the plaintiff sought an interlocutory injunction to restrain the defendant from publishing a book written by a deceased member of the British Secret

---

80 *Report of the Committee on Privacy*, Cmnd. 5012, 1972, para. 630. The Australian Law Reform Commission was also of the opinion that the law on breach of confidence:

> "...could be extended so that it would not only provide better protection to the interests of the person who imparts a confidence but would also provide some protection to the privacy interests of the subject of the confidence. The law of confidential relationships provides a solid foundation upon which further protections might be built. In particular, it might be used to control use and disclosure of personal information in the interests of privacy. But, to be effective, the law must provide mechanisms to deal with all aspects of information handling, including its collection, storage and destruction."(*Report No. 22 on Privacy*, para. 69).

81 *Report of the Committee on Privacy*, para. 631.

82 *Working Paper No. 58: Breach of Confidence.*

83 Law Com. No. 116, Cmnd. 8388.

84 *Consultative Memorandum No. 40.*

85 Scot. Law Com. No. 90.

86 M. McDonald, "Some Aspects of the Law on Disclosure of Information", (1979) 14 (n.s.) *Irish Jurist* 229 at 242.

87 *Ibid.* McDonald considers, at pp.247-251, whether the Constitution guarantees a right to non-disclosure of confidential information. What he says on the subject in this 1979 publication should be read in the light of the subsequent cases discussed below. What we are considering here is not the question of whether the Constitution guarantees a right to non-disclosure of confidential information as such, but rather the impact of the Constitution on the equitable doctrine of confidentialty.

88 [1987] I.L.R.M. 135.

Service. The injunction was sought on the ground that the book contained information which had been acquired while the authoress was in the employment of the Service and that it was therefore protected from disclosure by the principle of confidentiality. The defendant relied on the constitutional right of citizens to freedom of expression.[89] In rejecting the claim that confidentiality extended to such information emanating from a government source, and in finding that no cause of action had been shown to restrain publication, the Court attached great weight to the constitutional guarantee of freedom of expression.[90]

4.44 The Constitution apart, both commentaries on breach of confidence in Ireland and the sparse case law on the topic rely heavily on English precedent, suggesting that, despite the different constitutional context, the law in Ireland is substantially the same as that in England and Wales and contains therefore many of the uncertainties associated with the latter.

4.45 It is commonly stated that three conditions must be fulfilled for disclosure to constitute a breach of confidence.[91] First, the information disclosed must have the quality of confidence about it: that is, the information must not be "in the public domain"[92] or be "something which is public property and public knowledge".[93] Secondly, it must have been imparted in circumstances importing an obligation of confidence. Thirdly, it must have been used in an unauthorised way to the detriment of the person who communicated it. Various defences are available, such as compliance with a statutory duty of disclosure or with a court order to disclose. This apparently straightforward exposition of the law is however misleading in that it does not reveal the many complexities and issues relating to the existence, nature and scope of the duty of confidentiality.

4.46 The interpretation and application of the second condition, the circumstances in which an obligation of confidence arises, has been especially problematic. Much of the English case law and commentaries thereon attach importance to the relationship of the parties concerned. In an oft-quoted passage from one of the English cases, the Court suggested a general test rather

---

89 Article 40.6.1° & i.

90 At p.136. It should be noted that the plaintiff in this case was a foreign Government. Subsequent case law has made it clear that there is at least one category of Government information in Ireland the confidentiality of which is protected by the Constitution. In *Attorney General v. Hamilton* [1993] I.R. 250, [1993] 13 I.L.R.M. 81, the Supreme Court, by a majority of 3 to 2, held that, by virtue of Article 28.4 of the Constitution, complete confidentiality attaches to discussions at meetings of the Government and to their contents. The confidentiality does not extend to decisions made at these meetings and to documentary evidence of the decisions. Cf. *Attorney- General v. Jonathan Cape Ltd.* [1976] Q.B. 752; *Attorney-General v. Observer Ltd. and Others* and *Attorney-General v. Times Newspapers Ltd. and Another* [1990] 1 A.C. 109; and the decisions of the European Court of Human Rights, 26 November 1991, in *The Observer and Guardian v. United Kingdom*, Series A, No. 216, 14 E.H.R.R. 153 and *The Sunday Times v. United Kingdom (No. 2)*, Series A, No. 217, 14 E.H.R.R. 229.

91 See, e.g., *Malone v. Metropolitan Police Commissioner* [1979] 1 Ch. 344 at 375; *Francome and Another v. Mirror Group Newspapers Ltd. and Others* [1984] 2 All ER 408 at 414; *Private Research Ltd. v. Brosnan and Network Financial Services Ltd.*, High Court, unreported, 1 June 1995, p.5 (McCracken J., quoting *Copplnger and Skone James on Copyright*, 11th ed., para. 90); B.S. Markesinis and S.F. Deakin, *op. cit.*, p.612; and B.M.E. McMahon and W. Binchy, *op. cit.*, p.688.

92 *Woodward v. Hutchins* [1977] 1 W.L.R. 760 at 764.

93 *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.* (1948) 65 R.P.C. 203 at 215; later also reported at [1963] 3 All E.R. 413 at 415, and quoted with approval by Costello J. in *House of Spring Gardens and Others v. Point Blank Ltd. and Others* [1984] I.R. 611 at 660.

than one which focussed on the particular relationship of the parties. It proposed that:

> "... if the circumstances are such that any reasonable man standing in the shoes of the recipient of the information would have realised that upon reasonable grounds the information was being given to him in confidence, then this would suffice to impose upon him the equitable obligation of confidence."[94]

It cannot however be safely asserted that this broad test has been generally accepted.

4.47 In the *Brandon Book* case, the relationship which, it was argued, gave rise to an obligation of confidence was that between a government and a private individual, the former being the source of the information and the latter the recipient. Here the Court drew a distinction between information which is obtained by one individual from another and information which is obtained from a government source, and quoted with approval the following extract from the Judgment of Mason J. in the Australian case, *Commonwealth of Australia v. John Fairfax & Sons Ltd.*:

> "The equitable principle has been fashioned to protect the personal, private and proprietary rights of the citizen, not to protect the very different interests of the executive government. It acts, or is supposed to act, not according to standards of private interest, but in the public interest. This is not to say that equity will not protect information in the hands of the government, but it is to say that when equity protects government information it will look at the matter through different spectacles.
>
> It may be a sufficient detriment to the citizen that disclosure of information relating to his affairs will expose his actions to public discussion and criticism. But it can scarcely be a relevant detriment to the government that publication of material concerning its actions will merely expose it to public discussion and criticism. It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss, review and criticise government action.
>
> Accordingly the Court will determine the government's claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will not be protected."[95]

Applying this as a correct statement of the law in Ireland, the Court remarked

---

94 *Coco v. A. N. Clark (Engineers) Ltd.* [1969] R.P.C. 41 at 48.
95 (1980) 147 C.L.R. 39 at 51.

that the question of public interest would arise in the case if the Government of Ireland were the plaintiff; but, since the plaintiff was the representative of a foreign government, there was no question of the public interest of the State being affected. This, together with a number of other considerations, led the Court to conclude that no cause of action had been shown by the plaintiff and to refuse the application for an interlocutory injunction. The other considerations were that there was no breach of confidentiality in a private or commercial setting, there is no absolute confidentiality where the parties are a government and a private individual and the defendant possessed a constitutional right to publish information which did not involve any breach of copyright.[96]

4.48 In the earlier English case law, any public interest in the disclosure of the information was generally raised as a defence and, if accepted by the court, was regarded as justification for breaching a duty of confidence.[97] In the *Brandon Book* case, however, the Court considered the question of any public interest in determining whether or not an obligation of confidence arose with respect to the information; and it is in this context that the issue is now also generally considered in Britain.[98] There are some circumstances in which the public interest will be served by the preservation of confidentiality; and there are other circumstances in which the public interest will be best served by disclosure of the information. An example of the former is the confidentiality which attaches in Ireland to discussions at Government meetings.[99] As regards the latter, it has long been accepted that protection by the action for breach of confidence may not be afforded where the information relates to the commission of a crime or other misconduct.[100]

4.49 The leading case on breach of confidence in Ireland is *House of Spring Gardens Ltd. and Others v. Point Blank Ltd. and Others*,[101] in which the Supreme Court affirmed an award of substantial damages, *inter alia*, for breach of confidence and endorsed a number of principles identified by the High Court as pertaining to the latter. The case concerned commercial rather than privacy interests,[102] but is important for its review of many of the English decisions and for its pronouncements on the equitable principles applicable in this area in general. Having concluded from its review of the English cases that they all "show that there is no simple test for deciding what circumstances will give rise to an obligation of confidence"[103], and that equally "there are no hard and fast rules for judging whether or not information can properly be regarded as confidential",[104] the High Court went on to state that the English cases were nevertheless of "considerable assistance"[105] to it and drew thereon to formulate

---

96 [1987] I.L.R.M. 135 at 137.
97 See, e.g., Law Commission of England and Wales, *Working Paper No. 58 on Breach of Confidence*, paras. 91-93.
98 See, e.g., *Attorney General v. Jonathan Cape Ltd.* [1976] Q.B. 752.
99 See above n.90.
100 See, e.g., *Gartside v. Outram* (1856) 26 L.J.Ch. 113 at 114: "You cannot make [me] the confident of a crime or a fraud", and in general Law Commission of England and Wales, *Report on Breach of Confidence*, pp.41-51.
101 [1984] I.R. 611.
102 The information in this case concerned the manufacture of bullet proof vests.
103 At p.662.
104 *Ibid.*
105 At p.663.

the following principles which it thought should be applied in a case like the one before it:

> "[The court] must firstly decide whether there exists from the relationship between the parties an obligation of confidence regarding the information which has been imparted and it must then decide whether the information which was communicated can properly be regarded as confidential information. In considering both (i) the relationship and (ii) the nature of the information, it is relevant to take into account the degree of skill, time and labour involved in compiling the information. As to (i), if the informant himself has expended skill, time and labour on compiling the information, then he can reasonably regard it as of value and he can reasonably consider that he is conferring on its recipient a benefit. If this benefit is conferred for a specific purpose then an obligation may be imposed to use it for that purpose and for no other purpose. As to (ii), if the information has been compiled by the expenditure of skill, time and labour by the informant then, although he has obtained it from sources which are public, (in the sense that any member of the public with the same skills could obtain it had he acted like the compiler of the information) the information may still, because of its value, be regarded as "confidential" information and subject to an obligation of confidence. Furthermore, the court will readily decide that the informant correctly regarded the information he was imparting as confidential information if, although based on material which is accessible to the public, it is of a unique nature which has resulted from the skill and labour of the informant. Once it is established that an obligation in confidence exists and that the information is confidential, then the person to whom it is given has a duty to act in good faith, and this means that he must use the information for the purpose for which it has been imparted, and he cannot use it to the detriment of the informant."[106]

4.50 While the enunciation of these principles is clearly influenced by the commercial context of the case, some of them would appear to be applicable beyond this specific context.[107] Thus, the principle that a recipient of confidential information has a duty to act in good faith in respect of it, meaning that a recipient may only use confidential information for the purpose for which it has been communicated and should not use it to the detriment of the person who confided it, is not dependent upon the particular context of the case. Nevertheless, the statement of principles in the *House of Spring Gardens* case can only be of limited relevance in cases of surveillance not because of the commercial context as such but because the case concerned the communication

---

106 At pp.663-664; affirmed by the Supreme Court at p.696 (*per* O'Higgins C.J., with whom Griffin and McCarthy JJ. agreed).

107 Cf. the view of Carroll J. in *Attorney General for England and Wales v. Brandon Book Publishers Ltd.* that the principles apply only between private individuals in a commercial context: [1987] I.L.R.M. 135 at 136. The Home Office Committee on Privacy and Related Matters described the law on breach of confidence as being "most effective for the protection of commercial information rather than individual privacy": *Report*, para. 8.6.

of confidential information by one person to another and the use by the latter of this information. Surveillance generally does not involve the deliberate communication of information by the informant to the person who acquires it by means of the surveillance.[108]

(iv) Surveillance and confidentiality

4.51 In cases of surveillance, the information will usually have been acquired without the consent or knowledge of the person who imparted it in confidence, that is, the acquirer will not have been party to the confidence, and issues can be expected to arise where either the person who acquired the information in this way or another who becomes privy to the information discloses it to the detriment of the person who was its original source.

4.52 English cases on the extent to which telephone conversations are protected by the law on breach of confidence illustrate some of the uncertainties in this area.

4.53 The Younger Committee on Privacy stated that:

> "People who use the telephone expect to be heard by the person they are talking to and they are also aware that there are several well understood possibilities of being overheard. A realistic person would not therefore rely on the telephone system to protect the confidence of what he says because, by using the telephone, he would have discarded a large measure of security for his private speech."[109]

To discard a large measure of security is not to discard all security; and the Committee mentioned an unauthorised tap on the telephone as an example of circumstances in which a telephone user might be regarded as not having discarded security for private speech.[110] As to the "well understood possibilities of being overheard" on the telephone, examples offered by an English court are the overhearing opportunities provided by extension lines, private switchboards and crossed lines.[111]

4.54 In *Malone v. Metropolitan Police Commissioner*,[112] the Court took the view not only that an obligation of confidence will not arise where the possibility of being overheard is inherent in the circumstances of the communication, but also that the possibility of being overheard by means of the tapping of the telephone is today inherent in the use of this form of communication:

---

108 An exception would be participant monitoring where one person records a conversation with another. The other person may or may not be aware that the conversation is being recorded. See further below paras. 11.35-11.42 on this form of monitoring.

109 See para. 545 of the Committee's *Report*.

110 *Ibid.*

111 *Malone v. Metropolitan Police Commissioner* [1979] 1 Ch. 344 at 360. See also p.376 for examples of such possibilities not related to the use of a telephone.

112 [1979] 1 Ch. 344.

"... a person who utters confidential information must accept the risk of any unknown overhearing that is inherent in the circumstances of communication ....

When this is applied to telephone conversations, it appears to me that the speaker is taking such risks of being overheard as are inherent in the system ... the Younger Report referred to users of the telephone being aware that there are several well-understood possibilities of being overheard, and stated that a realistic person would not rely on the telephone system to protect the confidence of what he says. That comment seems unanswerable. In addition, so much publicity in recent years has been given to instances (real or fictional) of the deliberate tapping of telephones that it is difficult to envisage telephone users who are genuinely unaware of this possibility. No doubt a person who uses a telephone to give confidential information to another may do so in such a way as to impose an obligation of confidence on that other: but I do not see how it could be said that any such obligation is imposed on those who overhear the conversation, whether by means of tapping or otherwise."[113]

4.55 This view should however probably be confined to the facts of the particular case, and indeed the court in *Malone* did specifically state that its decision:

"... was confined to the tapping of the telephone lines of a particular person which is effected by the Post Office on Post Office premises in pursuance of a warrant of the Home Secretary in a case in which the police have just cause or excuse for requesting the tapping, in that it will assist them in performing their functions in relation to crime, whether in prevention, detection, discovering the criminals or otherwise, and in which the material obtained is used only by the police, and only for those purposes. In particular, I decide nothing on tapping effected for other purposes, or by other persons, or by other means; nothing on tapping when the information is supplied to persons other than the police; and nothing on tapping when the police use the material for purposes other than those I have mentioned. The principles involved in my decision may or may not be of some assistance in such other cases, whether by analogy or otherwise: but my actual decision is limited in the way that I have just stated."[114]

4.56 That the principles enunciated in *Malone* may be so limited was recognised in the later case of *Francome and Another v. Mirror Group Newspapers Ltd. and Others*.[115] In this case the Court of Appeal had to consider the proposed publication by a national newspaper of material based on telephone

---

113 At p.376.
114 At pp.383-384. See also pp.355-356.
115 [1984] 2 All ER 408; [1984] 1 W.L.R. 892.

conversations between a husband and wife which had been illegally recorded by bugging their home telephone. The newspaper itself had played no role in the bugging. Rather the eavesdroppers offered to sell a number of the taped conversations to the newspaper, and the newspaper was interested in using them for publication because they seemed to reveal breaches by Mr. Francome, a well-known and successful jockey, of the rules of racing which might also constitute criminal offences. In the exercise of its discretion to preserve the rights of parties pending trial, the Court upheld an interlocutory injunction restraining publication pending the trial of the action.[116] In its view, the case raised issues as to whether or not such conversations are protected by the law on confidentiality and, if so, as to the extent of this protection, issues which should properly be determined at the trial, not in interlocutory proceedings. One judge described as a "surprising proposition"[117] the argument of the defendants, in reliance on *Malone*, that the plaintiffs had no cause of action against them or the eavesdroppers for breach of an obligation of confidentiality. Another commented that what was under consideration in *Malone* was authorised tapping by the police and that:

> "[i]llegal tapping by private persons is quite another matter, since it must be questionable whether the user of a telephone can be regarded as accepting the risk of that in the same way as, for example, he accepts the risk that his conversation may be overheard in consequence of the accidents and imperfections of the telephone system itself."[118]

4.57 If the general principle is accepted that an obligation of confidence will not arise where the possibility of being overheard is inherent in the circumstances of the communication, then issues need to be considered regarding not only the application of the principle in specific circumstances where information is overheard but also its extension to circumstances in which information is obtained other than by overhearing it. In particular, should a comparable principle apply to the acquisition of information by visual as opposed to aural means? And, if so, how will it apply in these other circumstances? For example, should the viewing of a fax message by a person other than the sender or the intended recipient of the message give rise to an obligation of confidence on the part of that person towards the sender or is such viewing inherent in the circumstances of the communication? Does the answer depend on whether the fax was viewed by using a technological aid such as a camera with a telephoto lens or simply the person's ordinary eyesight?

4.58 Some commentators favour the extension of a duty of confidence not only to persons who acquire confidential information by illegal means , but also to those who acquire such information by means not in themselves illegal but

---

116 Breach of such an injunction constitutes contempt of court. In the context of confidentialty, see *The Council of the Bar of Ireland v. Sunday Business Post Ltd.*, High Court, unreported, 30 March 1993.

117 Sir John Donaldson M.R., at p.411.

118 Fox L.J., at p.415. In the Australian case of *Franklin v. Giddens* [1978] Qd.R. 72, an action for breach of confidence was successful where the information was contained in something which had been stolen: see the comment on this case by W.J. Braithwaite in (1979) 95 L.Q.R. 323.

nevertheless reprehensible. One Irish author is of the view that such an extension may be required by the constitutional guarantee of a right to privacy,[119] and there is some English case law to support such a view.[120]

4.59 As we have seen,[121] protection by the action for breach of confidence is subject to consideration of any countervailing public interest. It may be in the public interest that certain information be disclosed, for example, information about criminal activity or about a gross abuse of public trust, even if the information has been communicated by one person to another in confidence. This is often referred to in the literature and case law on breach of confidence as the doctrine of iniquity.

4.60 In *Francome*,[122] the defendants pleaded not only that they were under no obligation of confidence towards the plaintiffs but also that, irrespective of any such obligation, they were entitled to publish such information in that it exposed possible wrongdoing on the part of Mr. Francome. The court's response to this argument was that the public interest would be served by giving the information to the police and to the Jockey Club. The public interest did not require that the information be published in a national newspaper prior to trial.[123]

4.61 The question of the public interest in the exposure of crime was also addressed by the court in *Malone*.[124] Having decided that the tapping in question on behalf of the police did not breach any duty of confidentiality, the court went on to consider whether, if it was wrong on this point, the tapping was nevertheless justified. Approaching its consideration of this matter "with some measure of balance and common sense",[125] it identified the question as being:

> "not whether there is a certainty that the conversation tapped will be iniquitous, but whether there is just cause or excuse for the tapping and for the use made of the material obtained by the tapping."[126]

In its opinion, if certain requirements are satisfied, there will exist just cause or excuse both for the tapping and for using information obtained thereby. The requirements are:

> "... first, that there should be grounds for suspecting that the tapping of the particular telephone will be of material assistance in detecting or preventing crime, or discovering the criminals, or otherwise assisting in the discharge of the functions of the police in relation to crime. Second, no use should be made of any material obtained except for these purposes. Third, any knowledge of information which is not relevant to

---

119 R. Keane, *op. cit.*, pp.349-350.
120 *Ashburton v. Pape* [1913] 2 Ch. 469 at 475. Cf. Law Com. No. 110, paras. 4.7-4.10.
121 See above para. 4.48.
122 [1984] 2 All ER 408.
123 See pp.413, 414 & 416.
124 [1979] 1 Ch. 344.
125 At p.377.
126 *Ibid.*

those purposes should be confined to the minimum number of persons reasonably required to carry out the process of tapping."[127]

The Court made it clear that these requirements are not to be regarded as exhaustive of the circumstances in which just cause or excuse will exist, but that it was stating merely that, if these requirements are satisfied, there will be a just cause or excuse for tapping on behalf of the police and for the use of material obtained thereby.[128]

4.62 With specific reference to the publication of information by a third party, there is a line of English authority to the effect that, where an obligation of confidence is attached to the original acquisition of the information, a third party who subsequently comes into possession of the information is liable to be restrained from disclosing or using it if that person knows or ought to know the information was subject to an obligation of confidence.[129] If, at the time of acquiring the information, the third party had no active or constructive knowledge of its confidential character but subsequently learns or ought to know of its confidential character, the person may be liable for breach of confidence from then onwards.[130]

4.63 In the context of surveillance, information may be lawfully acquired in the first instance, as where a person records a conversation to which she or he is party.[131] Depending on the nature of the conversation and the relationship of the parties, an obligation of confidence may attach to the person in respect of the conversation. If an obligation attaches, then, if the law in Ireland is as stated in the English decisions above, a third party who comes into possession of any of the recorded information may not disclose it without incurring civil liability for breach of confidence - provided the party either knew or ought to have known that the information was subject to an obligation of confidence. It would moreover be somewhat strange if the law were to impose liablity on a third party for publication where the information was lawfully acquired by the person who supplied it to the third party, but not where the information was unlawfully obtained by the supplier, as by the unauthorised tapping of a telephone. Liability as a third party is of particular importance to the media, that is, not only newspapers and magazines but also the radio and television since, as the facts of *Francome*[132] demonstrate, they may have an interest in publishing information of a confidential nature.

---

127 *Ibid.*

128 *Ibid.*

129 See, e.g., *Prince Albert v. Strange* (1849) 1 Mac. & G. 25; *Morison v. Moat* (1851) 9 Hare 241; *Duchess of Argyll v. Duke of Argyll* [1967] Ch. 302.

130 These propositions were regarded by the Law Commission for England and Wales in 1981 as "fairly clear": see paras. 4.11-4.12 of its *Report on Breach of Confidence*. See also B.M.E. McMahon and W. Binchy, *op. cit.*, p.690.

131 It appears that the recording of a conversation by a party to it, whether with or without the knowledge of the other party or parties, is not *per se* unlawful. At least such recording is not a criminal offence: see below para. 5.53.

132 [1984] 2 All ER 408; [1984] 1 W.L.R. 892.

Contract

4.64 An obligation of confidence in respect of information may also be created by contract, express or implied. The High Court has held that a contract of motor insurance was "a contract based upon the exercise of the utmost good faith by each party."[133] For his part, the insured:

> "... was under an obligation to disclose to the insurers every material circumstance which might influence the judgment of the insurers in fixing the premium or indeed in deciding whether or not they would take on the risk. It is clear that such disclosure might involve matters of a very personal and private character so far as [the insured] was concerned, for instance the topic of his health. Concealment or non-disclosure of such matters by [the insured] might well entitle the insurers for their part to avoid the contract if they were subsequently to discover the fact of such concealment or non-disclosure. It seems to follow that the insurers for their part contracted an obligation of confidentiality in respect of such personal information furnished by the insured in the course of negotiating the insurance contract, more particularly when the information involved disclosures which might in particular circumstances lead to the detriment of the person seeking insurance."[134]

4.65 Another relationship in which an obligation of confidentiality may arise under contract is that of employer and employee. Where a contract of employment imposes an obligation of confidence on an employee in respect of information obtained while in employment, contractual liability will flow from the unauthorised disclosure of the information whether it was acquired incidentally as by overhearing a personal conversation, deliberately as by covert surveillance, or or was communicated to the employee in the normal course of employment. There may of course be an issue as to whether the particular information is covered by the contract or not, but if it is covered, then the means by which it was acquired would seem to be irrelevant to the question of liability for unauthorised disclosure.[135]

4.66 An obligation may arise under contract not only in respect of the disclosure of personal information but more generally in respect of the use of the information. This applies to information in the form of a photograph as well as to the spoken or written word. In the English case of *Pollard v. Photographic Company*,[136] an injunction was granted to restrain a photographer from selling or using a photograph of one of the plaintiffs for advertising purposes. The plaintiff had paid the photographer to take a number of pictures of herself and members of her family and to supply her with copies of the photographs. The photographer had however also exhibited in his shop window, apparently for the

---

133 *Murphy v. P.M.P.A.* [1978] I.L.R.M. 25 at 29.

134 *Ibid.* A statutory duty of disclosure may override this contractual obligation of confidentiality. It was argued unsuccessfully by the defendants in this case that the information in question was covered by such a statutory duty.

135 It may however be relevant to the quantum of damages, if any, to be afforded.

136 (1889) 40 Ch.D. 345.

purpose of sale, one of the pictures of the plaintiff made up as a Christmas card. One of the grounds for the granting of the injunction was that it was an implied term of the contract between the plaintiff and the photographer that prints taken from the negative were to be appropriated to the use of the customer only and were not to be used without her consent for any other purpose.[137]

4.67 By analogy with the decision in this and similar cases, it may be argued that where information is openly acquired under contract for a specific purpose, use of that information for another purpose without the consent or authority of the other party to the contract will constitute a breach of the contract.[138] This would apply to the acquisition of information by means of surveillance as well as by other means. The contractual duty will however be owed to the other party to the contract, who, in cases of surveillance, will often be a person other than the one subjected to surveillance. Thus, where a private security firm provides video surveillance of a shop, the contract will be between the firm and the shop. If the surveillance is conducted in a privacy-invasive manner as by focussing on the anatomy of female customers, the customers will have no remedy in contract against the security firm for the affront to their personal dignity.

4.68 Where information is surreptitiously acquired, as by covert surveillance, it may be possible, in a rare case, for the subject of the surveillance to claim that it is an implied term of a contract that such surveillance not occur or, at least, any personal information obtained in this way not be published without the person's consent. One such case may be the secret taking of photographs of the Princess of Wales working out in a gymnasium. The photographs were taken by the owner of the gymnasiuum and sold by him to a Sunday newpaper which then published them.[139]

4.69 The statutory duty of a broadcasting contractor not to encroach unreasonably on the privacy of any individual[140] is reinforced by the terms of the contract between the Independent Radio and Television Commission and the contractor.[141] Echoing the words of the statute, the contract provides that in programmes broadcast by the contractor and in the means employed to make programmes the contractor will not unreasonably encroach on the privacy of an individual. The Commission has the power to suspend or terminate a contract if the contractor has, in the opinion of the Commission, committed serious or repeated breaches of its obligations under the contract.[142]

---

137 At pp.349-350.

138 See, e.g., *Report of the Law Commission on Breach of Confidence*, para. 4.1.

139 The Princess' action against the owner of the gymnasium and Mirror Group Newspapers for, *inter alia*, breach of contract was reportedly settled out of court for the sum of £1,000,000. The Princess also received formal apologies from the persons concerned and it was agreed that the photographs and negatives would be surrendered for destruction: see "The Times" and "The Independent", 9 February 1995.

140 See below para. 8.10.

141 Contracts are open to inspection by members of the public at the Commission's registered office: ss.14(5) and 18(1) of the *Radio and Television Act, 1988*.

142 Sections 14(4)(a)(ii) and 18(1) of the *Radio and Television Act, 1988*.

Copyright

4.70 Copyright is largely regulated in Ireland by statute.[143] The main statute is the *Copyright Act, 1963.*

4.71 Copyright subsists in original literary, dramatic, musical and artistic works.[144] The latter include photographs, irrespective of their artistic quality.[145] Copyright generally vests in the author of the work, unless the work is made in the course of the author's employment, in which case the employer is entitled to the copyright.[146] There is a particular exception where a literary, dramatic or artistic work is made by the author in the course of employment by the proprietor of a newspaper, magazine or similar periodical made under a contract of service or apprenticeship, and is made for the purpose of publication in these media. In such cases, the proprietor is entitled to the copyright in the work in so far, but only in so far, as it relates to publication of the work in the relevant medium or to its reproduction for the purpose of it being so published. In all other respects the author is entitled to the copyright.[147] Also, the 1963 Act specifically provides that where a person commissions the taking of a photograph,[148] and pays or agrees to pay for it in money or money's worth, and the work is made in pursuance of that commission, that person is entitled to any copyright subsisting therein.[149] Certain dealings or acts in respect of artistic works are not to be regarded as an infringement of copyright.[150] One such act is the inclusion of a photograph in a television broadcast by way of background or incidental to the principal matters represented in the broadcast.[151]

4.72 Copyright also subsists in sound recordings, cinematograh films and broadcasts.[152] Of particular relevance for present purposes is the copyright in sound recordings and cinematograph films.[153] The owner of the copyright is generally the maker of the recording or film.[154] As in the case of photographs, there is an exception for commissioned recordings and films. Where a person

---

143 See the *Copyright Act, 1963*, s.60(4). The Act specifically provides that nothing in it shall affect the operation of any rule of equity relating to breaches of trust or confidence: s.60(3).

144 Section 8 & 9 of the 1963 Act. Part II of the Act deals with copyright in original works.

145 Section 9(1)(a).

146 See s.10(1) & (4).

147 Section 10(2).

148 Or the painting or drawing of a portrait, or the making of an engraving.

149 Section 10(3).

150 See generally s.14.

151 Section 11(4). See also s.11(5).

152 Section 17-19. Part III of the Act deals with copyright in these media.

153 "Sound recording" is defined in the Act as meaning "the aggregate of the sounds embodied in, and capable of being reproduced by means of, a record of any description, other than a sound-track associated with a cinematograph film": s.17(14). "Cinematograph film" is defined as meaning:

> "...any sequence of visual images recorded on material of any description (whether translucent or not) so as to be capable, by use of that material -
>
> (a) of being shown as a moving picture, or
> (b) of being recorded on other material (whether translucent or not) by the use of which it can be shown": s.18(1)).

For the purposes of the Act, a cinematograph film shall be taken to include the sounds embodied in any sound-track associated with the film: s.18(8). See also s.18(9) & (11).

154 Sections 17(3) and 18(3) respectively.

commissions the making of a sound recording or cinematograph film, and pays or agrees to pay for it in money or money's worth, and the recording or film is made in pursuance of that commission, that person is entitled to any copyright subsisting in the recording or film.[155]

4.73 Copyright furthermore subsists in certain published editions of literary, dramatic and musical works, the publisher being entitled to the copyright.[156]

4.74 Copyright law may therefore afford some protection in respect of an invasion of privacy where the literary or artistic work, or the sound recording or cinematograph film, contains personal information or has a personal dimension to it. For example, publication within the protected time-period[157] without the consent of the author of the work or maker of the recording or film would constitute an infringement of copyright. Remedies comprise "all such relief, by way of damages, injunction, accounts or otherwise ... as is available in any corresponding proceedings in respect of infringement of other proprietary rights."[158]

4.75 There are however two significant limitations to any protection afforded privacy by means of an action for infringement of copyright, one relating to the owner of copyright, the other to what may be the subject of copyright. First, infringement is only actionable at the suit of the owner of the copyright.[159] Thus this route to obtaining a remedy for invasion of privacy is not open to a person whose photograph was taken or whose voice was recorded by another, unless the photograph or recording was commissioned by that person. To the extent that any copyright exists, it is generally owned by the taker of the photograph or the recorder of the voice. In fact any copyright owner will often be the invader of privacy rather than the person whose privacy was invaded. Secondly, it is unlikely to be available in most cases of covert surveillance. It is improbable that the courts would regard a person as possessing copyright under the 1963 Act in his or her telephonic or other conversations. There is no copyright in one's own voice or image as such.[160] Only in the case of the reproduction or publication of a personal document might an action for breach of copyright be available, and then only to the author of the document. For example, the writer of a personal letter might claim copyright in the letter as a literary work and bring an action for infringement of copyright if the letter were secretly photographed and published, as in a newspaper.[161] There is however

---

155 *Ibid.*

156 Section 20. This copyright is additional to, and independent of, any copyright enjoyed by the author of an original work: s.21(2).

157 For these periods see ss.8(4) & (5), 9(5), (6) & (7), 15(2)(a), 17(2), 18(2), 19(2), 20(4) and 51(3), (4) & (5), as amended by the European Communities (Term of Protection of Copyright) Regulations, 1995, S.I. No. 158 of 1995.

158 Section 22(2). See also s.22(3) concerning the remedy where the defendant was not aware, and had no reasonable grounds for suspecting, that copyright existed in the work or other subject-matter to which the action relates.

159 Section 22(1).

160 Cf. German Act on Copyright in Artistic Creations, s.22f., dealt with below at para. 9.65.

161 The defendant might seek to argue that what was published was the photograph of the letter and that copyright in the photograph is enjoyed by the person who took it.

no copyright in information. The law of copyright would provide no remedy for the invasion of privacy where another person reads the letter and reproduces it in his or her own words.[162] Both these limitations would apply in Ireland to a case such as the secret recording and publication of a telephone conversation between the Prince of Wales and his close friend, Camilla Parker Bowles.[163]

4.76 Copyright law is clearly not designed to protect privacy, and any protection it affords is purely incidental. It recognises human creativity and places a value thereon by granting the creator of a 'work' a proprietary interest in the fruit of his or her creativity.

Conclusion

4.77 In drawing attention to the inadequacy of the legal protection of privacy in England and comparing English law in this regard unfavourably with German law, one writer has commented:

> "True, many aspects of the human personality and privacy are protected by a multitude of existing torts but this means fitting the facts of each case in the pigeon-hole of an existing tort and this process may not only involve strained constructions; often it may also leave a deserving plaintiff without a remedy."[164]

4.78 Much of the case law mentioned above bears testimony to the equal truth of this comment in relation to Irish law, more particularly, as regards the inadequacy of existing civil remedies in affording protection to privacy in cases of surveillance. Only by 'strained construction' will many of the civil actions be available in such cases, and in many cases 'a deserving plaintiff will be left without any remedy at all'. Many of the torts have been designed to protect interests other than privacy and only incidentally afford a remedy where there is an infringement of the latter. Even the doctrine of confidentiality which has been seen by some as carrying the potential for greater protection of privacy, was not fashioned with information privacy in mind, but rather without reference to the nature or content of the information being conveyed. It was not intended to promote human dignity but to fulfil the less ambitious task of protecting information entrusted in confidence by one person to another.

---

162 See, e.g., *Report of the Committee on Privacy and Related Matters*, para. 9.2.

163 The conversation was secretly taped on 18 December 1989 and first published in the magazine "New Idea" on 13 January 1993. On 17 January 1993, both "The Sunday Mirror" and "The People" broke a self-imposed embargo and published extracts of the conversation. Thereafter the conversation was widely reported.

Certain commercial dealings which infringe copyright are also criminal offences. These include selling, hiring, trading or importing into the State (otherwise than for private and domestic use) any article which a person knows to be an infinging copy of copyright work: see generally s.27 of the *Copyright Act, 1963*, as amended by s.2 of the *Copyright (Amendment) Act, 1987*.

164 B.S. Markesinis, *The German Law of Torts*, 3rd ed., Clarendon Press, Oxford, 1994, p.416. See also B.S. Markesinis, "Our Patchy Law of Privacy - Time to do Something about It", (1990) 53 M.L.R. 802; and for a general review of the treatment of privacy interests by the English courts from the beginning of the nineteenth century to the present day, D.J. Seipp, "English Judicial Recognition of a Right to Privacy", (1983) *Oxford Journal of Legal Studies* 325 at 334-345 & 353-362.

4.79 While the civil law therefore provides some protection against intrusive surveillance, this protection is patchy, usually incidental, and like the protection afforded by the Constitution, undeveloped and uncertain.

CHAPTER 5: CRIMINAL SANCTIONS

Introduction

5.1 A variety of criminal offences may be committed in the course of surveillance. Often the offence will be incidental or ancillary to the surveillance, as where an overenthusiastic press photographer, eager to take a picture, assaults someone in the process,[1] or a postal packet is intercepted with the ulterior intent of robbery.[2] It would not be appropriate for us in the context of this Paper to examine all these offences. Rather we consider below those offences, both at common law and under statute, which are most likely to be committed by a person engaged in surveillance by virtue of the surveillance activity itself. We also pay some attention to offences relevant to the disclosure of information obtained by means of surveillance. Finally, we note the power of the courts, on conviction of a person of an offence, to make a compensation order and consider, with specific reference to surveillance, the relationship between the making of such an order in a criminal context and the civil liability of an offender for personal injury or loss resulting from the offence.

Common Law Offences

(i) Breach of the peace

5.2 It has been held by the High Court of Justiciary in Scotland that a person who peered in at a lighted window of a dwelling-house after nightfall had been properly found guilty of a breach of the peace.[3] There was evidence of earlier "peeping Tom" activities in the street and the particulars of the offence

---

1 On the offence of assault in Ireland see, e.g., P. Charleton, *Offences Against the Person*, Round Hall Press, Dublin, 1992, ch. 6; and our *Report on Non-Fatal Offences Against the Person*, LRC 45-1994, para. 1.20f.

2 See, e.g., ss.50, 52, 53 & 55 of the *Post Office Act, 1908*, as amended by s.8(1) and the Fourth Schedule of the *Postal and Telecommunications Services Act, 1983*, and s.12 of the *Larceny Act, 1916*.

3 *Raffaelli v. Heatly* (1949) S.L.T. 284.

alleged that the defendant had put the residents in a state of fear and alarm by his conduct. One of the judges was satisfied:

> "... that this class of thing to the annoyance of the modesty of women, if persevered in, has always been from time immemorial treated both in England and here as a police offence of which the not too appropriate name, perhaps, is breach of the peace."[4]

Another stated:

> "It is usual to charge this offence as a breach of the peace, because it is a species of disorderly conduct; where something is done in breach of public order or decorum which might reasonably be expected to lead to the lieges being alarmed or upset, or tempted to make reprisals at their own hand, the circumstances are such as to amount to breach of the peace."[5]

5.3 In contrast, in England, a breach of the peace is not regarded as an offence but as a ground for arrest without warrant at common law.[6] Anyone can arrest another person where the latter commits a breach of the peace in the arrestor's presence, or where the arrestor reasonably believes that a breach will be committed in the immediate future unless the other person is arrested, or where a breach has been committed and the arrestor reasonably believes that a renewal of it is threatened.[7] Also, a person may be bound over by a magistrate to keep the peace. The order of the magistrate "is an exercise of the powers which have been exercised for many centuries as a measure of preventive justice."[8] The Court of Appeal in England has said that:

> "... there is a breach of the peace whenever harm is actually done or is likely to be done to a person or in his presence to his property or a person is in fear of being so harmed through an assault, an affray, a riot, an unlawful assembly or other disturbance. It is for this breach of the peace when done in his presence or the reasonable apprehension of it taking place that a constable, or anyone else, may arrest an offender without warrant"[9]

5.4 Moreover, it has also been held by the Court of Appeal that a breach of the peace can occur on private premises even if the only persons likely to be affected by the breach are inside the premises and no member of the public

---

4 (1949) S.L.T. 284 at 286, *per* Lord Mackay.

5 At 285, *per* Lord Justice-Clerk Thomson (Lord Jamieson concurring).

6 See, in general, *Archbold 1994*, Vol. 2, Sweet & Maxwell, London, 1993, paras. 19-343 & 344 and 29-45; J.C. Smith and B. Hogan, *Criminal Law*, 7th ed., Butterworths, London, 1992, p.437; and G. Williams, *Textbook of Criminal Law*, 2nd ed., Stevens, London, 1983, p.487; Law Commission, *Criminal Law. Binding Over: The Issues*, Working Paper No. 103, H.M.S.O., 1987 and *Binding Over*, Report, Law Com. No. 222, Cm 2439, H.M.S.O., 1994.

7 See *R. v. Howell* (1981) 73 Cr. App. Rep. 31 at 36, [1982] Q.B. 416 at 426, [1981] 3 All ER 383 at 388.

8 *R. v. County of London Quarter Sessions Appeals Committee, ex parte Metropolitan Police Commissioner* [1948] 1 K.B. 670 at 675 (*per* Lord Goddard C.J.).

9 *R. v. Howell* (1981) 73 Cr. App. Rep. 31 at 37, [1982] 1 Q.B. 416 at 427, [1981] 3 All ER 383 at 339.

outside the premises is involved.[10]

5.5 It is not altogether clear whether a breach of the peace constitutes an offence in Ireland, but there is some authority for the view that it does.[11] In a case where the defendant fired a shot into a dwelling-house, the Court of Criminal Appeal said that "[i]n order to constitute a breach of the peace an act must be such as to cause reasonable alarm and apprehension to members of the public".[12] This it described as "the substantial element of the offence."[13] Since the charge as framed did not reveal a breach of the peace, the Court allowed the defendant's appeal and reversed his conviction. Nevertheless, as there was uncontradicted evidence that there were persons in the house at the time, the Court held that he could properly be found guilty of having committed a breach of the peace; and it therefore directed him to enter into security to keep the peace and be of good behaviour for a period of 3 years and, in default of such security, ordered him to be imprisoned for a period of 6 months.

5.6 It is clear that the District Court has jurisdiction, irrespective of conviction, to bind a person over to keep the peace and to require sureties of the peace. This jurisdiction has been confirmed by the Irish courts. In *R. (Boylan) v. The Justices of Londonderry*,[14] it was held that, as there had been no conviction, the binding over order:

> "... should have shown either a threat by the prosecutor of future violence, or an attempt to or an intention to commit an assault, or some other state of facts which would render it reasonably probable that he would be guilty of a future breach of the peace."[15]

More recently, the High Court has described this jurisdiction as having "an ancient history"[16] and said that it has been exercised "by the courts for so many centuries that the origin of the jurisdiction is buried in the mists of the common law."[17] In this case the Court rejected a constitutional challenge to the jurisdiction on the ground that the common law powers of magistrates to bind to the peace had not been carried over on the enactment of the Constitution. It was alleged that these powers fail to hold citizens equal before the law, constitute preventative detention or preventative justice and punish conduct which has yet to occur and which may not occur. The Court took the view that the power of

---

10 *McConnell v. Constable of the Greater Manchester Police* [1990] 1 All ER 423. The premises in this case was a shop.

11 See, in general, on breach of the peace in Ireland, J. O'Connor, *The Irish Justice of the Peace*, vol. 2, 2nd ed., Ponsonby Ltd., Dublin, 1915, pp.29-46; E.F. Ryan and P.P. Magee, *The Irish Criminal Process*, Mercier Press, Dublin, 1983, p.96, and our *Report on Non-Fatal Offences Against the Person*, LRC 45-1994, paras. 1.275-277. It is treated as an offence in practice. Thus, several of the soccer hooligans who were involved in violence at the international match between Ireland and England at Lansdowne Road, in Dublin, on 15 February 1995 were charged with and convicted of being in breach of the peace: see "The Irish Times", 17 February 1995, p.8 and "Irish Independent", 17 February 1995, p.17.

12 *Attorney-General v. Cunningham* [1932] I.R. 28 at 33.

13 *Ibid.*

14 [1912] 2 K.B. 374.

15 At 380.

16 *Gregory and Others v. Windle and Others* [1995] 1 I.L.R.M. 131 at 136.

17 At p.139.

binding over "is a beneficial and necessary jurisdiction, which, if exercised prudently and with discretion, does not give rise to any conflict with the constitutional guarantee of personal liberty."[18] Any abuse of the jurisdiction could be rectified by invoking the supervisory role exercised by the superior courts in respect of the orders made by courts of limited and local jurisdiction and this constituted a sufficient safeguard for the liberty of the person.[19]

5.7 On the basis of the above case law, a person who is subject to surveillance and who being aware of the surveillance apprehends harm to their person (or possibly property) may, in the exercise of the power of arrest for breach of the peace, take action against the observer to avoid the harm. Where however the person is unaware of the surveillance, she or he will not be in a position to take such action. Similarly, where a third person sees another engaged in surveillance and apprehends harm to the subject of the surveillance, that person may arrest the observer in order to prevent the harm. In such cases the observer may also be subsequently bound over by the District Court to keep the peace. As understood by the English courts, the power of arrest for breach of the peace is concerned with the protection of persons and property. It is not concerned with counteracting an affront to human dignity or an invasion of privacy as such. The judges in the Scottish "peeping Tom" case, however, interpreted the concept of a breach of the peace more liberally. In their view the offence was designed not only to protect public order but also decorum and the modesty of women[20]; and in the latter instances it is more directly concerned with the protection of privacy as such.

5.8 Even if a liberal interpretation of a breach of the peace were to be preferred by the Irish courts, both the instances of surveillance to which it would apply and the protection which it would afford in those cases to which it applied are limited. The power of arrest without warrant may have a restraining effect but is dependent upon the person being observed or a third person taking action. And where a person is brought before the District Court in connection with a breach of the peace, the normal sanction is that the person will be bound over to keep the peace and to be of good behaviour for a period of time. Only in default will imprisonment be imposed.

(ii) Eavesdropping

5.9 The common law offence of eavesdropping is a form of common or public nuisance. According to *Blackstone's Commentaries* in the early nineteenth

---

18 At p.139. The Court continued:

> "A person who is the victim of abusive or intimidating or violent language or behaviour on the part of another person should be able to invoke the protection of the legal process without waiting for an actual assault to take place, and without having to embark on costly legal proceedings in search of an injunction. It seems to be reasonable and proper that a person who has been guilty of some form of outrageous behaviour or language should be asked to give guarantees in appropriate form that it will not be repeated in the future ..."

19 *Ibid.*

20 *Rafaelli v. Healty* (1949) S.L.T. 284 at 286.

century it was committed by listening under walls or windows or the eaves of a house, and framing slanderous and mischievous tales.[21]

5.10 More recently an English court has stated, "The gist of the offence [is] listening just outside a house with the object of spreading slanderous and mischievous tales."[22] It is an indictable offence, punishable by fine and finding sureties for good behaviour.

5.11 The offence would therefore seem to be concerned with surreptitious aural surveillance and to target disclosure of what is overheard rather than the surveillance itself. However, in *Russell on Crime* an English case of 1956 is mentioned in which the offence was extended to the activities of a "peeping Tom" and the author of that text detected a tendency in that jurisdiction to treat cases of spying, with no evidence of listening, as within the meaning of eavesdropping.[23]

5.12 The offence was abolished in England in 1967,[24] but has not been expressly abolished in Ireland. The author of *Russell on Crime* drew attention to the lack of specificity in the extension of the offence to spying and expressed the view that it was desirable that the law be enunciated in a more precise manner.[25] It may be that the offence does not possess the requisite degree of specificity to comply with the principle of legality and was not carried over in 1922 or subsequently in 1937 as the law of this State.[26] However, if the offence does still exist in Ireland, it affords only limited protection to privacy interests in cases of surveillance. Apart from the uncertainty of its application to cases of visual surveillance, it does not cover listening other than in proximity to a house and requires that the listening be done with the object of spreading slanderous and mischievous tales.[27] Clearly it bears the hallmark of an earlier, pre-electronic age and was not framed with sophisticated listening and optical devices such as exist today in mind.

Statutory Offences

(i) The Criminal Justice (Public Order) Act, 1994

5.13 Section 6 of the *Criminal Justice (Public Order) Act, 1994* makes it an offence for any person, *in a public place*, to "use or engage in any threatening,

---

21 Vol. 4, 15th ed., 1809, p.168. See also J.W.C. Turner, *Russell on Crime*, vol. 2, 12th ed., Stevens, London, 1964, p.1397; *Malone v. Metropolitan Police Commissioner* [1979] 1 Ch. 344 at 357; *Rhodes v. Graham* (1931) 37 S.W.(2d) 46 at 47 (Kentucky Court of Appeals); and cf. *R. v. County of London Quarter Sessions Appeals Committee* [1948] 1 K.B. 670 at 675.

22 *Malone v. Metropolitan Police Commissioner* [1979] 1 Ch. 344 at 373.

23 Vol. 2, 12th ed., 1964, by J.W.C. Turner, pp.1397-98: *R. v. Wyres.* The defendant had been detected looking through a window at night at a partially clothed woman washing herself in a kitchen. He was bound over to keep the peace and ordered to pay 15s 3d costs.

24 *Criminal Law Act*, s.13(1).

25 At p.1398.

26 On the compatibility of common law crimes in general with this principle, see T. O'Malley, "Common Law Crimes and The Principle of Legality," (1989) 7 *Irish Law Times* 243.

27 See *Malone v. Metropolitan Police Commissioner* [1979] 1 Ch. 344 at 373-74.

abusive or insulting words or behaviour with intent to provoke a breach of the peace or being reckless as to whether a breach of the peace may be occasioned". This offence is punishable, on summary conviction, to a fine not exceeding £500 and/or to imprisonment for a term not exceeding 3 months.

5.14 Section 12 of the *Criminal Justice (Public Order) Act, 1994* amends section 4 of the *Vagrancy Act, 1824*. Section 4 of the latter Act deems certain persons to be rogues and vagabonds who, on conviction, may be sentenced to a maximum of 3 months hard labour. This section originally included within its ambit anyone "being found in or upon any dwelling house, warehouse, coach-house, stable, or outhouse, or in any inclosed yard, garden, or area, for any unlawful purpose".[28] This category has however been deleted by virtue of the 1994 Act.[29]

(ii) Railways (Conveyance of Mails) Act, 1838

5.15 The *Railways (Conveyance of Mails) Act, 1838*, as amended by the *Postal and Telecommunications Services Act, 1983*,[30] empowers An Post, "for the greater security of the mails or post letter bags", to make reasonable regulations in respect of their conveyance by rail,[31] and breach of the regulations is an offence.[32] An Post has not exercised this power and it would appear that there is no need for it to do so, since, at the present time, An Post does not use rail services for the conveyance of post.

(iii) The Malicious Damage Act, 1861

5.16 Under section 37 of the *Malicious Damage Act, 1861*, as amended by s.14(2)(a) of the *Criminal Damage Act, 1991*:

> "Whosoever shall unlawfully and maliciously cut, break, throw down, destroy, injure, or remove any Battery, Machinery, Wire, Cable, Post, or other Matter or Thing whatsoever, being Part of or being used or employed in or about any telegraph (within the meaning of the *Telegraph Acts, 1863* to *1916*), or in the working thereof, or shall unlawfully and maliciously prevent or obstruct in any Manner whatsoever the sending, Conveyance, or Delivery of any Communication by any such Telegraph, shall be guilty of a Misdemeanour ..."

---

28 We commented on this provision in our *Report on Vagrancy and Related Offences* (LRC 11-1985), and noted that it had been decided at Circuit Court level that a "peeping Tom" in an enclosed area was there for an unlawful purpose. The case is reported in "The Irish Times", 10 April 1981, p.13.

29 We recommended in our earlier *Report on Vagrancy and Related Offences* that section 4 should be repealed and replaced with two new offences, an offence of being found in or upon any building or in any yard or garden or in any enclosed area with intent to commit an offence, and an offence of trespassing on residential premises in a manner which causes or is calculated to cause nuisance or annoyance or fear to another person: para. 14.13.

30 Section 8(1) and the Fourth Schedule.

31 Section 5. On the conveyance of mails by tramway or tramroad, see the *Conveyance of Mails Act, 1893*, ss.2(1) & 3.

32 Section 12. Summary proceedings in relation to any function of An Post may be brought and prosecuted by An Post: s.5(4) of the *Postal and Telecommunications Services Act, 1983*.

The offence is punishable, on summary conviction, with imprisonment for a term not exceeding 3 months or a fine not exceeding £10 and, on conviction on indictment, with imprisonment for a term not exceeding 2 years. An attempt to commit any of the offences mentioned in section 37 is punishable with imprisonment for a term not exceeding 3 months or with a fine not exceeding £10.[33]

5.17 Telephone tapping which involves cutting, breaking, injuring or removing a telegraph wire may constitute an offence under section 37,[34] as would preventing or obstructing thereby any communication by telegraph, though such prevention or obstruction is unlikely to arise in the case of tapping, at least if it is efficiently carried out. It would moreover be necessary to show that the defendant had acted maliciously and without lawful authority.

(iv) Telegraph Act, 1863

5.18 Section 45 of the *Telegraph Act, 1863*, as amended by the *Postal and Telecommunications Services Act, 1983*,[35] provides:

> "If any Person in the Employment of the Company -
>
> > Wilfully or negligently omits or delays to transmit or deliver any Message;
> >
> > Or by any wilful or negligent Act or omission prevents or delays the Transmission or Delivery of any Message;
>
> he shall be guilty of an offence."[36]

An offence under this section is punishable, on summary conviction, with a fine not exceeding £800 or with imprisonment for a term not exceeding 12 months or both, and on conviction on indictment, with a fine not exceeding £50,000 or with imprisonment for a term not exceeding 5 years or both.[37] A person is exempt from liability under this section in the same four circumstances as apply to offences under s.98(1) of the *Postal and Telecommunications Services Act,*

---

33 Section 38. On the meaning of "telegraph", see further below paras. 5.62-5.63.

34 A telegraph wire usually consists of 4 cables encased in PVC insulation. Only 2 of the cables are used for connection. Installation of an "inseries tap" involves the cutting or breaking of one of these cables. The installation of a "parallel tap" involves breaking through the PVC insulation and clipping the device on to both cables. Weare grateful to Liam Brady, electronics engineer and private investigator, Dublin, for providing us with this and other technical information.

35 Section 8(1) and the Fourth Schedule.

36 Summary proceedings in relation to any function of Bord Telecom Éireann may be brought and prosecuted by Bord Telecom Éireann: s.5(5) of the *Postal and Telecommunications Act, 1983*. In general proceedings for an offence under this section or for an ancillary offence may only be taken by or with the consent of the Director of Public Prosecutions: see s.10(1) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. The consent of the D.P.P. is however not required where proceedings are brought by the Minister for Transport, Energy and Communications or Bord Telecom Éireann.

37 Section 4(1) of the *Postal and Telecommunications Services Act, 1983*. See also s.4(2).

1983.[38]

5.19 If an employee of Bord Telecom Éireann were deliberately to withhold transmission of a telegram without falling into one of the four exempted categories, that employee may be guilty of an offence under this section.

(v) The Conspiracy and Protection of Property Act, 1875

5.20 It is an offence under subsection 2 of section 7 of the *Conspiracy and Protection of Property Act, 1875* for a person persistently to follow another person about from place to place.[39] It is an offence under subsection 4 of section 7 to watch or beset the house or other place where another person resides, or works, or carries on business, or happens to be, or the approach to such a house or place.[40] Offences are committed under each subsection only if the defendant acted "wrongfully" and "without lawful authority". The defendant must moreover have acted "with a view to compel [the] other person to abstain from doing or to do any act which such other person has a legal right to do or abstain from doing".[41] The offences are punishable with a fine not exceeding £20 or a term of imprisonment not exceeding 3 months.

5.21 One of the grounds of appeal to the Supreme Court in *Kane v. Governor of Mountjoy Prison*[42] was that the extent and nature of the surveillance to which Kane had been subjected constituted an unlawful harassment of him, representing an offence under s.7 of the 1875 Act,[43] and that this, together with other reasons, vitiated the legality of his arrest. The Supreme Court was unanimous in rejecting the appeal and in holding that Kane's detention was lawful. The surveillance was justified either in the expectation of an extradition warrant from the British authorities or in order to track down illegally-held arms and was not excessive. It is implicit in this decision that no offence under s.7 of the 1875 Act was committed by the gardaí. The judges, being more concerned to deal with the constitutional than the criminal dimension of the case, did not link their reasoning to the wording of this particular statutory provision; but since it would appear that the police did persistently follow Kane about from place to place, the missing ingredient of the offence was most probably that the police were not acting "wrongfully" or "without lawful authority". It is also doubtful whether they

---

38 See s.13(1) of the *Interception of Postal Packets and Telecommunications Messages Act, 1993* and further below paras. 5.54-5.58.

39 On the meaning of "persistently follow", see *Smith v. Thomasson* 16 Cox 740 (Pollock B.) All the English cases up to 1896 are discussed in the U.S. case *Vegelahn v. Guntner* 167 Mass. 92.

40 It is specifically provided by section 7 that:

> "Attending at or near the house or place where a person resides, or works, or carries on business, or happens to be, or the approach to such house or place, in order merely to obtain or communicate information, shall not be deemed a watching or besetting within the meaning of this section."

41 Where the defendants and others had continually watched and walked up and down before the prosecutor's business premises, and had followed him through the streets to his private residence, it was held that, if the acts of "watching" and "persistently following" were done with the intention of coercing the prosecutor to take back a dismissed employee, the defendants ought to be found guilty: *R. v. Wall* 21 Cox (Ir.) 401.

42 [1988] I.R. 757.

43 [1988] I.R. 757 at 788.

were acting 'with a view to compelling Kane to abstain from doing or to do any act which he had a legal right to do or abstain from doing'.

(vi) Post Office (Protection) Act, 1884

5.22 The second paragraph of section 11 of the *Post Office (Protection) Act, 1884*, as amended by the *Postal and Telecommunications Act, 1983*[44] provides:

> "If any person, being in the employment of a telegraph company as defined by this section -
>
> Improperly divulges to any person the purport of any telegram;
>
> such person shall be guilty of an offence ..."[45]

For the purposes of this section the expression "telegraph company" means "any company, corporation, or persons carrying on the business of sending telegrams for the public under whatever authority or in whatever manner such company, corporation, or persons may act or be constituted"; and the expression "telegram" means "a written or printed message or communication sent to or delivered at the office of a telegraph company, for transmission by telegraph, or delivered by a telegraph company as a message or communication transmitted by telegraph." The expression "telegraph" has the same meaning as in the *Telegraph Act, 1869*, and the Acts amending the same. The same penalties apply as in respect of s.45 of the *Telegraph Act, 1863*,[46] as do the same four categories of exemption from liability.[47]

5.23 Given that the offences under s.98 of the *Postal and Telecommunications Services Act, 1983* may only be committed when a telecommunications message is in the course of transmission by Bord Telecom Éireann,[48] two aspects of this provision are worth noting. First, it applies to the improper disclosure of the purport of a telegram at any time including the pre and the post transmission stages. Secondly, the offence may be committed by an employee of any telegraph company, not merely an employee of Bord Telecom Éireann, and this is of some importance in the context of the deregulation of telecommunications services.[49]

---

44 Section 8(1) and the Fourth Schedule.

45 Summary proceedings in relation to any function of Bord Telecom Éireann may be brought and prosecuted by Bord Telecom Éireann: s.5(5) of the *Postal and Telecommunications Services Act, 1983*. Proceedings for an offence under this paragraph or for an ancillary offence may likewise only be taken by or with the consent of the Director of Public Prosecutions, except that the consent of the D.P.P. is not required where proceedings are brought by the Minister for Transport, Energy and Communications, An Post or Bord Telecom Éireann: see s.10(1) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*.

46 See s.4(1) & (2) of the *Postal and Telecommunications Services Act, 1983*.

47 Section 13(1) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. See above para. 5.18 and below paras. 5.54-5.58.

48 See below para. 5.52.

49 See above para. 2.12ff.

(vii) Post Office Act, 1908

5.24 Section 51 of the *Post Office Act, 1908*, as amended by the *Postal and Telecommunications Services Act, 1983*, provides:

> "If any person unlawfully takes away or opens a mail bag sent by any vessel employed by or under An Post for the transmission of postal packets under contract, or unlawfully takes a postal packet in course of transmission by post out of a mail bag so sent, he shall be guilty of felony, and on conviction shall be liable, at the discretion of the court, to penal servitude for any term not exceeding fourteen years or not less than three years, or to imprisonment, with or without hard labour, for any term not exceeding two years."[50]

5.25 Whereas the offences under s.84(1) of the *Postal and Telecommunications Services Act, 1983* relate only to interference with postal packets,[51] this provision catches ancillary improper conduct in that it applies to the unlawful opening of a mail bag and the unlawful taking of a postal packet in course of transmission by post out of a mail bag. However, it is narrowly drawn in that it applies only to such conduct when the mail bag is "sent by any vessel employed by or under An Post for the transmission of postal packets under contract." The expression "mail bag" includes "a bag, box, parcel, or any other envelope or covering in which postal packets in course of transmission by post are conveyed, whether it does or does not contain any such packets."[52]

5.26 Under section 62 of the 1908 Act, as amended by the *Postal and Telecommunications Services Act, 1983*,[53] it is an offence, *inter alia*, without lawful authority, to affix or to attempt to affix anything in or on or in association or conjunction with a telegraph post or other property belonging to or used by or on behalf of An Post or Bord Telecom Éireann and to disfigure such property. The interception of telecommunications may entail the commission of such an offence, e.g., where a listening device is clipped to a telegraph wire. An offence under this section is punishable, on summary conviction, with a fine not exceeding £800 or imprisonment for a term not exceeding 12 months or both, and, on conviction on indictment, with a fine not exceeding £50,000 or imprisonment for a term not exceeding 5 years or both.[54] On conviction on indictment, the court may also order any apparatus, equipment or other thing used to commit the offence to be forfeited.[55]

---

50 Summary proceedings for an offence under the 1908 Act in relation to any function of An Post may be brought and prosecuted by An Post: s.5(4) of the *Postal and Telecommunications Services Act, 1983*.

51 See below para. 5.37.

52 Section 89.

53 Section 8(1) and the Fourth Schedule. Summary proceedings for any offence under the 1908 Act in relation to any function of Bord Telecom Éireann may be brought and prosecuted by Bord Telecom Éireann: s.5(5) of the 1983 Act.

54 Section 4(1) of the *Postal and Telecommunications Services Act, 1983*.

55 Section 4(2) of the 1983 Act.

5.27 The Act also contains special provisions relating to ship letters,[56] and one of these provisions deals with the opening of such post. Section 28 provides:

> "(1) If a master of a vessel -
>
> (a) opens a sealed mail bag with which he is entrusted for conveyance, or
> (b) takes out of a mail bag with which he is entrusted for conveyance any postal packet or other thing,
>
> he shall forfeit two hundred pounds.
>
> (2) If any person to whom postal packets have been entrusted by the master of a vessel to bring on shore breaks the seal, or in any manner wilfully opens them, he shall on summary conviction be liable to a fine not exceeding twenty pounds."

(viii) Larceny Act, 1916

5.28 Under s.10 of the *Larceny Act, 1916*:

> "Every person who maliciously or fraudulently abstracts, causes to be wasted or diverted, consumes or uses any electricity shall be guilty of felony, and on conviction thereof shall be liable to be punished as in the case of simple larceny."

Simple larceny is "punishable with penal servitude for any term not exceeding five years, and the offender, if a male under the age of sixteen years, shall be liable to be once privately whipped in addition to any other punishment to which he may by law be liable."[57] The form of trial and penalty for an offence under section 10 has subsequently been modified in that s.6(1) of the *Electricity (Supply)(Amendment) Act, 1942*, allows that such an offence:

> "... may (in lieu of prosecution by indictment) be prosecuted and tried summarily in the District Court, subject to the restriction that the punishment inflicted on conviction by that Court shall not exceed a fine of fifty pounds or imprisonment for six months."

Summary proceedings may be brought at the suit of the Electricity Supply Board or of any other person.[58]

5.29 Some forms of telephone tapping involve the abstraction of a very small

---

56 Sections 26-30 & 32 (Section 31 was repealed by the 1983 Act).

57 Section 2 of the Act. It is doubtful whether the latter part of this sanction which provides for the whipping of a male under the age of 16 years has been carried over post independence into the law of the State in that arguably it offends against a number of constitutional guarantees (equality before the law, the right of bodily integrity, the right to freedom from torture and from inhuman or degrading punishment).

58 Section 6(2) of the *Electricity (Supply)(Amendment) Act, 1942.*

amount of electricity from the tapped wire or cable, and may therefore constitute an offence under section 10.[59] However, since the amount of abstracted electricity is negligible, the *de minimis* principle may apply to any prosecution.[60] This offence is clearly not targeted at the protection of privacy as such, and may only incidentally afford protection to the latter. It is concerned with the protection of property.

(ix) The Wireless Telegraphy Acts, 1926-1988

5.30 It is prohibited to keep or have in one's possession anywhere in the State any apparatus for wireless telegraphy without a licence.[61] Moreover, anyone who possesses such apparatus under licence is required to instal, maintain, work or use it in accordance with the terms and conditions of the licence.[62] A condition is generally attached to the grant of a licence in order to protect from improper disclosure messages which were not intended for the recipient. For example, personal (citizen band) radio licences are granted subject to the condition that the holder of the licence:

> "... shall not make known or allow to be made known the contents, origin, destination or existence of any message which he received by means of such apparatus, and which he was not entitled to receive, to any person and shall not record by any means, produce in writing, copy by any means of reproduction, or make any use of such message or allow the same to be recorded by any means, produced in writing, copied by any means of reproduction or made use of."[63]

---

59 A negligible amount of electricity is abstracted in the use of both an 'inseries tap' and a 'parallel tap'. On these forms of tap, see above n.34.

60 On the operation of this principle see, e.g., G. Williams, *op. cit.*, pp.619-622.

61 Section 3(1) of the *Wireless Telegraphy Act, 1926*. The offence may also be committed in a ship or aircraft: see further s.3(5). Sound broadcasting receivers, such as ordinary household radios, were exempted from the licensing requirement in 1972: see the *Wireless Telegraphy Act, 1926* (Section 3) (Exemption of Sound Broadcasting Receivers) Order, 1972, S.I. No.211 of 1972.

62 Section 3(2) of the *Wireless Telegraphy Act, 1926*, as amended by s.11(a) of the *Wireless Telegraphy Act, 1972*. See s.5 concerning the grant of licences.

63 Regulation 7(2)(f) of the Wireless Telegraphy (Personal Radio Licence) Regulations, 1982, S.I. No.8 of 1982. See also Regulation 13 and Condition 15 in the Third Schedule to the Wireless Telegraphy (Experimenter's Licence) Regulations, 1937, S.R.&O. No.330 of 1937, which provides:

> 'The licensee shall not use or allow the station to be used for the receipt of messages other than messages intended for receipt thereby or sent for general reception. If any other message is unintentionally received by means of the station the licensee shall not make known or allow to be made known its contents, its origin or destination, or the fact of its receipt by any person (other than a duly authorised officer of the Government ... or a competent legal tribunal).';

and Regulation 11 and Condition 8 in the Second Schedule to the Wireless Telegraphy (Business Radio Licence) Regulations 1949, S.I. No.320 of 1949, which is headed 'Secrecy of correspondence' and reads:

> 'The licensee and his authorised agents shall preserve the secrecy of correspondence.
>
> If any message which the Licensee or his authorised agents are not entitled to receive is received the Licensee or his authorised agents shall not make known or allow to be made known its contents its origin or destination its existence or the fact of its receipt to any person (other than a duly authorised officer of the government or a competent legal tribunal) and shall not produce in writing copy or make any use of such message or allow the same to be reproduced in writing copied or made use of.'

It is an offence to keep, have in one's possession, instal, maintain, work or use any apparatus without a licence or in contravention of the terms and conditions of a licence.[64]

5.31 In cases where the apparatus is not a television set, these offences are punishable, on summary conviction, with a fine not exceeding £1,000, and, on conviction on indictment, with a fine not exceeding £20,000.[65] On conviction on indictment, any interest of the offender in the apparatus in respect of which the offence was committed is forfeited, and the apparatus may be destroyed or sold or otherwise disposed of.[66] Summary proceedings may only be taken at the suit of the Minister for Transport, Energy and Communications.[67]

The expression "wireless telegraphy":

> "... means the emitting and receiving, or emitting only or receiving only, over paths which are not provided by any material substance constructed or arranged for that purpose, of electric, magnetic or electro-magnetic energy of a frequency not exceeding 3 million megahertz, whether or not such energy serves the conveying (whether they are actually received or not) of communications, sounds, signs, visual images or signals, or the actuation or control of machinery or apparatus."[68]

The expression "apparatus for wireless telegraphy" is similarly defined as apparatus capable of such emitting and receiving, and is stated to include "any part of such apparatus, or any article capable of being used as part of such apparatus",[69] as well as "any other apparatus which is associated with, or electrically coupled to, apparatus capable of so emitting such energy".[70]

5.32 Certain listening devices fall within this statutory definition of "apparatus for wireless telegraphy" and are therefore subject to the licence requirements. Such a device would typically comprise a microphone which picks up voice, converts it into wave-form radio signals and then transmits it over a distance to a radio receiver which reconverts the wave-form radio into intelligible audio form. Both the apparatus by which the sound is transmitted and that by which it is received are covered by these licence provisions. Similarly, radio scanning devices are covered. The operation of such devices does not normally entail interference with licensed wireless telegraphy, but if it should, such interference

---

64 Section 3(3) of the *Wireless Telegraphy Act, 1926*, as substituted by s.12(1)(a) of the *Broadcasting and Wireless Telegraphy Act, 1988*. Breach of the conditions of a licence may also result in the suspension or revocation of the licence: see, e.g., Regulation 15 of the Wireless Telegraphy (Personal Radio Licence) Regulations, 1982; and cf. Regulation 14 of the Wireless Telegraphy (Experimenter's Licence) Regulations, 1937 and Regulation 12 of the Wireless Telegraphy (Business Radio Licence) Regulations, 1949.

65 Section 3(3)(a)(ii).

66 See s.3(3A), (3B) & (3C), inserted by s.12(1)(a) of the *Broadcasting and Wireless Telegraphy Act, 1988*. See also s.9(1) & (2) of the *Wireless Telegraphy Act, 1972* concerning prosecutions.

67 Section 13 of the 1926 Act.

68 Section 2 of the *Wireless Telegraphy Act, 1926*, as amended by s.2(1)(b) of the *Broadcasting and Wireless Telegraphy Act, 1988*.

69 Section 2 of the *Wireless Telegraphy Act, 1926*, as amended by s.2(1)(a) of the *Broadcasting and Wireless Telegraphy Act, 1988*.

70 *Ibid.*

may also constitute an offence.[71]

5.33 It is also an offence under subsections 2 and 3 of section 2 of the 1926 Act improperly to divulge the purport of any message, communication, or signal sent or proposed to be sent by wireless telegraphy. The offence is punishable, on summary conviction, with a fine not exceeding £1,000 or a term of imprisonment not exceeding 6 months, or both, and, on conviction on indictment, with a fine not exceeding £20,000 or a term of imprisonment not exceeding 12 months or both.[72]

5.34 Furthermore, section 7 of the *Wireless Telegraphy Act, 1972*, empowers the Minister for Transport, Energy and Communications by order to specify apparatus of any class or description which may not be sold, let on hire, manufactured or imported without a licence. For the purpose of the Act, "manufacture" includes construction by any method and the assembly of component parts.[73] An order under s.7 may be made where it appears expedient to the Minister for the purpose of preventing or reducing the risk of interference with wireless telegraphy, or for such other purpose as the Minister shall specify.[74] In 1981, the Minister made an order specifying for the purposes of section 7:

> "... wireless telegraphy apparatus consisting of a radio transceiver capable of transmitting and receiving voice communication on any frequency between 26.96 and 27.41 MHz, and designed to use, or capable of using, amplitude modulation".[75]

This order was made to control personal radio (citizen band) equipment. It is an offence to sell, let on hire, manufacture or import specified apparatus without a licence or to do so other than in compliance with the terms and conditions of any licence applying thereto.[76] These offences are punishable, on summary conviction, with a fine not exceeding £1,000, and, on conviction on indictment, with a fine not exceeding £20,000 and forfeiture of any interest in apparatus in relation to which the offence was committed.[77]

---

71 See s.12 of the *Wireless Telegraphy Act, 1926*, as amended by s.12(1)(g) of the *Broadcasting and Wireless Telegraphy Act, 1988*, and s.8 of the *Wireless Telegraphy Act, 1972*.

72 Section 2(3) of the *Wireless Telegraphy Act, 1926*, as substituted by s.12(1)(f) of the *Broadcasting and Wireless Telegraphy Act, 1988*.

73 Section 1(1).

74 An order may only be made with the consent of the Minister for Tourism and Trade.

75 Wireless Telegraphy (Control of Sale, Letting on Hire or Manufacture, and Importation of Radio Transceivers) Order, 1981, S.I. No. 400 of 1981. The Order cites the purpose of preventing or reducing the risk of interference with wireless telegraphy and came into operation on 1 January 1982.

76 Section 10(2) of the *Wireless Telegraphy Act, 1972*.

77 Section 10(4) of the *Wireless Telegraphy Act, 1972*, as substituted by s.12(2)(b) of the *Broadcasting and Wireless Telegraphy Act, 1988*.

(x) The Postal and Telecommunications Services Act, 1983

(a) Disclosure of confidential information

5.35 Section 37 of the *Postal and Telecommunications Services Act, 1983* makes it an offence for a person to disclose confidential information obtained while performing duties as a director or member of staff, or an adviser or consultant to, An Post or Bord Telecom Éireann or as a postmaster unless the person is duly authorised to do so. "Confidential" means that which is expressed to be confidential either as regards particular information or as regards information of a particular class or description.[78] "Duly authorised" means authorised by either An Post or Bord Telecom Éireann or by some person authorised in that behalf by either company. A person found guilty of an offence under this section is liable, on summary conviction, to a fine not exceeding £800 or to imprisonment for a term not exceeding 12 months, and, on conviction on indictment, to a fine not exceeding £50,000 or to imprisonment for a term not exceeding 5 years or both.[79]

(b) Interception of postal packets

5.36 The principle of the inviolability of post has long been recognised in statutes regulating postal services.[80] The currently applicable statutory provision is section 66(1) of the *Postal and Telecommunications Services Act, 1983*, which reads:

> "Postal packets and mail bags in course of post shall be immune from examination, detention or seizure except as provided under this Act or any other enactment."

5.37 The principle of the inviolability of the post is backed up with criminal sanctions. Section 84(1) of the 1983 Act provides:

> "A person who -
>
> (a) opens or attempts to open a postal packet addressed to another person or delays or detains any such postal packet or does anything to prevent its due delivery or authorises, suffers or permits another person (who is not the person to whom the postal packet is addressed) to do so, or
> (b) discloses the existence or contents of any such postal packet, or
> (c) uses for any purpose any information obtained from any such postal packet, or
> (d) tampers with any such postal packet,

---

78 Section 37(3).

79 Section 4(1). See also s.4(2). Summary proceedings may be brought and prosecuted by An Post or Bord Telecom Éireann, as the case may require: s.5(1).

80 See, e.g., ss.28, 51 & 56 of the *Post Office Act, 1908*.

without the agreement of the person to whom the postal packet is addressed shall be guilty of an offence."[81]

Such a person is liable to the same penalties as apply in respect of an offence under s.37.[82]

5.38 The 1983 Act also however provides that criminal liability shall not attach to a person engaging in the above conduct if the person is acting in any of the following three capacities:

(i) by virtue of any power conferred on An Post by section 83 of the Act;

(ii) in pursuance of a direction issued by the Minister for Transport, Energy and Communications under section 110;

(iii) under other lawful authority.[83]

5.39 Section 83 empowers An Post, *inter alia*, to refuse, detain, defer delivery or dispose of postal packets in certain circumstances. It also specifically empowers the company to open:

(i) unsealed postal packets,

(ii) postal packets which are undeliverable,

(iii) postal packets awaiting collection *poste restante* and not collected,

(iv) parcels due for collection and not collected.

This power to open certain postal packets and parcels is unqualified. In particular, it is to be noted that the mere fact that a packet is unsealed renders it liable to being opened by the company.

5.40 Section 110 empowers the Minister for Transport, Energy and Communications to issue directions in writing to An Post. In particular, the Minister may by direction require An Post "to do (or refrain from doing) anything which he may specify from time to time as necessary in the national interest."[84] Where such a direction involves the interception of a postal packet, under the *Interception of Postal Packets and Telecommunications Messages*

---

81 In addition to these general offences of interference with postal packets, a few other statutory offences exist which may only be committed by a particular person or persons or in particular circumstances: see, e.g., ss.28 & 51 of the *Post Office Act, 1908*, and above paras. 5.24 & 5.27.

82 See above para. 5.35. Summary proceedings may be brought and prosecuted by An Post: s.5(2). See also s.10(1) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. Where a person is charged with an offence under section 84 or an ancillary offence, no further proceeding in the matter shall be taken except by or with the consent of the Director of Public Prosecutions. The consent of the D.P.P. is however not required where proceedings are brought by An Post.

83 Section 84(2).

84 Section 111(1)(b).

(Regulation) Act, 1993, an authorisation is required.[85]

5.41 Lastly, a person who acts "under other lawful authority" is also exempt from criminal liability under section 84 of the 1983 Act. Several statutes provide such authority. For example, customs and excise officers may, subject to certain conditions, open and examine a packet suspected of containing contraband goods.[86]

5.42 Two aspects of the offences created by s.84(1) should be noted. First, unlike the comparable offences in relation to telecommunications messages,[87] they are not explicitly limited to postal packets conveyed by the relevant semi-state body, that is, An Post. Secondly, on the face of it, they apply to postal packets wherever they may be and not merely to postal packets in the course of their transmission by post - unless, of course, the term "postal packet" is to be understood as incorporating this limitation.[88] Hence the inviolability afforded postal packets by this provision would appear to be broader than that recognised by section 66(1) which applies only "in course of post".[89]

5.43 Section 84 also empowers An Post, with the consent of the Minister for Transport, Energy and Communications, to make regulations to carry out the intentions of the section in so far as concerns members of its staff,[90] and contravention of any applicable regulation is an offence punishable with the penalties given above.[91] No such regulations have however been made to date.

The meaning of postal packets

5.44 Since the offences under section 84 relate to postal packets, the meaning of this term is of some importance. There is no definition of the term "postal packet" in the 1983 Act; but it should be noted that the several references in the Act to the term in the context of services provided by persons other than An Post[92] mean that the term is not to be understood as meaning only packets handled by the latter.

5.45 Although the Act contains no definition of the term, it does state that:

> "Any word or expression to which a particular meaning is assigned by

---

85 Section 3. See further below ch. 6.

86 See section 18 of the *Post Office Act, 1908*.

87 See below para. 5.52.

88 Cf. the offences under s.54 of the *Post Office Act, 1908* of the unauthorised opening of a letter and of preventing or impeding the due delivery of a letter. A letter for the purpose of this section was defined as "a postal packet in course of transmission by post and any other letter which has been delivered by post": s.54(4). Cf. also the offences of opening any postal packet in course of transmission by post and of detaining or delaying any such postal packet under section 56 of the 1908 Act. Sections 54 and 56 were repealed by section 7 and Part I of the Third Schedule of the 1983 Act.

89 Again there is no definition of the word "post" in the 1983 Act. Nor is there a definition in the *Post Office Acts, 1908* to *1951*.

90 Section 84(3)(a). The Minister, after consultation with An Post, may also direct it to make, amend or revoke such regulations: s.84(3)(b).

91 Sections 4(1) and 84(3)(c).

92 Notably in section 63(3).

the *Post Office Acts, 1908* to *1951*, the *Post Office Savings Bank Acts, 1861* to *1958*, or the *Telegraph Acts, 1863* to *1916*, has in this Act, except where the context otherwise requires, the meaning so assigned."[93]

5.46 In the *Post Office Act, 1908*, unless the context otherwise requires, the expression "postal packet" means:

> "a letter, post card, reply post card, newspaper, book packet, pattern or sample packet, or parcel, and every packet or parcel transmissible by post, and includes a telegram."[94]

Section 19 of the 1908 Act further provided that:

> "If any question arises whether any postal packet is a letter or any other description of postal packet within the meaning of this Act, or any warrant or regulations made under this Act, the decision thereon of the Postmaster-General shall be final, save that the Treasury may, if they think fit, on the application of any person interested, reverse or modify the decision, and order accordingly."[95]

For the reference to the Postmaster-General in this section was substituted first the Minister for Posts and Telegraphs and more recently An Post.[96]

5.47 Two relevant amendments were made to these provisions of the 1908 Act by the *Post Office and Telegraph Act, 1920*. The first was the substitution of the expression "printed packet" for the expression "book packet" in section 89 of the 1908 Act.[97] The 1920 Act has since been repealed by the *Postal and Telecommunications Services Act, 1983*,[98] but the substitution may have survived by reason of the provision in the 1983 Act (the saving provision) whereby particular meanings assigned to any word or expression by these earlier Acts were retained for the purpose of the 1983 Act. If the 1920 substitution is regarded as affecting the meaning of the expression "postal packet", then it may concern an "expression to which a particular meaning is assigned by the *Post Office Acts, 1908* to *1951*, and hence remain operative despite the repeal of the 1920 Act. However, since the 1983 Act expressly repealed the *whole* of the 1920 Act and not merely all provisions other than the one dealing with the substitution, a contrary interpretation is possible. The second amendment provided that the final phrase of section 19 of the 1908 Act allowing the Treasury to reverse or modify the decision of the postal authority should cease to have effect.[99] Since this amendment did not concern the assignment by statute of a particular meaning to any word or expression but rather the assignment to a

---

93 Section 1(2).
94 Section 89.
95 See also s.74 concerning prosecution of an offence under the Act.
96 See section 8(1) of the *Postal and Telecommunications Services Act, 1983* and Part I of the Fourth Schedule thereto.
97 See section 1(2).
98 By section 7 and Part I of the Third Schedule thereto.
99 See section 5.

person of the determination of a question as to the appropriate category of a postal packet, i.e. whether it was a letter or other description of postal packet, it does not fall within the saving provision. Moreover, in that the determination of such a question by the executive offends against the doctrine of the separation of powers, the phrase almost certainly was not carried over by the 1937 Constitution and ceased to have effect at that time, if not earlier.

5.48 Although the 1983 Act contains no definition of the term "postal packet", it does however state that in section 63 the term "does not include a telegram, a newspaper or a parcel unless a communication or, in the case of a newspaper, a communication not forming part of a newspaper is contained in it."[100] Section 63 is the provision of the 1983 Act which deals with the exclusive privilege of An Post and with those postal services which are not to be regarded as a breach of this privilege.

5.49 It would therefore appear that in section 63 of the 1983 Act, "postal packet" means a letter, post card, reply post card, book packet (or possibly printed packet), pattern or sample packet, parcel containing a communication, newspaper containing a communication which does not form part of the newspaper, and every other packet or article transmissible by post, excluding a telegram. Since the definition is stated to apply in section 63 rather than in the Act, the question arises whether the definition is to be strictly limited to this section, in which case the 1908 definition will apply wherever the term appears elsewhere in the Act, or whether it must be implied elsewhere in the Act, at least where some connection exists between section 63 and the other provision. Common sense and the interpretation of the Act as a whole suggests that where the term appears elsewhere in provisions dealing with the postal services, it should be understood as carrying the same meaning in these provisions as in section 63,[101] but its meaning in provisions other than s.63 cannot be regarded as free from doubt. It is particularly undesirable that the meaning of the expression in s.84 should be open to more than one interpretation since this section penalises certain conduct in respect of postal packets.

5.50 As regards the 1908 definition, it should also be noted that this definition does not require that a "packet" be in the course of transmission by post to constitute a "postal packet". The reference to transmissibility by post is to be distinguished from actual transmission.[102] The expression "postal packet" is not therefore inextricably linked to transmission by post. In fact, in contrast to the wording of the offences under s.84(1) of the 1983 Act, the offences under ss.54 and 56 of the 1908 Act, since repealed, explicitly applied only to postal packets in course of transmission by post.[103]

---

100 Section 63(7).

101 Sections 65, 66(1), 83 & 84.

102 There are certain articles which may not legally be transmitted by post, e.g contraband goods and explosive substances, and An Post may impose conditions and restrictions as to the mode of packing, colour, form and design of packets and classes of packets: see s.63 of the *Post Office Act, 1908* and s.83(c) of the *Postal and Telecommunications Services Act, 1983*. See also s.70 of the 1983 Act.

103 See above n.88.

5.51 By virtue of a 1983 amendment to s.74 of the *Post Office Act, 1908*,[104] on the prosecution of any offence under the 1983 Act, evidence that an article is in the course of transmission by post, or has been accepted on behalf of An Post for transmission by post, shall be sufficient evidence that the article is a postal packet.[105] This evidential provision can however only be of limited effect in that it will not apply to offences involving the transmission of postal packets by persons other than An Post, and it cannot therefore be regarded as determinative of the meaning of the expression "postal packet" for the purpose of all offences under the 1983 Act, let alone for the purpose of all offences relating to interference with correspondence.

(c) Interception of telecommunications messages

5.52 No principle of inviolability comparable to that enjoyed by the post extends to telecommunications. However, section 98(1) of the *Postal and Telecommunications Services Act, 1983*, provides that:

> "A person who -
>
> (a) intercepts or attempts to intercept, or
> (b) authorises, suffers or permits another person to intercept, or
> (c) does anything that will enable him or another person to intercept,
>
> telecommunications messages being transmitted by the company or who discloses the existence, substance or purport of any such message which has been intercepted or uses for any purpose any information obtained from any such message shall be guilty of an offence."

"Intercept" means:

> "listen to, or record by any means, in the course of its transmission, a telecommunications message but does not include such listening or

---

104 Section 8(1) and Part I of the Fourth Schedule of the 1983 Act.

105 This evidential provision also applies to prosecutions of an offence under the 1908 Act. Section 90 of the 1908 Act, as amended by s.8(1) and the Fourth Schedule of the 1983 Act, provides that, for the purposes of the 1908 Act:

> "(a) A postal packet shall be deemed to be in course of transmission by post from the time of its being delivered to a post office to the time of its being delivered to the person to whom it is addressed; and
>
> (b) The delivery of a postal packet of any description to a letter carrier or other person authorised to receive postal packets of that description for the post shall be a delivery to a post office; and
>
> (c) The delivery of a postal packet at the house or office of the person to whom the packet is addressed, or to him or to his servant or agent or other person considered to be authorised to receive the packet, according to the usual manner of delivering that person's postal packets, or under an arrangement authorised under the provisions of *section 65* of the *Postal and Telecommunications Services Act, 1983*, shall be a delivery to the person addressed."

recording where either the person on whose behalf the message is transmitted or the person intended to receive the message has consented to the listening or recording."[106]

The offences under section 98(1) concern only messages transmitted by Bord Telecom Éireann. Moreover they apply to messages only in the course of their transmission. They are punishable with the same penalties as apply to the comparable offences in respect of postal packets, which penalties include, upon conviction on indictment, forfeiture of any apparatus, equipment or other thing used to commit the offence.[107]

5.53 The 1983 Act originally contained a definition of the noun "interception", which was stated to mean:

> "listening to, or recording by any means, or acquiring the substance or purport of, any telecommunications message without the agreement of the person on whose behalf that message is transmitted by the company and of the person intended by him to receive that message."[108]

The new definition is narrower in one important respect. It does not apply where either the person on whose behalf the message is transmitted or the person intended to receive the message has consented to the listening or recording.[109] The "agreement" of both persons was required for the earlier definition not to apply.

5.54 Criminal liability does not attach under s.98(1) to a person in four situations: that is, where the person is acting:

(i) for the purpose of an investigation by a member of the Garda Síochána of a suspected offence under section 13 of the *Post Office (Amendment) Act, 1951* on the complaint of a person claiming to have received a message by telephone of the type covered by the section, or

(ii) in pursuance of a direction issued by the Minister for Justice under

---

106 Section 9(6), as substituted by s.13(3) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*, which also states that cognate words shall be construed accordingly. The interception of broadcasting services is governed by ss.9-15 of the *Broadcasting Act, 1990*. We are not concerned with such interception in this Paper. See our *Report on the Law Relating to Dishonesty*, LRC 43-1992, para. 9.12.

107 Section 4(1) & (2). The Act also provides for the making of regulations by Bord Telecom Éireann to carry out the intentions of section 98 in so far as concerns members of its staff: s.98(3)(a) & (b). A person who contravenes any of these regulations shall be guilty of an offence: s.98(3)(c). No regulations have however been made under these subsections. Summary proceedings may be brought and prosecuted by Bord Telecom Éireann: s.5(3). Where a person is charged with an offence under s.98 or an ancillary offence, no further proceedings shall be taken in the matter except by or with the consent of the Director of Public Prosecutions: see s.10(1) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. The consent of the D.P.P. is however not required where proceedings are brought by the Minister for Transport, Energy and Communications or Bord Telecom Éireann.

108 Section 98(5). The subsection did not provide that cognate words were to be construed accordingly.

109 It also clearly applies only to a telecommunications message in the course of its transmission. While this may have been implied in the earlier definition, it was not explicitly stated. Furthermore, the definition no longer encompasses acquiring the substance or purport of any telecommunications message other than by listening or recording.

section 110 of the 1983 Act, or

(iii) under other lawful authority, or

(iv) in the course of and to the extent required by the person's operating duties for or in connection with the installation or maintenance of a line, apparatus or equipment for the transmission of telecommunications messages by An Post.[110]

5.55 Section 13(1) of the *Post Office (Amendment) Act, 1951* makes liable to a penalty any person who:

> "(a) sends any message by telephone which is grossly offensive or of an indecent, obscene or menacing character;
> (b) sends any message by telephone which he knows to be false, for the purpose of causing annoyance, inconvenience, or needless anxiety to any other person; or
> (c) persistently makes telephone calls without reasonable cause and for any such purpose as aforesaid."

5.56 As in the case of An Post, section 110 of the Postal and Telecommunications Services Act, 1983 empowers the Minister for Transport, Energy and Communications to issue directions in writing also to Bord Telecom Éireann.[111] Where a direction involves the interception of a telecommunications message, under the *Interception of Postal Packets and Telecommunications (Regulation) Act, 1993*, an authorisation is required,[112] and as with the interception of postal packets, interception of a telecommunications message is subject to strict conditions and safeguards.[113]

5.57 As in the case of interference with postal packets, a person who intercepts a telecommunications message while acting "under lawful authority" is also exempt from criminal liability under section 98(1) of the 1983 Act.

5.58 The fourth and last exemption protects persons from criminal liability who engage in such conduct in the course of their employment. The exemption is limited to certain types of work (operating, installation or maintenance work); the conduct must occur in the course of this work; and the conduct must be required by the person's duties.

5.59 The four exemptions also apply to an offence under s.98(5) of the *Postal and Telecommunications Services Act, 1983* (as inserted by section 13(3) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993)* which provides:

---

110 Section 98(2).
111 See above para. 5.40.
112 Section 3 of the 1993 Act.
113 See below para. 6.4ff.

"A person who discloses the existence, substance or purport of a telecommunications message that was transmitted by the Minister before the vesting day and intercepted or who uses for any purpose any information obtained from any such message shall be guilty of an offence."[114]

The meaning of telecommunications messages

5.60 Since the offences under s.98 relate to telecommunications messages, it is important that this term be clearly defined. The 1983 Act contains no definition of the term "telecommunications message". As in the case of postal packets, it merely states that, except where the context otherwise requires, "[a]ny word or expression to which a particular meaning is assigned by the *Post Office Acts, 1908* to *1951*, the *Post Office Savings Bank Acts, 1861* to *1958*, or the *Telegraph Acts, 1863* to *1916*" has the same meaning in the 1983 Act.[115]

5.61 The expression "telecommunications message" does not appear in any of these earlier statutes. Rather the expressions used in the Telegraph Acts of the late nineteenth century are "telegraph message",[116] "telegraphic message",[117] "telegraphic communication"[118] and "telephonic communication",[119] the latter two expressions referring to the method or system of communication as well as to what is communicated. The *Telegraph Act, 1868* also refers to the transmission of messages by means of electric or other telegraphs,[120] messages for transmission by telegraph wires,[121] and the transmission of messages by means of the electric telegraph.[122]

5.62 It is interesting to note that the full title of the *Telegraph (Construction) Act, 1908* is "An Act to amend the *Telegraph Acts, 1863* to *1907*, with respect to the Construction and Maintenance of Telegraphic Lines for telephonic and other telegraphic purposes." It would seem therefore that at the turn of the twentieth

---

114 The vesting day was 6 June 1993. An additional offence was inserted in section 98 of the 1983 Act by the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. The offence may only be committed by an employee of Bord Telecom Éireann and comprises disclosure to any person of any information concerning the use made of telecommunications services provided for any other person by the Bord. The offence is not committed where the disclosure is made -

> "(a) at the request or with the consent of [the] other person,
> (b) for the prevention or detection of crime or for the purpose of any criminal proceedings,
> (c) in the interests of the security of the State,
> (d) in pursuance of an order of a court,
> (e) for the purpose of civil proceedings in any court, or
> (f) to another person to whom [the employee] is required, in the course of his duty as such employee, to make such disclosure."

115 Section 22.

116 Sections 9(6)(a) & 17 of the *Telegraph Act, 1868*.

117 Sections 8(3), 9(6)(b) & (9), 18, 20 and 21 of the *Telegraph Act, 1868*; Preamble of the *Telegraph Act, 1869*; and section 2 of the *Telegraph Act, 1878*.

118 Section 16 of the *Telegraph Act, 1868*; and section 2 of the *Telegraph Act, 1878*. See also section 4 of the *Telegraph (Construction) Act, 1908*.

119 Sections 2(1) and 3(1), (2), (4) & (5) of the *Telegraph Act, 1899*.

120 Section 3. See also section 7.

121 Section 9(7).

122 Section 19.

century a telegraphic purpose encompassed a telephonic purpose and that a telephonic communication was regarded as a sub-category of telegraphic communications and likewise a telephonic message as a sub-category of telegraphic messages. This view is confirmed by case law in which it was held that a telephone was a "telegraph" within the meaning of the *Telegraph Acts, 1863* and *1869*, although the telephone had not been invented at the time this legislation was passed: *Attorney-General v. The Edison Telephone Company of London (Ltd.)*.[123] Moreover, although the telephone apparatus in this case involved the passing of an electric current through a telegraphic wire, the Court was of the opinion that any apparatus for transmitting messages by electric signals is a telegraph within the meaning of the Telegraph Acts, whether a wire is used or not.[124] This understanding of the term is important in the era of cord-less and wire-less telephones.

5.63 As regards the meaning of the word "telegraph", it has the same meaning in both the *Telegraph Act, 1869* and the *Telegraph Act, 1884*, and this meaning can be traced back to the definition in the *Telegraph Act, 1863*. Under section 3 of the 1863 Act:

> "The term "Telegraph" means a Wire or Wires used for the purpose of Telegraphic Communication, with any Casing, Coating, Tube or Pipe inclosing the same, and any Apparatus connected therewith for the Purpose of Telegraphic Communication."

The 1869 Act extended the meaning to include "any apparatus for transmitting messages or other communications by means of electric signals".[125] Since wireless telegraphy involves emitting and/or receiving electric energy, a radio message legally constitutes a telegraphic message.

5.64 The phrases "transmission of messages by telephone"[126] and "any message by telephone"[127] appear in the *Post Office (Amendment) Act, 1951*, and there is a reference in the 1983 Act to the section of the 1951 Act in which the latter phrase appears. Such messages are parenthetically described in the reference as "telecommunications messages".[128] It would therefore seem that the drafters of the 1983 legislation understood the term "telecommunications messages" to include messages sent by telephone. Whether the term includes all telegraphic messages is less clear. While an interpretation of the expression "telecommunications messages" as including all telegraphic messages would accord with dictionary definitions of the words "telecommunications", "telegraph" and "telephone" and with the scientific understanding of the term "telecommunications", no legislative definition exists for the purposes of the 1983

---

123 (1880) 6 Q.B.D. 244.

124 (1880) 6 Q.B.D. 244 at 249 and 254. They also thought that any apparatus, of which a wire used for telegraphic communication is an essential part, is a telegraph, whether the communication is made by electricity or not.

125 Section 3.

126 Section 11(1).

127 Section 13(1).

128 Section 98(2)(a)(i).

Act.

5.65 As regards the meaning of the word "message", no definition of the word is found in the Telegraph Acts. Of importance for our inquiry is the question whether the word is to be restrictively interpreted according to the form, content or purpose of a communication or whether it is to be construed broadly to encompass any communication, whatever its form, content or purpose. Dictionary definitions allow of both narrow and broad definitions. It may signify an oral or written communication sent from one person to another[129]: that is, it may be limited to certain forms of communication (oral and written); or it may signify any communication passed or sent between persons.[130]

5.66 A particular difficulty in this regard concerns whether or not telegrams are included in the category of telecommunications messages. Dictionary definitions of the word "telegram" equate it with a telegraphic message or communication[131]; and it is defined in the *Telegraph Act, 1869* as meaning "any message or other communication transmitted or intended for transmission by a telegraph".[132] The word "telegram" would therefore appear to be interchangeable with the terms "telegraphic message" and "telegraphic communication"; and if the expression "telecommunications messages" encompasses "telegraphic messages", then telegrams are included in the category. Moreover, it was held in *Attorney-General v. The Edison Telephone Company of London (Ltd.)* that a conversation held through a telephone is a message, or, at all events, a communication transmitted by a telegraph, and therefore a "telegram" within the meaning of the Telegraph Acts.[133]

5.67 Difficulty arises because the expression "postal packet" is defined in the *Post Office Act, 1908* as including a telegram[134]; and, although the expression in section 63 of the 1983 Act does not include a telegram,[135] the 1908 definition may still apply where the expression is used elsewhere in the Act.[136]

5.68 It seems therefore that between 1869 and 1908 telegrams were telegraphic messages, and that, with the enactment of the *Post Office Act, 1908*, they also entered the category of "postal packets". It might be thought that since a postal packet in section 63 of the 1983 Act does not include a telegram, it was intended that henceforth telegrams should be decoupled from the category of "postal packets" and regarded solely as telegraphic messages" or "telegraphic

---

129 This is one of the meanings of the word given in the *Shorter Oxford English Dictionary*, 3rd rev. ed., 1975.

130 This definition is given in *Webster's New World Dictionary*, 2nd College ed., 1976.

131 See the *Shorter Oxford English Dictionary* and *Webster's New World Dictionary*.

132 Section 3. The *Post Office (Protection) Act, 1884* also contains a definition of the term "telegram" but only for the purpose of section 11 of that Act. This definition is:

> "a written or printed message or communication sent to or delivered at a post office, or the office of a telegraph company, for transmission by telegraph, or delivered by the post office or a telegraph company as a message or communication transmitted by telegraph."

133 (1880) 6 Q.B.D. 244 at 258.

134 Section 89.

135 Section 63(7).

136 See above para. 5.49.

communications". However, although they were decoupled for the purpose of section 63 of the Act, they were not expressly excluded from the category of "postal packets" where the expression appears elsewhere in the Act, and were certainly not expressly included in the category of "telecommunications messages."[137]

5.69 With specific reference to electronic mail, provided a message sent by this form of mail falls within the category of "telecommunications messages", the Act will apply to a message intercepted while it is "being transmitted" by Bord Telecom Éireann[138]; but if the message is intercepted at the personal computer or computer modem stages, an issue arises as to whether at these stages the message can be regarded as "being transmitted" by the Bord. A computer modem is a device which connects a computer to a telecommunications system. It alters the signals emitted from a personal computer and makes them compatible with the signals required for the telecommunications system. Modems and computers are supplied, installed and maintained by persons and companies specialising in the computer field. They are not supplied or controlled by Bord Telecom Éireann. Until a message enters the telecommunications system, it is not being transmitted by the Bord and, similarly, after it leaves the system and enters the computer modem, it is no longer being transmitted by the company - in which cases the Postal and Telecommunications Services Act does not apply.

(xi) The Data Protection Act, 1988

5.70 The *Data Protection Act, 1988* is intended to give effect to Ireland's obligations under the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981.[139] It regulates the collection, processing, keeping, use and disclosure of personal data that is processed automatically. It affords safeguards to individuals with respect to information held about them on computer, which safeguards include a right of access of an individual to information held about that person[140] and to rectification of incorrect information.[141] The Act also established the office of Data Protection Commissioner to oversee compliance with the provisions of the Act.[142] With specific reference to the disclosure of computerised personal

---

137 It is explicitly declared in the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* that the expression "telecommunications message" includes a telegram: see s.1. It may have been intended this should also be understood to be the meaning of the expression in the *Postal and Telecommunications Services Act, 1983.* The relevant sentence of s.1 reads:

> "postal packet' and 'telecommunications message' have the meanings that they have respectively in the Act of 1983, but, for the avoidance of doubt, it is hereby declared that the latter expression includes a telegram."

However, section 1 applies only to expressions "in this Act", i.e. the 1993 Act.

138 Section 98(1).

139 With regard to data protection in Ireland generally see R. Clark, *Data Protection Law in Ireland*, Round Hall Press, Dublin, 1990.

140 Section 4.

141 Section 6.

142 Section 9. Among the powers of the Commissioner is the power to prohibit the transfer of personal data from the State to a place outside the State: section 11.

information, a data controller[143] is under an obligation to keep such data only for one or more specified and lawful purposes and not to use or disclose the data in any manner incompatible with that or those purposes.[144] Also, both a data controller and a data processor[145] are required to take appropriate measures against, *inter alia*, unauthorised access to, or alteration, disclosure or destruction of the data.[146]

5.71 Criminal liability may accrue under the Act where safeguards are not observed. The Act provides that:

> "Personal data processed by a data processor shall not be disclosed by him, or by an employee or agent of his, without the prior authority of the data controller on behalf of whom the data are processed"[147];

and that a person who knowingly discloses data contrary to this provision shall be guilty of an offence.[148] The Act also provides more generally with respect to disclosure following upon unauthorised access that:

> "A person who -
>
> (a) obtains access to personal data, or obtains any information constituting such data, without the prior authority of the data controller or data processor by whom the data are kept, and
> (b) discloses the data or information to another person,
>
> shall be guilty of an offence."[149]

5.72 The Act however also contains an important proviso exempting from the limitations on disclosure imposed by it disclosure in a number of particular circumstances. Section 8 states:

> "Any restrictions in this Act on the disclosure of personal data do not apply if the disclosure is:
>
> (a) in the opinion of a member of the Garda Síochána not below the rank of chief superintendent or an officer of the Permanent Defence Force who holds an army rank not below that of colonel and is designated by the Minister for Defence under this paragraph, required for the purpose of safeguarding the

---

143 The expression "data controller" is defined in section 1(1) of the Act as meaning "a person who, either alone or with others, controls the contents and use of personal data".
144 Section 2(1)(c)(i) & (ii).
145 A "data processor" is defined in section 1(1) of the Act as meaning "a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment".
146 Section 2(1)(d) & (2).
147 Section 21(1).
148 Section 21(2).
149 Section 22(1). This subsection does not apply to a person who is an employee or agent of the data controller or data processor concerned: s.22(2).

security of the State,

(b) required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid,

(c) required in the interests of protecting the international relations of the State,

(d) required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property,

(e) required by or under any enactment or by a rule of law or order of a court,

(f) required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness,

(g) made to the data subject concerned or to a person acting on his behalf, or

(h) made at the request or with the consent of the data subject or a person acting on his behalf."

It is important to note that although these exceptions mean that, for example, a data processor who discloses personal data in one of the listed circumstances without the prior authority of the data controller is exempt from criminal liability under the Act,[150] the Act says nothing about the conditions or circumstances in which disclosure may lawfully be required; in other words, although the discloser will be exempt from liability under the Act in respect of the disclosure, the Act does not specify when a person will be under an obligation to disclose personal data or information for any of the listed purposes. Moreover, although no liability may arise under the Act in such circumstances, liability may arise under other legal or constitutional provisions if disclosure is made where no legal obligation to disclose exists.

5.73 The Act also does not apply to personal data kept by an individual and concerned only with the management of the individual's personal, family or household affairs.[151] The content and purport of electronic mail range, as with other correspondence, over a very broad spectrum from the most intimate and private information to the purely commercial. Personal data is defined by the Act to mean data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller.[152] Such data, even if it relates to the personal affairs of an individual and/or the individual's family or household affairs may not be "concerned only with the management" of these affairs and so may fall within the scope of the Act.

---

150 See section 21.

151 Section 1(4)(c). It also does not apply to personal data kept by an individual only for recreational purposes.

152 Section 1(1).

(xii) The Criminal Damage Act, 1991

5.74 In addition to the safeguards under the *Data Protection Act, 1988* in respect of computerised personal data, unauthorised access to any computerised data may constitute an offence under the *Criminal Damage Act, 1991*. Section 5 of that Act provides:

> "(1) A person who without lawful excuse operates a computer-
>
> (a) within the State with intent to access any data kept either within or outside the State, or
>
> (b) outside the State with intent to access any data kept within the State,
>
> shall, whether or not he accesses any data, be guilty of an offence and shall be liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 3 months or both.
>
> (2) *Subsection (1)* applies whether or not the person intended to access any particular data or any particular category of data or data kept by any particular person."[153]

For the purposes of the Act, a person charged with an offence under section 5 is to be treated as having a lawful excuse if he or she is entitled to consent to or to authorise accessing of the data concerned, or if they believed that the person or persons whom they believed to be entitled to consent to or authorise accessing of the data had consented or would have consented to or authorised the accessing had they known of it.[154] "Data" means information in a form in which it can be accessed by means of a computer and includes a program.[155]

5.75 Since the interception of electronic mail involves accessing computerised data, if a person operates a computer with the intention of intercepting such mail, that person may commit an offence under section 5 if she or he has no lawful excuse for so doing. However, the wording of section 5 requires that the data be "kept" somewhere, and it is possible that data which is being transmitted is not to be regarded as "kept" anywhere. It may be noted in this connection that under the scheme applying to EIRPAC, the Irish National Packet Switched Data Network, operated by Bord Telecom Éireann for the purpose of conveying data by means of telecommunications, a subscriber is responsible for obtaining at her or his own expense all necessary consents from the owners or operators of computers or terminals with which the subscriber wishes to communicate. Provision of service to a subscriber does not give the subscriber or any other

---

153 "Data" is defined in section 1(1) of the Act as meaning information in a form in which it can be accessed by means of a computer and includes a program. Unauthorised access to a computer and the obtaining of information therefrom raise much larger issues than merely the interception of electronic communications or messages. These larger issues were considered by us in our 1992 *Report on the Law Relating to Dishonesty*, LRC 43-1992, in which we recommended the creation of an offence of dishonest use of a computer: see paras. 9.6f. and 29.19-22 & 28 of the *Report*.

154 Section 6(2)(a) & (b).

155 Section 1(1).

person access by right to any computer or terminal to which access is available.[156] The interception of electronic mail by other means than the operation of a computer is not caught by section 5.

5.76 Also, certain forms of surveillance may entail an offence under section 2 of the Act. Under subsection 1 of section 2:

> "A person who without lawful excuse damages any property belonging to another intending to damage such property or being reckless as to whether any such property would be damaged shall be guilty of an offence."

In relation to property other than data, "to damage" includes "to destroy, deface, dismantle or, whether temporarily or otherwise, render inoperable or unfit for use or prevent or impair the operation of".[157] An offence under the subsection is punishable on summary conviction with a fine not exceeding £1,000 or imprisonment for a term not exceeding 12 months or both, and on conviction on indictment with a fine not exceeding £10,000 or imprisonment for a term not exceeding 10 years or both.[158]

5.77 As we have seen, certain forms of telephone tapping involve damage to property, but the damage is usually of a minor kind.[159] Moreover, the installation of a tap may temporarily render inoperable or prevent or impair the operation of a telephone line. With respect to the interception of electronic mail, moving accessed data to another storage medium or to a different location in the storage medium may constitute an offence under section 2(1).

Compensation Orders

5.78 Section 6(1) of the *Criminal Justice Act, 1993* confers on the courts a power, on conviction of any person of an offence, to make a compensation order requiring the offender to pay compensation to any person who has suffered personal injury or loss resulting from the offence.

5.79 Where therefore a person has suffered personal injury or loss as a result of surveillance, and an offence was committed in conducting the surveillance, that person now has a direct financial interest in the outcome of any prosecution for

---

156 S.I. No. 311 of 1984, para. 6(2). The scheme was made by Bord Telecom Éireann in exercise of the powers conferred on it by s.90 of the *Postal and Telecommunications Services Act, 1983*. A similar provision applies to the EIRMAIL Computer Messaging Service operated by or on behalf of Bord Telecom Éireann, in conjunction with Dialcom services networks and facilities outside the State operated by ITT Dialcom Incorporated or its licensees, for the purpose of storing and conveying messages or information in the form of data by means of telecommunications through the medium of such Dialcom systems: see para. 6(3) of S.I. No. 323 of 1985.

157 Section 1(1). "Property" is defined in this subsection as meaning -

> "(a) property of a tangible nature, whether real or personal, including money and animals that are capable of being stolen, and
>
> (b) data."

158 Section 2(5)(a) & (b)(ii).

159 See above para. 5.17.

the offence. Rather than taking an action in tort, the person may prefer to await the outcome of the prosecution and, in case of conviction, seek recompense from the court under this section. Furthermore, as we have shown in the previous chapter, an action in tort may not always be available to the subject of surveillance or it may be uncertain whether the injury suffered by the plaintiff falls within the scope of a particular tort. In particular, given the lack of clarity in the law with respect to the tort of breach of a statutory duty and the legislative proclivity for criminal sanctions in respect of unlawful surveillance, section 6 may afford a surer route for the recovery of damages than the taking of a civil action - provided, of course, there has been a conviction.

5.80 The making of a compensation order is at the discretion of the court.[160] The court may make an order instead of or in addition to dealing with the offender in any other way and unless it sees reason to the contrary. The compensation payable shall be of such amount as the court considers appropriate, having regard to any evidence and to any representations that are made by or on behalf of the offender, the injured party or the prosecution.[161] It may not however exceed the amount of damages that, in the opinion of the court, the injured party would be entitled to recover in a civil action against the convicted person in respect of the injury or loss concerned. In determining both whether to make a compensation order and the amount of any compensation, the court must have regard to the means of the offender;[162] and in assessing the latter's means, must take into account his or her financial commitments.[163]

5.81 The extent to which the courts will afford a remedy under this section in cases of surveillance, as in other cases, awaits elucidation by the courts themselves. While in many cases there will be no real issue as to whether the damage suffered constituted "personal injury or loss", as where physical injury or damage to property is shown, the damage suffered as a result of an invasion of privacy may not always be so readily classifiable as such. Where a conversation between two friends containing intimate personal details of their lives is electronically eavesdropped by a third person on property belonging to a fourth person, the tort of trespass to land will afford neither friend a remedy. There may have been an offence under s.98 of the *Postal and Telecommunications Services Act, 1983*, but the damage to the friends may not have resulted in any tangible or financial loss. The damage may rather have been the affront to their human dignity, and if compensation were to be sought under section 6, an issue might well arise as to whether psychological trauma or mental distress constitutes "personal injury" within the meaning of this legislation. Similarly, if the personal details are revealed by the eavesdropper to others, the result may be a loss of reputation or acute embarrassment for the friends, and there may be an issue as to whether such a result constitutes "personal injury or loss".[164] Moreover,

---

160 See s.6(2).
161 Subject to the legal limits of the court's jurisdiction in tort.
162 Section 6(5).
163 Section 6(13).
164 The meaning of "loss" in a very specific context is dealt with in s.6(12)(a).

there may be an issue as to whether the injury or loss resulted from the offence.[165]

5.82 The Criminal Justice Act addresses the effect of a compensation order on civil proceedings in relation to the injury or loss concerned. Section 9 provides:

> "Where -
>
> (a) a compensation order has been made in favour of a person, and
> (b) damages in respect of the injury or loss concerned fall to be assessed in civil proceedings,
>
> then -
>
> (i) if the damages, as so assessed, exceed any amount paid under the compensation order, the damages awarded shall not exceed the amount of that excess, and
>
> (ii) if any amount paid under the compensation order exceeds the damages, as so assessed, the court may order that the amount of the excess be repaid by that person to the person against whom the compensation order was made,
>
> and, upon the award of damages or, as the case may be, the making of the order by the court, the compensation order shall cease to have effect."

Conclusion

5.83 A certain amount of surveillance activity is penalised by the law, as is the unauthorised disclosure of information obtained by means of surveillance. Often however surveillance activity is not penalised as such but is caught by offences designed to protect values other than privacy such as property, e.g. offences of malicious damage. Several offences, as e.g. eavesdropping, bear the imprint of an earlier age when surveillance meant personal snooping rather than the use of sophisticated listening and optical devices. Some surveillance activities are specifically targeted by legislation for criminal sanction. Principal among these are the interception of post and telecommunications and the accessing of computerised data; but there are clear gaps, the most obvious perhaps being the lack of any criminal sanction applying specifically to video surveillance. Also, the criminal sanctions applicable to the use of listening devices other than in the context of the interception of a telecommunications message in the course of

---

165 Section 6(3) specifically provides that where the commission of the offence involved the taking of property, any loss arising from damage to the property, howsoever and by whomsoever caused, shall be treated as having resulted from the offence.

transmission by Bord Telecom Éireann are weak.

5.84 Where offences exist, there is some overlap. For example, the disclosure of the purport of a telegram by a person in the employment of Bord Telecom Éireann may constitute an offence under both s.11 of the *Post Office (Protection) Act, 1884* and under s.98(1) of the *Postal and Telecommunications Act, 1983*. In addition, the same surveillance activity may constitute more than one discrete offence, e.g. use of a radio scanner to intercept a mobile telephone conversation may constitute an offence under both s.98(1) of the 1983 Act and, because of licence requirements, wireless telegraphy legislation. This isn't necessarily undesirable, but sometimes protection, though substantial, is unsatisfactory. In particular, the legislation criminalising other than in certain circumstances the interception of post and telecommunications uses the terms "postal packets" and "telecommunications messages", for neither of which there is a clear definition.

5.85 Finally, the power of a court to make a compensation order in the context of a criminal conviction may afford a person who has suffered personal injury or loss as a result of the offence some satisfaction, but the injury suffered in cases of surveillance will probably often not be of either kind. Moreover, the possibility that a judge may exercise this power in a criminal case cannot substitute for adequate civil remedies.

CHAPTER 6: STATE INTERCEPTION OF COMMUNICATIONS

Introduction

6.1 It is generally accepted that there are some circumstances in which state authorities should be permitted, in the common interest, to exercise special powers denied to the ordinary citizen. Such powers include the interception of communications.

6.2 Until recent years the power of the State to interfere with correspondence did not rest on any clear legal basis. It was exercised for many years purely as a matter of practice. In line with pre-independence British practice, the Minister for Justice would issue a warrant authorising interception and the interception would be carried out by staff of the Department of Posts and Telegraphs. In 1983, this practice was put on a legislative basis. The *Postal and Telecommunications Services Act* empowered the Minister for Posts and Telegraphs[1] to issue directions to An Post and Bord Telecom Éireann "to do (or refrain from doing) anything which he may specify from time to time as necessary in the national interest".[2] It is under this provision that State interception of correspondence has subsequently been conducted. The provision does not explicitly refer to such a power. Nor is it explicit as to the precise grounds on which such a direction may be given or subject a direction to any conditions. Rather the provision states merely that a direction should be prompted by the national interest as perceived by the Minister. Although some safeguards existed in practice against abuse of the power of interception, as the case of *Kennedy and Arnold v. Ireland*[3] shows, these were inadequate to prevent abuse. In 1993, therefore, the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act* was passed to rectify this situation.

---

1 Now the Minister for Transport, Energy and Communications.

2 Section 110.

3 [1987] I.R. 587, [1988] I.L.R.M. 472. See above paras. 3.18-3.19 concerning this case.

6.3 In this Chapter we will examine this legislation. The Act affords recognition to the value of privacy in relation to communications. It requires authorisation by the Minister for Justice before a direction to intercept may be issued under s.110 of the 1983 Act,[4] and among the matters to which the Minister must give some thought before giving an authorisation is the importance of preserving the privacy of postal packets and telecommunications messages.[5]

The Interception Of Postal Packets And Telecommunications Messages Under The 1993 Act

6.4 For years an administrative practice was followed whereby the Minister for Justice issued warrants in certain circumstances for the interception of postal packets and telecommunications messages. The practice was described thus by the State in complying with its obligations under Article 40 of the International Covenant on Civil and Political Rights,

> "Warrants authorising the interception of telephone conversations or the opening of letters can be issued by the Minister for Justice and implemented under general directions given by the Minister for Communications under section 110 of the *Postal and Telecommunications Act, 1983*. Warrants are issued only where they are certified to be required for security purposes or for the prevention or detection of serious crime, information as to which can be got in no other way. In the case of an application by the police for a warrant, the Garda Commissioner must certify that the necessary conditions have been fulfilled. An application from the military authorities must be certified by the Director of Military Intelligence and backed personally by the Minister for Defence. A warrant remains in force for three months unless renewed on the same conditions as applied to the original warrant."[6]

6.5 The State's international obligations required that this practice be put on a legislative basis and that the legislation contain safeguards against the arbitrary interception of communications.[7] The result was the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*, which is designed to protect the privacy of correspondence by limiting the circumstances in which a person's communications may lawfully be intercepted and subjecting interception to strict conditions and safeguards.

6.6 A "communication" is defined under the Act as meaning a postal packet or a telecommunications message,[8] and

---

4 Section 3 of the 1993 Act.
5 Sections 2(3), 4(b) and 5(e) of the 1993 Act.
6 Paragraph 170 of the *First Report* by Ireland on the measures adopted to give effect to the provisions of the Covenant, 1992. See further below paras. 7.51-7.52.
7 See below paras. 7.29-7.36.
8 Section 1.

"interception" as -

"(a) an act -

(i) that consists of the opening or attempted opening of a postal packet addressed to any person or the delaying or detaining of any such postal packet or the doing of anything to prevent its due delivery or the authorising, suffering or permitting of another person (who is not the person to whom the postal packet is addressed) to do so, and

(ii) that, if done otherwise than in pursuance of a direction under section 110 of the Act of 1983, constitutes an offence under section 84 of that Act,

or

(b) an act-

(i) that consists of the listening or attempted listening to, or the recording or attempted recording, by any means, in the course of its transmission, of a telecommunications message, other than such listening or recording, or such an attempt, where either the person on whose behalf the message is transmitted or the person intended to receive the message has consented to the listening or recording,

and

(ii) that, if done otherwise than in pursuance of a direction under section 110 of the Act of 1983, constitutes an offence under section 98 of that Act".[9]

This definition of interception in relation to postal packets is clearly modelled on section 84 of the 1983 Act, and in fact accords with those offences specified in section 84(1)(a) of the Act.[10] In relation to telecommunication messages, the definition accords with the new definition of "intercept" under the 1983 Act and the offences specified in section 98(1) of that Act.[11]

6.7 The 1993 Act provides that the expressions "postal packet" and "telecommunications message" "have the meaning that they have respectively in

---

9 *Ibid.* Cognate words shall be construed accordingly.
10 See above para. 5.37.
11 See above para. 5.52.

the Act of 1983".[12] We have seen that neither expression is defined in the 1983 Act, and that it is unclear whether or not telegrams were included in the category of "telecommunications messages" under the 1983 Act.[13] So, "for the avoidance of doubt", it is declared that, in the 1993 Act, the expression "telecommunications message" includes a telegram.[14]

6.8 Section 3 of the 1993 Act provides:

> "A direction under section 110 of the Act of 1983 requiring an interception shall not be issued or remain in force unless there is in force an authorisation relating to the interception or the direction is a general one requiring an interception if and for so long as an authorisation is in force."

The special régime established by the Act in relation to the interception of communications only applies therefore to interceptions required by a direction under section 110 of the 1983 Act.

6.9 In accordance with the former practice, the Minister for Justice is empowered by the Act to give an authorisation, but the purposes for which an authorisation may be given are strictly limited and specified. An authorisation may only be given for two purposes, namely, for the purpose of criminal investigation or in the interests of the security of the State.[15] Moreover these are not blanket purposes, but are narrowed considerably by the requirement that a number of further conditions be fulfilled.

6.10 In relation to the investigation of crime, these conditions are:

> "(a) (i) that -
>
> (I) investigations are being carried out by the Garda Síochána, or another public authority charged with the investigation of offences of the kind in question, concerning a serious offence or a suspected serious offence,
>
> (II) investigations not involving interception have failed, or are likely to fail, to produce, or to produce sufficiently quickly, either or, as the case may be, both of the following, that is to say:
>
> (A) information such as to show whether

12 Section 1.
13 See above paras. 5.66-5.68.
14 Section 1.
15 Section 2(1).

the offence has been committed or as to the facts relating to it,

(B) evidence for the purpose of criminal proceedings in relation to the offence,

and

(III) there is a reasonable prospect that the interception of postal packets sent to a particular address or of telecommunications messages sent to or from a particular telecommunications address would be of material assistance (by itself or in conjunction with other information or evidence) in providing information, or evidence, such as aforesaid,

or

(ii) that -

(I) in the case of a serious offence that is apprehended but has not been committed, investigations are being carried out, for the purpose of preventing the commission of the offence or of enabling it to be detected, if it is committed, by the Garda Síochána or another public authority charged with the prevention or investigation of offences of the kind in question,

(II) investigations not involving interception have failed, or are likely to fail, to produce, or to produce sufficiently quickly, information as to the perpetrators, the time, the place, and the other circumstances, of the offence that would enable the offence to be prevented or detected, as the case may be, and

(III) there is a reasonable prospect that the interception of postal packets sent to a particular address or of a telecommunications message sent to or from a particular telecommunications address would be of material assistance (by itself or in conjunction with other information) in preventing or detecting the offence, as the case may be,

and

(b) that the importance of obtaining the information or evidence concerned is, having regard to all the circumstances and notwithstanding the importance of preserving the privacy of postal packets and telecommunications messages, sufficient to justify the interception.[16]

The power to authorise an interception therefore covers both the prevention of crime and the detection of crime which has been committed, but only if the crime constitutes a serious offence. A "serious offence" is an offence for which a person aged 21 years or over, of full capacity and not previously convicted may be punished by imprisonment for a term of 5 years or more and must fall within 1 of 3 categories. It must (i) involve loss of human life, serious personal injury or serious loss of or damage to property or a serious risk of any such loss, injury or damage, or (ii) result or be likely to result in substantial gain, or (iii) the facts and circumstances must be such as to render it a specially serious case of its kind.[17] Acts or omissions done or made outside the State are covered if they would fall within the definition of a serious offence if done or made in the State.[18]

6.11 In relation to the security of the State, the conditions which must be fulfilled are:

"(a) that there are reasonable grounds for believing that particular activities that are endangering or likely to endanger the security of the State are being carried on or are proposed to be carried on,

(b) that investigations are being carried out by or on behalf of the person applying for the authorisation concerned to ascertain whether activities of the kind aforesaid are in fact being carried on or proposed to be carried on and, if so, by whom and their nature and extent,

(c) that investigations not involving interception have failed, or are likely to fail, to produce, or to produce sufficiently quickly, information that would show whether the activities are being carried on or proposed to be carried on and, if so, by whom and their nature and extent,

(d) that there is a reasonable prospect that the interception of postal packets sent to a particular postal address or of telecommunications messages sent to or from a particular

---

16 Section 4.
17 Section 1.
18 *Ibid.*

telecommunications address would be of material assistance (by itself or in conjunction with other information) in providing information such as aforesaid, and

(e) that the importance of obtaining the information concerned is, having regard to all the circumstances and notwithstanding the importance of preserving the privacy of postal packets and telecommunications messages, sufficient to justify the interception."[19]

6.12 The number of persons who may request an authorisation from the Minister for Justice is also strictly limited by the Act. Only the Commissioner of the Garda Síochána may apply for an authorisation for the purpose of criminal investigation.[20] In the case of an authorisation in the interests of the security of the State, the application must be made by either the Garda Commissioner or the Chief of Staff of the Defence Forces[21]; and, in the latter eventuality, the application must be accompanied by a recommendation in writing of the Minister for Defence supporting it.[22]

6.13 All applications must be made in writing and sent or given to an officer of the Minister for Justice specifically nominated by the Minister for the purposes of the Act ("the nominated officer").[23] They must contain sufficient information to enable the Minister to determine whether or not the required conditions for the giving of an authorisation are fulfilled.[24] The application is examined in the first instance by the nominated officer who considers whether the conditions have in fact been fulfilled and may make any necessary inquiries in this regard. The officer then makes a submission to the Minister indicating whether or not, in the opinion of the officer, the conditions stand fulfilled and, if not, the respects in which they do not appear to be fulfilled.[25] The submission must be signed by the nominated officer.[26] In the absence of the nominated officer, the officer's duties may be discharged by another officer designated by the Minister for this purpose.[27]

6.14 Authorisation is by way of a warrant given under the hand of the Minister[28]; and the Minister shall not give an authorisation unless satisfied that the conditions are fulfilled for interception for the purpose of a criminal investigation or in the interests of the security of the State, as the case may be, and that the requirements in relation to an application have been complied with.[29] What the warrant should contain is specified in the Act. The warrant -

---

19 Section 5.
20 Section 6(1)(a)(i).
21 Section 6(1)(a)(ii).
22 Section 6(1)(c).
23 Section 6(1)(a).
24 Section 6(1)(b).
25 Section 6(2).
26 *Ibid.*
27 Section 6(4).
28 Section 2(2)(a).
29 Section 2(3).

"(a) shall bear the date on which the authorisation to which it relates is given,

(b) shall state -

(i) whether the proposed interception is in relation to postal packets or telecommunications messages or both, and

(ii) that the requirements of [the] Act in relation to the giving of the authorisation to which the warrant relates have been complied with,

(c) shall specify -

(i) the postal address to which and (unless the Minister considers that to restrict the authorisation to which the warrant relates to a specified person or persons would be prejudicial to the purposes of the proposed interception) the person or persons to whom the proposed interception relates, or

(ii) the telecommunications address to which the proposed interception relates,

or, where appropriate, the matters specified in both *subparagraphs (i) and (ii)* of this paragraph, and

(d) may require the person to whom it is addressed to disclose the intercepted material to such persons as are specified in the warrant.[30]

6.15 An authorisation remains in force for 3 months[31] unless either the Garda Commissioner of the Chief of Staff of the Defence Forces considers that interceptions to which an authorisation relates are no longer required[32] or the judge appointed to review the operation of the Act thinks an authorisation should be cancelled.[33] An authorisation may be extended for further periods not exceeding 3 months each, which means that there is a ministerial check at least every 3 months on the continuance of an authorisation.[34] The extension of an authorisation is in general subject to the same requirements as apply to the initial authorisation.[35] In case of exceptional urgency, an initial or an extended authorisation may be given orally by the Minister, but if so given, it must be

---

30 Section 2(4).
31 Section 2(5).
32 Section 7.
33 Section 8(6). See further below para. 6.19.
34 Section 2(5) & (6)(a).
35 Section 2(6)(b).

confirmed, as soon as may be, by warrant.[36]

6.16 Issues of compliance with the requirements relating to an authorisation are by and large excluded from the jurisdiction of the courts and entrusted to two other independent forms of scrutiny.

6.17 First, the Act provides for the designation of a High Court judge ("the designated judge") who "shall have the duty of keeping the operation of [the] Act under review, of ascertaining whether its provisions are being complied with and of reporting to the Taoiseach."[37] While the judge may report to the Taoiseach from time to time on any matter relating to the Act, he or she must report at least once every twelve months on the general operation of the Act.[38] The judge may also communicate with the Taoiseach or Minister for Justice on any matter concerning interceptions.[39] The Taoiseach shall cause a copy of a report by the judge to be laid before each House of the Oireachtas[40]; but if, after consultation with the judge, the Taoiseach considers that the publication of any matter in a report would be prejudicial to the prevention or detection of crime or to the security of the State, that matter may be excluded from the laid copy, in which case a statement that the matter has been excluded must accompany the copy.[41] Furthermore, before deciding whether or not to give an authorisation or an extension in any particular case or in a case of any particular class, the Minister for Justice may consult the designated judge.[42] The judge also plays a supplementary role in the operation of the second form of independent scrutiny with respect to the determination whether an offence is a serious one or not.[43]

6.18 The Act confers on the designated judge the power to investigate any case in which an authorisation has been given,[44] and provides that the judge shall have access to and may inspect any official documents relating to an authorisation or an application for an authorisation.[45] The Act further requires that persons give to the designated judge, upon request, any information in their possession relating to an application for an authorisation or to an authorisation itself.[46]

6.19 After first informing the Minister for Transport, Energy and Communications, the Minister for Justice shall cancel an authorisation -

> "[i]f the designated judge informs the Minister [for Justice] that he considers that a particular authorisation that is in force should not have been given or (because of circumstances arising after it had been given)

---

36 Section 2(2)(b), (c) & (6)(b).
37 Section 8(1). Mr. Justice Declan Costello has been appointed as the first designated judge.
38 Section 8(2).
39 Section 8(4).
40 Section 8(7).
41 Section 8(7) & (8).
42 Section 2(7).
43 Section 9(6). See below paras. 6.24-6.25.
44 Section 8(3)(a).
45 Section 8(3)(b).
46 Section 8(5).

should be cancelled or that the period for which it was in force should not have been extended or further extended."[47]

6.20 While the judge who fulfils these functions is designated by the Government,[48] the independence of this form of scrutiny of authorisations is assured by the method of nomination of the judge and by the fact that the person designated continues to serve as a judge of the High Court. The Act requires that the invitation to undertake the duties of designated judge issue from the President of the High Court after consultation with the Minister for Justice. It is therefore the President of the High Court who issues the invitation and, if the invitation is accepted, the Government shall designate that person for the purposes of the Act.[49] Furthermore, although no term of office is prescribed in the Act for the designated judge, the tenure of judges of the High Court is constitutionally protected. They may not be removed from office except for stated misbehaviour or incapacity, and then only upon resolutions passed by Dáil Éireann and by Seanad Éireann calling for their removal.[50] Nor may their remuneration be reduced during their continuance in office as a High Court judge.[51]

6.21 The second form of independent scrutiny is afforded by the Complaints Referee ("the Referee"). The Act provides for the establishment of the office of Complaints Referee and that the person appointed shall be a judge of either the Circuit or the District Court or a practising barrister or solicitor of not less than 10 years' standing.[52] Appointment is by the Taoiseach for a term of 5 years, which is renewable.[53]

6.22 Persons who believe that a communication sent to or by them has been intercepted in the course of its transmission by An Post or Bord Telecom Éireann may apply to the Referee for an investigation into the matter.[54] Unless the application appears to the Referee to be frivolous or vexatious, the Referee shall investigate whether there has been any contravention of a number of provisions of the Act in relation to the authorisation.[55] These provisions are those relating to applications for an authorisation,[56] the issuing and, where relevant, the extension of an authorisation,[57] the cesser of interceptions when the Garda Commissioner or the Chief of Staff of the Defence Forces (as

---

47 Section 8(6).
48 Section 8(1).
49 *Ibid.*
50 Constitution, Article 35.4.1°.
51 Constitution, Article 35.5. See also Art. 35.2 & 3.
52 Section 9(2)(a) & (b).
53 Section 9(2)(c). Judge Esmond Smyth of the Circuit Court was appointed Complaints Referee in April 1994.
54 Section 9(3). Although the *Postal and Telecommunications Services Act, 1983* provided for the establishment of a separate Users' Council for both An Post and Bord Telecom Éireann and one of the functions of these Councils is to consider any complaint or representation made to it by or on behalf of a user of the relevant services, consideration of any matter relating to public order or security was expressly excluded from their functions: see sections 48 and 49(1)(a) & (2). Moreover, the Act also provided that neither An Post nor Bord Telecom Éireann shall be required to advise its Users' Council of any plans or projected developments which relate to public order or security: see section 49(9).
55 Section 9(4).
56 Section 6.
57 Section 2.

appropriate) is of the view that interception is no longer required,[58] and the cancellation of an authorisation at the initiative of the designated judge.[59]

6.23 If the Referee, after investigation, concludes that there has been a contravention of any of these provisions, the Referee must notify the applicant in writing of that conclusion and make a report thereon to the Taoiseach.[60] The Referee may also, at his or her discretion, by order do one or more of three things. The Referee may (i) quash the relevant authorisation, (ii) direct the destruction of any copy of the communications intercepted pursuant to the authorisation, (iii) make a recommendation for the payment to the applicant of such sum by way of compensation as may be specified in the order.[61] Should the Referee recommend payment of a sum of money by way of compensation, the Minister for Justice is legally obliged to implement this recommendation.[62]

6.24 If the Referee concludes that there has been no contravention of any of the relevant provisions, the general position is that he or she shall give notice in writing to the applicant stating only that there has been no contravention of the provisions.[63] This general position is qualified in that should the Referee conclude that, although there has been no contravention, the offence concerned was not a serious offence within the meaning of the Act, then the Referee must refer the question whether the offence was a serious one or not to the designated judge for the latter's determination and must give the Minister for Justice prior notice of the referral.[64]

6.25 If the designated judge is of the view that the offence was serious, the Referee must give notice in writing to the applicant stating only that there has been no contravention of the specified statutory provisions.[65] However, if the designated judge also does not regard the offence as serious, then the Referee is placed under the same duties of notification to the applicant and of reporting to the Taoiseach and enjoys the same powers in respect of making an order as in the case of a contravention.[66] Likewise, should the Referee by order recommend the payment of a sum of money by way of compensation to the applicant, the Minister for Justice must implement the recommendation.[67]

6.26 As in the case of the designated judge, the Act provides that the Referee shall have access to and may inspect any relevant official documents,[68] and that persons shall cooperate with the Referee by affording him or her, on request, any relevant information in their possession.[69]

---

58 Section 7.
59 Section 8(6).
60 Section 9(5)(a) & (b).
61 Section 9(5)(c).
62 Section 9(12).
63 Section 9(8).
64 Section 9(6).
65 Section 9(6)(b).
66 Section 9(6)(a).
67 Section 9(12). See also s.9(7).
68 Section 9(10).
69 Section 9(11).

6.27 Provision is also made in the Act for the independence of the Complaints Referee. Although the Referee is appointed and may be removed from office by the Taoiseach, removal from office may only occur for stated misbehaviour or incapacity and upon resolutions passed by Dáil Éireann and by Seanad Éireann calling for the person's removal.[70]

6.28 All official documents relating to an authorisation and an application for an authorisation must be retained for a period of at least 3 years from the date on which the authorisation ceases to be in force.[71] This requirement to retain official documents for a minimum period does not apply to copies of a communication intercepted pursuant to an authorisation.[72] The Act does however seek to limit the number of such copies and to procure their destruction once they are no longer needed. It provides that the Minister for Justice shall ensure that such arrangements as he or she considers necessary exist to secure that such copies are not made to any extent greater than is necessary and are destroyed as soon as their retention is no longer necessary.[73] "Necessary" in this context is stated to mean necessary for the purpose of the prevention or detection of serious offences or in the interests of the security of the State. The Act does not require the destruction at any stage of other official documents relating to authorisations and applications. It does however provide, as in the case of copies, that the Minister for Justice shall ensure that such arrangements as he or she considers necessary exist to limit to the minimum necessary the disclosure of the fact an authorisation has been given and the contents of any intercepted communication.[74] "Necessary" has the same meaning in relation to disclosure as in relation to the making and destruction of copies.[75]

6.29 The Act further states that a contravention of specified provisions (relating to the authorisation of interceptions,[76] applications for authorisations,[77] the cesser of interceptions[78] or the cancellation of an authorisation upon information supplied by the designated judge[79]) or a failure to fulfil any of the specific conditions relating to an interception for the purpose

---

70 Section 9(2)(f). With respect to the remuneration and other terms and conditions of the office, the Act provides:

> 'Subject to the provisions of this subsection, the terms and conditions, including terms and conditions relating -
>
> (i) except in a case where the Referee is a judge of the Circuit Court or a judge of the District Court, to remuneration, and
>
> (ii) to allowances for expenses,
>
> upon which the Referee shall hold office shall be such as may be determined by the Minister, with the consent of the Minister for Finance, at the time of his appointment or reappointment.'

71 Section 11(1).
72 Section 11(2).
73 Section 12(1)(b).
74 Section 12(1)(a).
75 Section 12(2).
76 Section 2.
77 Section 6.
78 Section 7.
79 Section 8(6).

of criminal investigation or in the interests of the security of the State[80] "shall not of itself render the authorisation invalid or constitute a cause of action at the suit of a person affected by the authorisation."[81] It is clearly intended that any alleged contravention of these provisions or conditions be subject to investigation by the Complaints Referee rather than to adjudication in the courts, and it is specifically provided that a decision of the Referee on these matters shall be final.[82] There is however an express saver in respect of the constitutional jurisdiction of the courts. Nothing in the relevant subsection "shall affect a cause of action for the infringement of a constitutional right".[83] Moreover, an alleged contravention of any other provision of the Act, including the provisions relating to the Complaints Referee, is not excluded from adjudication by the courts.

Conclusion

6.30 State interception of communications is now subject to extensive regulation by law. The scope of this law is however limited in two important respects.

6.31 First, the legislation regulating the interception of post and telecommunications is based on premises which are gradually being eroded by economic and technological developments. Interception is conducted by employees of An Post and Bord Telecom Éireann, the two companies which, in 1983, took over these services from the Department of Posts and Telegraphs. Yet deregulation of postal and telecommunications services means that persons and bodies other than An Post and Bord Telecom Éireann are already offering such services to the public. Post and telecommunications conveyed by these persons and bodies fall outside the scheme provided for by the 1993 Act.

6.32 Secondly, the legislation deals only with the interception of post and telecommunications. Other forms of State surveillance are not specifically regulated by law. For example, listening devices designed to pick up face-to-face conversations are not included within the ambit of the Act, nor are optical devices. No special legislative provision has been made for the use of such devices by state authorities whether in the interests of national security, for the prevention and detection of crime, or for any other purpose. Their use is relatively unregulated by law.

---

80 Sections 4 and 5.
81 Section 9(1).
82 Section 9(9).
83 Section 9(1).

PART 3: THE INTERNATIONAL DIMENSION

CHAPTER 7: INTERNATIONAL STANDARDS AND OBLIGATIONS

Introduction

7.1 There are a number of international instruments and regulations which deal with privacy and some of these require safeguards in respect of the threat to privacy posed by surveillance. We are aware of these internationally agreed standards and of the State's obligations in this regard and, in our review of the relevant Irish law and practice, are concerned that these standards and obligations should be taken fully into account, and that any recommendations we make for reform of the law in this area should be consistent therewith.

7.2 Principal among the State's international obligations are those arising from its membership of the European Union. By virtue of Article 29.4.5° of the Constitution, no provision thereof prevents laws enacted, acts done or measures adopted by the European Union from having the force of law in the State.[1] Special regard should therefore be had, where relevant, to any such laws, acts and measures; and we will first consider the extent to which European law and policy impose restraints upon the State's freedom of action in relation to surveillance and the extent to which they afford markers for the development of the law in this area.

7.3 Secondly, we will have regard to the State's international human rights obligations, especially those relating to the protection of privacy. Of particular significance are the relevant provisions of the European Convention on Human Rights and of the International Covenant on Civil and Political Rights, to both of which treaties Ireland is party and which prescribe standards for the

---

1 This also applies to laws, acts and measures adopted by the European Communities or by institutions of the European Union or the Communities, or by bodies competent under the Treaties establishing the Communities. Article 29.4.5° further provides that no provision of the Constitution "invalidates laws enacted, acts done or measures adopted by the State which are necessitated by the obligations of membership of the European Union or of the Communities".

promotion of human dignity and worth, the former at the regional level in Europe and the latter at the global level.

7.4 Lastly, we will consider the State's obligations flowing from its membership of two intergovernmental organisations whose remit it is to co-ordinate and to oversee two forms of communication between states, that is, telecommunications and the post. The former is the concern of the International Telecommunication Union and the latter of the Universal Postal Union.

Membership Of The European Union

7.5 Ireland's membership of the European Union is of profound significance for certain areas of Irish law and policy.[2] Not only are some of Ireland's obligations as a member of the Union expressly afforded priority by the Constitution over national law, but the Union is the forum in which policy and the future law on matters covered by the Union are decided.

7.6 The free movement of goods and services among the Member States is a fundamental principle of the Union. This freedom is however not unlimited. Certain restrictions are permitted provided they comply with Community law.

7.7 Title I of the EEC Treaty governs the free movement of goods and provides for the elimination of quantitative restrictions[3] on imports and exports between Member States. Prohibitions on imports, exports or goods in transit are however still permitted:

> ... on grounds of public morality, public policy or public security; the protection of health and life of humans, animals or plants; the protection of national treasures possessing artistic, historic or archaeological value; or the protection of industrial and commercial property",[4]

provided they do not "constitute a means of arbitrary discrimination or a disguised restriction on trade between Member States."[5] Moreover, Member States are required to adjust any state monopolies of a commercial character so that no discrimination regarding the conditions under which goods are procured and marketed exists between nationals of Member States.[6]

7.8 The free trade in surveillance devices, as in other goods, may therefore be restricted on any of the listed grounds, most notably on the grounds of public

---

2 See further above para. 2.10ff.

3 And all measures having equivalent effect: Arts. 30 & 34.

4 Art. 36 of the EEC Treaty.

5 *Ibid.*

6 Art. 37(1) of the EEC Treaty, which further provides -

> "The provisions of this Article shall apply to any body through which a Member State, in law or in fact, either directly or indirectly supervises, determines or appreciably influences imports or exports between Member States. These provisions shall likewise apply to monopolies delegated by the State to others."

morality, public policy, public security and the protection of the health of human beings, provided the restriction is not discriminatory and does not constitute a disguised restriction on trade between Member States. Accordingly under EU law Ireland is permitted to ban imports of a particular device on any of these grounds within the specified limits. As to state monopolies of a commercial character, although Ireland, as indeed most other European states, still controls the public postal and telecommunications networks, the market in telecommunications equipment has been liberalised as the variety of handsets readily available on the market illustrates.[7]

7.9 The freedom to provide services is guaranteed by Chapter 3 of Title III of the EEC Treaty. This freedom is enjoyed by nationals of Member States who are established in a State of the Community other than that of the person for whom the services are intended.[8] We have already noted the gradual liberalisation of postal and telecommunications services which, though not complete, is well-advanced and can be expected to continue for the foreseeable future.

7.10 In the postal and telecommunications sectors, a situation is fast emerging where the State retains control of the public network or infrastructure while allowing access thereto and the provision of postal and telecommunications services by a number of private actors. Such access and provision may be regulated in order, for example, to ensure that there is no harmful interference with radio frequencies and that services are available at a reasonable cost to persons in outlying areas of the Union. The Member States and institutions of the Union have shown an awareness and a concern over the threats to privacy posed by the economic and technological developments in the postal and telecommunications fields and action with a view to harmonizing the divergent laws of member States in order to protect confidentiality, secrecy and privacy in these fields has been set in train.

7.11 In a 1986 Recommendation on the co-ordinated introduction of the integrated services digital network (ISDN) in the European Community, the Council specified that "the implementation of such policy should pay proper attention to user privacy protection"[9]; and three years later, in 1989, in a Resolution on the strengthening of co-ordination for the introduction of ISDN in the Community, it re-emphasised the importance of the protection of personal data and privacy because of the increased threats to privacy arising from the greater functionality of digital switches and networks.[10] In a number of

---

7 See above para. 2.13.

8 Art. 59, which, as amended by Art. 16(3) of the Single European Act, also provides -

> "The Council may, acting on a qualified majority on a proposal from the Commission, extend the provisions of the Chapter to nationals of a third country who provide services and who are established within the Community."

See also Arts. 56 & 60.

9 Recommendation 86/659/EEC, 22 December 1986, Preamble.

10 Resolution of 18 July 1989.

subsequent Directives, it has addressed the particular grounds on which access to a network may be denied or regulated and privacy considerations are either explicitly or implicitly included among these grounds. For example, a 1990 Directive on the establishment of the internal market for telecommunications services through the implementation of open network provision, states:

> "Open network provision conditions must not restrict access to public telecommunications networks or public telecommunications services, except for reasons based on essential requirements within the framework of Community law"[11];

and these reasons are then itemised and include the "security of network operations" and the "protection of data, as appropriate."[12] The Council has also addressed the extent to which access to networks and use of services may be restricted in a number of Recommendations. Thus, in 1992, in a Recommendation on the harmonized provision of a minimum set of packet-switched data services (PSDS) in accordance with open network provision (ONP) principles, it noted that:

> "... Member States may restrict use and provision of PSDS to the extent necessary to ensure compliance with the regulations on the protection of data, including protection of personal data, the confidentiality of information transmitted or stored and the protection of privacy compatible with Community law."[13]

In the same year, in a Recommendation on the provision of harmonized ISDN access arrangements and a minimum set of ISDN offerings in accordance with ONP principles, it adverted not only to the fact that restrictions may be justified on the grounds, *inter alia*, of essential requirements but also to the permissible scope of restrictions where legitimate grounds exist:

> "... Member States may restrict use of ISDN to the extent necessary to ensure compliance with regulations on the protection of data, including protection of personal data, the confidentiality of information transmitted or stored, as well as the protection of privacy compatible with Community law; ... those restrictions should be objectively justified, follow the principle of proportionality and not be excessive in relation to the aim pursued."[14]

---

11 Art. 3(2) of Directive 90/387/EEC, 28 June 1990.

12 The other reasons are the maintenance of network integrity and the interoperability of services, in justified cases. In addition, the conditions generally applicable to the connection of terminal equipment to the network shall apply. Also, the open network provision conditions must comply with a number of basic principles, namely, they must be based on objective criteria, they must be transparent and published in an appropriate manner, they must guarantee equality of access and must be non-discriminatory, in accordance with Community law: Art. 3(1). See also Art. 3(3). Article 3(5) provides that the rules for uniform application of the essential requirements in Member States shall be determined, where appropriate, by the Commission, in accordance with a procedure laid down in Art. 10. The manner in which the essential requirements specified in Art. 3(2) of this Directive shall apply to leased lines was subsequently laid down in Art. 6(3) of Directive 92/44/EEC, 5 June 1992.

13 Recommendation 92/382/EEC, Preamble.

14 Recommendation 92/383/EEC, 5 June 1992, Preamble.

7.12 With specific reference to the protection of personal data, a Directive has been passed on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[15] It is designed to achieve a proper balance between the free flow of personal data from one member State to another and the protection of the fundamental rights of individuals, notably the right to privacy.[16] The difference in the levels of protection of privacy with regard to the processing of personal data in Member States is seen as an obstacle to the pursuit of a number of economic activities at Community level, and co-ordination of the relevant laws of Member States as vital to the internal market.[17] The protection principles contained in the Directive applies to the processing of personal data by any person whose activities are governed by Community law. Specifically excluded however from the scope of the Directive is the processing of sound and image data, as in cases of video surveillance:

> "... if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law."[18]

Furthermore, where the processing of personal data is carried out for purposes of journalism or of literary or artistic expression, the principles of the Directive apply in a restricted manner according to the provisions laid down in Article 9.[19] Article 9 is headed "Processing of personal data and freedom of expression", and addresses the balance to be drawn between freedom of information and the protection of personal data in the context of journalism. It provides:

> "Member States shall provide for exemptions or derogations ... for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression."[20]

Also of interest in the context of this Paper is Article 17 which deals with the security of processing.[21] Under this Article, Member States are required to

---

15 Directive 95/46/EC of 24 October 1995; (1995) OJ L 281.

16 Art. 1 of the Directive deals with the object of the Directive and reads:

> "1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded pursuant to paragraph 1."

17 Recitals 7 and 8.

18 Recital 16.

19 Recital 17.

20 See also Recital 37.

21 See also Recital 46.

provide that the controller[22] must implement appropriate technical and organizational measures to protect personal data against, *inter alia*, alteration or unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network. "Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected."[23]

7.13 It is intended that the protective principles set out in the Directive be supplemented and clarified in certain sectors by specific rules based on the principles,[24] and a further Directive is planned on the protection of personal data and privacy in the context of public digital telecommunications networks.[25] This Directive will require "the harmonization of the provisions required to ensure an equal level of protection of privacy in the Community and to provide for the free movement of telecommunications equipment and services within and between Member States."[26] It recognises that "currently in the European Community new advanced digital public telephone networks are emerging which give rise to specific requirements concerning the protection of personal data and privacy of the user",[27] and that "this is the case, in particular, with the introduction of the integrated services digital network (ISDN) and public digital mobile networks".[28] It further states that "in the case of public digital networks, specific legal, regulatory, and technical provisions must be made in order to protect personal data and the privacy of users with regard to the increasing risks connected with the computerized storage and processing of personal data in such networks."[29] It will make it clear that the collection, storage and processing of personal data by a telecommunications organisation is justified for the purposes of the intended service only and may not be used without specific authorization by law or the subscriber's prior consent for any other purpose."[30] It will also implement in the telecommunications sector the general principles concerning a subscriber's rights to inspect personal data stored about her or him, to request the rectification or erasure of incorrect data, and to prevent non-authorised disclosure of personal data.[31] Moreover, it provides that:

---

22 "Controller" is defined under Article 2(d) to mean -

> "... the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by a national or Community law."

23 Article 17(1). See also Article 17(2) concerning the situation where processing is carried out on behalf of the controller.

24 Recital 68.

25 The proposed Directive is reproduced in *Denton Hall*, B9-B15.

26 Art. 1(1) of the Draft Directive.

27 Recital 2.

28 Recital 13.

29 Recital 10.

30 Recital 14 and Art. 4. Art. 4(2) specifically provides -

> "The telecommunications organization shall not use such data to set up electronic profiles of the subscribers or classifications of individual subscribers by category."

31 Recital 15 and Arts. 6 & 7.

"1. The telecommunications organization must provide adequate, state-of-the-art protection of personal data against unauthorized access and use.

2. In case of particular risk of a breach of the security of the network, for example, in the field of mobile radio telephony, the telecommunications organization must inform the subscribers concerning such risk and offer them an end-to-end encryption service."[32]

Furthermore,

"If the content of telephone calls is made accessible to third parties via technical devices, such as loudspeakers or other on-hook equipment, or stored on tape for own use or use by third parties, provision must be made in order that the parties concerned are informed via an appropriate procedure of such diffusion or storage before the diffusion or storage is initiated and for so long as it continues."[33]

The application of the Directive's provisions to service providers other than telecommunications organizations will be entrusted to the Commission[34]; and excluded altogether from the Directive's scope are issues of protection of personal data and privacy related to national security.[35]

7.14 It is interesting to note that recognition has been afforded in this Directive to the role to be played by evolving technology in privacy protection as opposed to privacy invasion, and that a degree of responsibility for privacy protection is to be placed on telecommunications organizations. While problems will doubtless arise in practice as to whether particular protection was "state-of-the-art" or not and as to the precise extent of the obligations of a telecommunications organization to ensure user privacy, responsibility for the protection of this privacy is to be shared by the user, the telecommunications organization (or other service provider) and the State.[36]

7.15 With respect to privacy in general, the Maastricht Treaty provides that:

"The Union shall respect fundamental rights, as guaranteed by the

---

32 Art. 8.

33 Art. 15(1). This is subject to the exception that, for a limited period of time, the telecommunications organization may override the elimination of the calling line identification: Arts. 12, 13(1) & 15(2).

34 Art. 20.

35 Recital 22.

36 The many and varied threats to privacy posed by universal personal communication (UPT) have been considered in some detail by the European Telecommunications Standards Institute. A number of "eavesdropping" threats have been identified by the Institute, including eavesdropping of user and recipient identity, authentication information and registration data on both incoming and outgoing UPT calls, a remote registration message and information during subscription. The Institute evaluated these threats as of minor importance in comparison to others.

We are concerned in this Paper principally with the interception of telecommunications messages and will return to consider in much greater detail these threats to telecommunications privacy in our research and proposals on information privacy.

European Convention for the Protection of Human Rights and Fundamental Freedoms ... and as they result from the constitutional traditions common to the Member States, as general principles of Community law."[37]

The importance of the European Convention on Human Rights as a source of fundamental rights within the Community had already been recognised by the European Court of Justice[38] and in the Single European Act,[39] and its endorsement by the Maastricht Treaty means that no longer will countries such as Ireland, which subscribe to the dualist view of international law[40] and which have not incorporated the Convention into their domestic law, be able to treat the Convention and its attendant case law as having effect purely at the international level. To the extent that the Convention impacts on Community law, it, albeit indirectly, may have legal effect in Member States. This is as true for the privacy guarantee in the Convention as it is for the other fundamental rights recognised therein.

The European Convention On Human Rights

7.16 Ireland signed the European Convention on Human Rights on 4 November 1950 and the Convention entered into force for it and the other signatories on 3 September 1953. The Convention and its attendant Protocols[41] set forth a substantial number of human rights guarantees which the State has undertaken to secure to everyone within its jurisdiction.[42] Although, strictly speaking, decisions of the Court are only binding under international law on states parties to a case,[43] as authoritative interpretations of the guarantees laid down by the Convention, they often enunciate standards which are applicable to states parties in general. Thus, although the Court has not been seised to date of a complaint against Ireland in respect of surveillance, it has had to consider several such complaints against other states parties, and its Judgments in these cases afford indications of the standards and obligations of Ireland as a state party in this regard. Also, admissibility decisions of the Commission and its Reports on the merits of complaints throw light on the understanding by this body of the guarantees contained in the Convention. The principal guarantee in matters of privacy is provided by Article 8. Of relevance also are Article 6 which concerns the right to a fair trial and Article 13 which requires an effective

---

37 Title I, Art. F2.

38 See, e.g., D. Wyatt and A. Dashwood, *European Community Law*, 3rd ed., Sweet & Maxwell, London, 1993, pp.99-100 and the case law cited thereat.

39 Preamble.

40 According to the dualist view, international law and municipal law are separate legal orders: see, e.g., I. Brownlie, *Principles of Public International law*, 4th ed., Clarendon Press, Oxford, 1990, pp.32-33; M. Dixon, *International Law*, Blackstone Press, London, 1990, p.37; and D. J. Harris, *Cases and Materials on International Law*, 4th ed., Sweet & Maxwell, London, 1991, pp.69-72.

41 Ten Protocols have been agreed to date. Ireland is party to the First, Second, Third, Fourth, Fifth and Eighth Protocols.

42 Article 1 of the Convention provides:

> "The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention."

43 See Article 53 of the Convention.

remedy before a national authority for a breach of a person's rights under the Convention.

(i) **Article 8**

7.17 Article 8 provides:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

7.18 The first thing to note about this Article in the context of the present study is that it explicitly protects correspondence from interference: that is, freedom of correspondence has been perceived as of sufficient importance to warrant protection in its own right.[44] Moreover, the fact that freedom of correspondence is protected in its own right means that protection is not dependent upon the content or circumstances of the correspondence or the identity or relationship of the correspondents.[45] There is no need for a person claiming the protection of Article 8 in respect of correspondence to establish a link between the correspondence and his or her "private life".

7.19 Secondly, the grounds on which interference with correspondence or with other privacy interests is permitted are exhaustively listed in paragraph 2 of Article 8.[46] Interference is only allowed on one or more of the following grounds:

- in the interests of national security;
- in the interests of public safety;
- in the interests of the economic well-being of the country;
- for the prevention of disorder;
- for the prevention of crime;
- for the protection of health;
- for the protection of morals;
- for the protection of the rights and freedoms of others.

---

44 It is also worthy of note that it is protected as part of a general privacy guarantee rather than as an aspect of freedom of expression. This accords with other international privacy guarantees: see, e.g., Article 12 of the Universal Declaration of Human Rights, Article 17 of the International Covenant on Civil and Political Rights (below para. 7.45), Article 11 of the American Convention on Human Rights, and cf. the omission of any such explicit guarantee from the African Charter on Human and Peoples' Rights.

45 These matters may however be relevant to the scope of the protection afforded.

46 The Court first made this clear in its Judgment in the case of *Golder*, 21 February 1975, Series A, No. 18, at para. 44, 1 E.H.R.R. 524 at 539.

The State may not therefore, consistently with its international obligations, interfere with privacy for any other reason than those specified.

7.20 Thirdly, not only must an interference pursue one or more of the above "legitimate aims" as they are termed in the Strasbourg case law. Two further conditions must be satisfied for it to be acceptable. The interference must be "in accordance with the law" and it must be "necessary in a democratic society" as a means of achieving the aim or aims pursued.

7.21 Through its Judgments the Court has gradually clarified the meaning of the phrase "in accordance with the law". The expression refers not only to the existence of a provision in national law but also to the quality of this law. The interference must be permitted, and regulated by a national legal provision. Also, this provision must be accessible so that a person may become acquainted with it,[47] and it must be phrased with a sufficient degree of clarity and precision that a person can reasonably foresee the circumstances and conditions in which an interference may occur.[48] Where the law allows a discretion to national authorities to interfere, the discretion may not be so broad that it may be arbitrarily exercised. Rather safeguards must exist in the law against abuse of the discretion. The Court recently summarised its understanding of this condition as follows:

> "... the expression "in accordance with the law", within the meaning of Article 8 § 2, requires firstly that the impugned measures should have a basis in domestic law. It also refers to the quality of the law in question, requiring that it be accessible to the persons concerned and formulated with sufficient precision - if need be, with appropriate advice - to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail. A law which confers a discretion is not in itself inconsistent with this requirement, provided that the scope of the discretion and the manner of its exercise are indicated with sufficient clarity, having regard to the legitimate aim in question, to give the individual adequate protection against arbitrary interference."[49]

7.22 Similarly, the Court has gradually elucidated the meaning of necessity in a democratic society. It has stated that necessity is a stricter test than desirability or reasonableness, and that necessity is to be assessed by reference to the type of democratic society which the Convention was meant to uphold, that is, a

---

47 The law may take any form, e.g. statute, secondary legislation, case law: see, e.g., *The Sunday Times* case, Court Judgment, 26 April 1979, Series A, No. 30, para. 47, 2 E.H.R.R. 245 at 270; and *Huvig* and *Kruslin*, Court Judgments of 24 April 1990, Series A, Nos. 176-B and 176-A, paras. 28 & 29 respectively, 12 E.H.R.R. 528 at 542 and 12 E.H.R.R. 547 at 561-562.

48 If need be, with the assistance of legal advice: see, e.g., *The Sunday Times* Judgment, para. 49, 2 E.H.R.R. 245 at 271.

49 *Anderson v. Sweden*, Court Judgment, 25 February 1992, para. 75, Series A, No. 226, 14 E.H.R.R. 615 at 643-644. See also paras. 85-90 of the Court's Judgment in the *Case of Silver and Others*, 25 March 1983, Series A, No. 61, 5 E.H.R.R. 347 at 371-373, where the Court listed these considerations as general principles applicable to the interpretation of the expression "in accordance with the law". This case concerned interference with prisoners' correspondence.

liberal democracy which values pluralism and tolerance and which is the antithesis of an authoritarian state. Two key elements of the test are that the interference must be a response to "a pressing social need" and that its impact on the applicant must be proportionate to the legitimate aim or aims pursued. One particularly problematic aspect of the necessity criterion concerns the state's "margin of appreciation" in relation to the necessity of the interference, that is, the extent to which the Commission and the Court will accept the view of national authorities as to the need for interference and the extent to which they will substitute their own view of the need for that of the national authorities. It is clear that this margin is not uniform in all cases. The Court has said that, "The scope of the margin of appreciation will vary according to the circumstances, the subject matter and its background"[50]; and that it "will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved."[51] In 1981, the Court identified the following principles as relevant to the assessment of the necessity in a democratic society of a measure taken in furtherance of an aim that is legitimate under the Convention:

> "Firstly, "necessary" in this context does not have the flexibility of such expressions as "useful", "reasonable", or "desirable", but implies the existence of a "pressing social need" for the interference in question ...
>
> In the second place, it is for the national authorities to make the initial assessment of the pressing social need in each case; accordingly, a margin of appreciation is left to them ... However, their decision remains subject to review by the Court ...
>
> ... not only the nature of the aim of the restriction but also the nature of the activities involved will affect the scope of the margin of appreciation. The present case concerns a most intimate aspect of private life. Accordingly, there must exist particularly serious reasons before interferences on the part of the public authorities can be legitimate for the purposes of paragraph 2 of Article 8.
>
> Finally, ... the notion of "necessity" is linked to that of a "democratic society" ... a restriction on a Convention right cannot be regarded as "necessary in a democratic society" - two hallmarks of which are tolerance and broadmindedness - unless, amongst other things, it is

50 *Rasmussen*, Court Judgment, 28 November 1984, Series A, No. 87, para. 40, 7 E.H.R.R. 371 at 380.
51 *Leander*, Court Judgment, 26 March 1987, Series A, No. 116, para. 59, 9 E.H.R.R. 433 at 452.

proportionate to the legitimate aim pursued ..."[52]

7.23 Last, although Article 8 is phrased in terms of interference by a public authority with the exercise of the guaranteed right, the Court has held that on occasion a state's obligations under the Convention may require it to ensure not only that any interference by a public authority with privacy conforms to the provisions of Article 8 but also that an individual's privacy is protected against intrusion thereon by other non-state actors. This is of particular significance in the present context with respect to private surveillance, such as the taking of pictures by press photographers while a person is at home or on private property and the use of telephone tapping and listening devices by private investigators. The Court has given the following guidance as to when it will interpret the Convention as imposing a "positive obligation" upon states Parties in relation to the protection of privacy -

> "...as far as ... positive obligations are concerned, the notion of "respect" is not clear-cut: having regard to the diversity of the practices followed and the situations obtaining in the Contracting States, the notion's requirements will vary considerably from case to case. Accordingly, this is an area in which the Contracting Parties enjoy a wide margin of appreciation in determining the steps to be taken to ensure compliance with the Convention with due regard to the needs and resources of the community and of individuals"[53];

and,

> "In determining whether or not a positive obligation exists regard must be had to the fair balance that has to be struck between the general interest of the community and the interests of the individual ... In striking this balance the aims mentioned in the second paragraph of Article 8 may be of a certain relevance, although this provision refers in terms only to "interferences" with the right protected by the first

---

52 *Dudgeon*, Court Judgment, 22 October 1981, Series A, No. 45, paras. 50-53, 4 E.H.R.R. 149 at 164-165. Cf. the following summary of principles given by the Court at para. 97 of its Judgment in the *Case of Silver and Others*, 25 March 1983, Series A, No. 61, 5 E.H.R.R. 347 at 376-377:

> "(a) the adjective 'necessary' is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable' (see the Handyside judgment of 7 December, Series A no. 24, p.22, para. 48);
>
> (b) the Contracting States enjoy a certain but not unlimited margin of appreciation in the matter of the imposition of restrictions, but it is for the Court to give the final ruling on whether they are compatible with the Convention (*ibid.*, p.23, para. 49);
>
> (c) the phrase 'necessary in a democratic society' means that, to be compatible with the Convention, the interference must, *inter alia*, correspond to a 'pressing social need' and be 'proportionate to the legitimate aim pursued' (*ibid.*, pp.22-23, paras. 48-49);
>
> (d) those paragraphs of Articles of the Convention which provide for an exception to a right guaranteed are to be narrowly interpreted (see the ... Klass and others judgment, Series A no. 28, p.21, para. 42)."

53 *Abdulaziz, Cabales and Balkandali*, Judgment, 28 May 1985, Series A, No. 94, para. 67, 7 E.H.R.R. 471 at 497.

paragraph ..."[54]

7.24 In the recent case of *A. v. France*,[55] which concerned the clandestine recording of a telephone conversation by a private citizen with the assistance of a high-ranking police officer, the Court, having found that the public authorities were involved to such an extent that the state's responsibility under the Convention was engaged, then added:

> "In any event the recording represented an interference in respect of which the applicant was entitled to the protection of the French legal system."[56]

This suggests that the Court will expect secret surveillance, at least of telecommunications, by non-state actors to be regulated by domestic law and that the law contain safeguards for the individual in this regard.

7.25 The admission as evidence in a personal injuries claim of photographs taken by a private investigator was challenged in a recent application against Ireland.[57] The investigator had been hired by an insurance company in its defence of the claim, and the photographs were mostly of the applicant in the street with shopping bags and entering her house. There were however also one or two photographs of her inside the house closing a window. The investigator took the photographs from outside the physical boundaries of the applicant's home. Since the application was found to be inadmissible for failure to exhaust domestic remedies, the Commission did not have to express a view on whether the facts of the case disclosed any privacy interest on the part of the applicant, and if they did, whether the admission as evidence in judicial proceedings of the photographs was compatible with the applicant's rights under Article 8.

7.26 That surveillance will not necessarily impinge upon the sphere of private life protected by Article 8 is illustrated by the finding of the Court in *Ludi v. Switzerland*[58] that the use of an undercover agent did not, either alone or in combination with the interception of the applicant's telephone conversations, affect the applicant's private life within the meaning of Article 8.[59] The Court reasoned that the agent, a police officer, had been selected to infiltrate what the authorities suspected was a large network of traffickers intending to dispose of a quantity of drugs in Switzerland. The aim of the operation was to arrest the dealers when the drugs were handed over; and when the applicant was contacted by the agent, the applicant offered to sell him a quantity of cocaine. From then

---

54 *Rees*, Judgment, 17 October 1986, Series A, No. 106, para. 37, 9 E.H.R.R. 56 at 64. See also *Cossey*, Judgment, 27 September 1990, Series A, No. 184, para. 37, 13 E.H.R.R. 622 at 639; and *B. v. France*, Judgment, 25 March 1992, Series A, No. 232-C, para. 44, 16 E.H.R.R. 24 at 27.

55 Court Judgment, 23 November 1993, Series A, No. 277-B, 17 E.H.R.R. 462.

56 Para. 36, 17 E.H.R.R. 462 at 477. The Court found that there was no basis in French law for the interference.

57 Application No. 18670/91, admissibility decision of the European Commission of Human Rights, 1 December 1993. See further above paras. 3.21-3.22 concerning this case.

58 Court Judgment, 15 June 1992, Series A, No. 238, 15 E.H.R.R. 197.

59 Para. 40 of the Judgment, 15 E.H.R.R. 197 at 199. Cf. the view of the Swiss Federal Court, *Annuaire suisse de droit international*, 1987, pp.229-230 & 232-234 and of the Commission, *Report*, 6 December 1990, paras. 53-58, 15 E.H.R.R. 184 at 187-188.

on the applicant must have been aware that he was engaged in a criminal act and that he was running the risk of encountering an undercover police officer whose task would be to expose him.

7.27 The difficulty of defining the notion of privacy is widely recognised, and the Commission and the Court have not found it easy to formulate with any precision the meaning of the cognate term, "private life".[60] Many issues that may be expected to arise in cases of surveillance remain unresolved, e.g. whether the taking of a photograph from a public highway of a person in a private garden constitutes an interference with that person's private life; whether the use of a parabolic microphone to overhear an office conversation impinges upon the private life of those holding the conversation.

7.28 The threshold question of whether a complaint pertains to the applicant's private life is generally avoided where the complaint concerns interference with correspondence since, as we have seen, freedom of correspondence is protected irrespective of the content of the correspondence etc.[61] "Correspondence " has been interpreted by the Court to include both the post and telecommunications.[62] Whether the term includes electronic mail has not been expressly considered to date, but there would appear to be no reason in principle why other forms of communication should not also be covered. It may however be doubted whether face-to-face conversations are to be regarded as correspondence. If they occur within the home, then the protection of Article 8 will apply. If not, protection may depend upon whether or not they fall within the scope of either the term "private life" or "family life".[63] Complaints of interference with the post and telecommunications have come before the Court on several occasions in the context of secret surveillance, and the Court's Judgments in these cases throw considerable light on the requirements which must be satisfied if such interference is to be compatible with a state's obligations under the Convention.[64]

7.29 The first case in which the Court had to consider measures of secret

---

60 For an examination of the concept of private life as interpreted by the Commission and the Court see, e.g., A. Connelly, "Problems of Interpretation of Article 8 of the European Convention on Human Rights", (1986) 35 I.C.L.Q. 567 at 578-580; L. Doswald-Beck, "The Meaning of the Right to Respect for Private Life under the European Convention on Human Rights", (1983) 4 H.R.L.J. 283 at 287-301; J.E.S. Fawcett, *The Application of the European Convention on Human Rights*, 2nd ed., Clarendon Press, Oxford, 1987, pp.211-216; and P. van Dijk and G.J.H. van Hoof, *Theory and Practice of the European Convention on Human Rights*, 2nd ed., Kluwer Law and Taxation Publishers, Deventer, 1990, pp.369-378.

61 See above para. 7.18.

62 Indeed the Court has specifically stated that although telephone conversations are not expressly mentioned in the first paragraph of Article 8, it considers them to be covered by both the notions of "private life" and "correspondence": see the Court's Judgments in the *Case of Klass and Others*, 6 September 1978, Series A, No. 28, para. 41, 2 E.H.R.R. 214 at 230 and in the *Malone Case*, 2 August 1984, Series A, No. 82, para. 64, 7 E.H.R.R. 14 at 38.

63 It may also be queried whether all communications, irrespective of content, are to be regarded as correspondence. Do, for example, goods sent by post constitute correspondence, or does the term imply the conveyance of some information?

64 The Court has also examined many complaints of interference with prisoners' correspondence. We will consider these in detail later when we review the situation with respect to surveillance in a number of specific contexts. The Court has also examined restrictions on communications between a parent and child taken into public care, and these will likewise be considered in the context of our study of particular contextual issues pertaining to surveillance.

surveillance was that of *Klass and Others*.[65] The case concerned surveillance by the state of post and telecommunications for security purposes and, under the German law in question, all persons could potentially have their mail, post and telecommunications monitored without ever necessarily being informed or aware of any surveillance. Although the applicants were not able to show that they had been subject to surveillance, in order to uphold the effectiveness of the procedures and remedies of the Convention in relation to such surveillance, the Court accepted their *locus standi* to bring the applications. It was of the view that the:

> "... in the mere existence of the legislation, there is involved for all those to whom the legislation could be applied, a menace of surveillance: this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence"[66];

and identified the "cardinal issue under Article 8"[67] as being whether the interference was justified by the terms of paragraph 2 of the Article. It described powers of secret surveillance as characterising the police state and hence as "tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions".[68] While acknowledging that some surveillance was needed in order to combat highly sophisticated forms of espionage and terrorism, the Court voiced its concern at the danger which a law authorising surveillance poses "of undermining or even destroying democracy on the ground of defending it",[69] and affirmed that "the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[70] Indeed, the Court "must be satisfied that whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse."[71]

7.30 As to the question whether such guarantees exist, it commented generally that:

> "This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures,

---

65 Court Judgment, 6 September 1978, Series A, No. 28, 2 E.H.R.R. 214.
66 Para. 41 of the Judgment, 2 E.H.R.R. 214 at 230.
67 At para. 42, 2 E.H.R.R. 214 at 230.
68 Para. 42, 2 E.H.R.R. 214 at 231.
69 Para. 49, 2 E.H.R.R. 214 at 232.
70 *Ibid.*
71 Para. 50, 2 E.H.R.R. 214 at 232-233.

and the kind of remedy provided by the national law."[72]

Later in the Judgment, however, it did afford some more specific guidance as to what safeguards would be expected in relation to the monitoring and control of state surveillance -

> "Review of surveillance may intervene at three stages; when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding the individual's rights. In addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 § 2, are not to be exceeded. One of the fundamental principles of a democratic society is the rule of law, which is expressly referred to in the Preamble to the Convention .... The rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence,

---

72 *Ibid.* On examination, the German law in question did provide "adequate and effective guarantees against abuse". It did not permit exploratory or general surveillance. Surveillance was only authorised where a person was under suspicion with respect to the commission of certain serious criminal acts and where other means of establishing the facts were without prospect of success or considerably more difficult. Only the specific suspect or the suspect's presumed contacts could be subjected to surveillance. A written application giving reasons was required and could only be made by a select number of persons. Only a Federal Minister or a supreme *Land* authority could authorise surveillance, and although not required by legislation, the competent Minister would in practice seek the prior consent of an independent Commission (the G10 Commission). Strict conditions also applied to the implementation of surveillance measures and to the processing of information obtained thereby. A measure could only remain in force for a maximum of three months and could be renewed only on fresh application; it had to cease immediately it was no longer necessary or the conditions for its authorisation no longer existed; knowledge and documents obtained could only be used for the purpose for which the surveillance was authorised; and documents had to be destroyed as soon as they were no longer needed to achieve the required purpose. An initial control of the information gained was carried out by an official qualified for judicial office who destroyed any irrelevant material sending on to the service concerned only such information as was authorised by the legislation. Subsequent control was provided by two independent bodies appointed by elected representatives: the G10 Commission and a Parliamentary Board. Every six months, the competent Minister had to report on the application of the legislation to a Parliamentary Board of five Members of Parliament who were appointed in proportion to the parliamentary groupings. In addition, the Minister was legally obliged to provide the G10 Commission every month with an account of the measures ordered and a person who believed that she or he was under surveillance could apply to the Commission for a review both of the legality and of the necessity for the measure, and if the Commission declared any measure to be illegal or unnecessary, the Minister had to terminate it immediately. The Commission consisted of three members, the Chair being held by a person qualified to hold judicial office and the other two members being appointed by the Parliamentary Board. Although the legislation provided that there would be no legal remedy before the courts in respect of the ordering and implementation of surveillance measures, a person who had applied unsuccessfully to the Commission retained the right to apply for a remedy to the Constitutional Court: see paras. 16-25 & 51-60 of the Court's Judgment, 2 E.H.R.R. 214 at 220-224 & 233-237.

impartiality and a proper procedure."[73]

As regards review at the third stage, after the termination of a measure of surveillance, the Court recognised that the activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the termination of the measures and that subsequent notification to each individual affected by a measure might well jeopardise the long-term purpose that originally prompted the surveillance. Moreover, notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. The Court therefore refused to require among the "adequate and effective guarantees against abuse" subsequent notification in all cases. In its view, "the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with [the second paragraph of Article 8] since it is this very fact which ensures the efficacy of the "interference"."[74] As the Court, in dealing with this matter, remarked that:

> "there is in principle little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality"[75],

it would seem that access to the courts at the third stage by a person who has been subjected to secret surveillance in order to challenge the legality of that surveillance is not required either.[76]

7.31 What was in issue in the *Klass* case was the acceptability under the Convention of state security measures involving secret surveillance. Secret surveillance in the context of the 'ordinary' criminal process came under scrutiny by the Court a few years later in the British case of *Malone*.[77] In this case, the Court again required the existence in domestic law of safeguards against the abuse of powers of secret surveillance, but did so in applying the criterion that an interference must be "in accordance with the law" rather than under the rubric of necessity in a democratic society.

7.32 Malone was suspected of receiving stolen goods, and at his trial it became apparent that the police were in possession of information which could

---

73 Para. 55, 2 E.H.R.R. 214 at 234-235. Although "in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge" (para. 56), the Court held that, given their independence of the authorities, their power of control and their democratic character, the G10 Commission and the Parliamentary Board ensured sufficient review during the first two stages.

74 Para. 58, 2 E.H.R.R. 214 at 236.

75 Para. 57, 2 E.H.R.R. 214 at 235.

76 It is not clear whether all judicial control may be excluded at this stage. The facts of this case disclosed that there was an element of judicial control in Germany in that, according to a judgment of the German Federal Constitutional Court, a person who had been subject to surveillance had to be informed after the termination of the surveillance measures as soon as notification could be made without jeopardising the purpose of the measures, and thereupon several legal remedies became available to the person: see para. 24 of the Court's Judgment for these remedies, 2 E.H.R.R. 214 at 224.

77 Court Judgment, 2 August 1984, Series A, No. 82, 7 E.H.R.R. 14.

only have been gained by the tapping of his home telephone. Again, the "principal issue"[78] was whether the interference with the applicant's communications was justified under paragraph 2 of Article 8.

7.33 The phrase "in accordance with the law" implies, said the Court:

> "that there must be a measure of legal protection in domestic law against arbitrary interference by public authorities with the rights safeguarded by paragraph 1 ... Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident. Undoubtedly ... the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."[79]

It must "indicate the scope of any ... discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."[80]

---

78 Para. 65 of the Judgment, 7 E.H.R.R. 14 at 39.

79 Para. 67, 7 E.H.R.R. 14 at 40-41.

80 Para. 68, 7 E.H.R.R. 14 at 41. The British law in question did not meet these criteria. Indeed the exact legal basis of the executive's power of surveillance was obscure, the law being open to different interpretations. Moreover, it was not possible to identify 'with any reasonable certainty what elements of the powers to intercept were incorporated in legal rules and what elements remained within the discretion of the executive'. In view of this obscurity and uncertainty, the Court was of the opinion that 'the law of England and Wales did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities', and 'to that extent, the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society was lacking.': see para. 69-79 of the Court's Judgment, 7 E.H.R.R. 14 at 41-45.

The Court also considered the compatibility with Article 8 of a process of metering. This involves the use of a device called a meter check printer which registers the numbers dialled on a particular telephone and the time and duration of each call. The Court accepted that a metal check printer records information which a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. It took the view that "[b]y its very nature, metering is ... to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified", but that an issue might arise under Article 8 in that the records of metering contain information (in particular, the numbers dialled) which is an integral element in the communications made by telephone. Release of that information to the police without the consent of the subscriber constitutes an interference with correspondence which required to be justified under paragraph 2. In the case before it, the Court found that there was no basis in the law of England and Wales for the practice of the Post Office whereby it would, on occasion and on request, make and supply records of metering to the police. Moreover, there appeared to be no legal rules concerning the scope and manner of exercise of the discretion enjoyed by the public authorities. See the Court's Judgment, paras. 83-87, 7 E.H.R.R. 14 at 46-47.

7.34 Some six years later the Court again considered the compatibility of telephone tapping with the Convention in the context of a criminal investigation: *Huvig*[81] and *Kruslin*[82] cases. Mr. and Mrs. Huvig had their business and private telephone calls monitored on suspicion of tax evasion and other financial offences. Mr. Kruslin was wanted in connection with murder. While staying with another person suspected of murder, he had used this person's telephone, and in a monitored telephone conversation with someone calling from a public telephone-box, had spoken in veiled terms about another murder. The recording of this conversation was a decisive piece of evidence in subsequent criminal proceedings against him. As in *Malone*, the decisions of the European Human Rights Court in these cases also turned on its application to the facts of the cases of the requirement that the interception be "in accordance with the law"; and they are important in that they show that, even where there is judicial control of surveillance, this form of control in itself will not suffice if it does not afford "adequate and effective guarantees" against abuse of surveillance by the executive.

7.35 The interceptions had been authorised by investigating judges during the course of the respective criminal investigations. The Court found that they had a basis in French law,[83] and that the accessibility of this law did not raise any problem. However, the law failed the foreseeability test. In the Court's view:

> "Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated."[84]

7.36 The French Government had pleaded a large number of safeguards against arbitrary interceptions,[85] some of which were expressly provided for in the Code of Criminal Procedure and others which had been laid down in court judgments over the years. However, some of the safeguards were not to be found in the Code or in case law, but were rather to be inferred from general enactments or principles or from an analogical interpretation of legislative

---

81 24 April 1990, Series A, No. 176-B, 12 E.H.R.R. 528.

82 24 April 1990, Series A, No. 176-A, 12 E.H.R.R. 547.

83 In the Code of Criminal Procedure and in case law: see *Huvig* Judgment, para. 28, 12 E.H.R.R. 528 at 542 and *Kruslin* Judgment, para. 29, 12 E.H.R.R. 547 at 561-562.

84 *Huvig* Judgment, para. 32, 12 E.H.R.R. 528 at 544; *Kruslin* Judgment, para. 33, 12 E.H.R.R. 547 at 563-564.

85 The Government listed seventeen safeguards which it said were provided for in French law. These included:

- the need for an investigating judge, that is, an independent judicial authority, to authorise surveillance;
- supervision by the judge of senior police officers and the possible supervision of the judge by the Indictment Division of the Court of Appeal, by trial courts and courts of appeal and, if need be, by the Court of Cassation;
- the exclusion of any subterfuge or ruse consisting not merely in the use of telephone tapping but in an actual trick, trap or provocation;
- the duty to respect the confidentiality of relations between suspect or accused and lawyer.

See the *Huvig* Judgment, paras. 32-33, the *Kruslin* Judgment, paras. 33-34, and, for a full list, the Reports of the Commission in *Huvig* and *Kruslin*, 14 December 1988, paras. 31 and 37 respectively.

provisions or court decisions dealing with investigative measures. Such "extrapolation" did not in the Court's opinion, "provide sufficient legal certainty".[86] By way of example of the lack of sufficient legal certainty and of adequate safeguards against possible abuse of the power of surveillance, the Court mentioned that:

> "... the categories of people liable to have their telephones tapped by judicial order and the nature of the offences which may give rise to such an order are nowhere defined. Nothing obliges a judge to set a limit on the duration of telephone tapping. Similarly unspecified are the procedure for drawing up the summary reports containing intercepted conversations; the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge (who can hardly verify the number and length of the original tapes on the spot) and by the defence; and the circumstances in which recordings may or must be erased or the tapes be destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court." [87]

(ii) Article 13

7.37 Article 13 provides:

> "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

7.38 This provision is not to be read literally. The right to an effective remedy before a national authority does not cover only situations where a person's rights or freedoms as set forth in the Convention have actually been violated. It is not "a prerequisite for the application of Article 13 that the Convention be in fact violated."[88] What Article 13 guarantees is an effective remedy before a national authority to persons who claim that their rights and freedoms under the Convention have been violated.

> "... Article 13 requires that where an individual considers himself to have been prejudiced by a measure allegedly in breach of the Convention, he should have a remedy before a national authority both to have his claim decided and, if appropriate, to obtain redress. Thus, Article 13 must be interpreted as guaranteeing an "effective remedy before a national authority" to everyone who *claims* that his rights and freedoms under the Convention have been violated"[89]

---

86 *Huvig* Judgment, para. 33, 12 E.H.R.R. 528 at 542; *Kruslin* Judgment, para. 34, 12 E.H.R.R. 547 at 564.
87 *Huvig* Judgment, para. 34, 12 E.H.R.R. 528 at 545; *Kruslin* Judgment, para. 35, 12 E.H.R.R. 547 at 564-565.
88 *Klass and Others*, Court Judgment, 6 September 1978, Series A, No. 28, para. 64, 2 E.H.R.R. 214 at 238.
89 *Ibid.*

The national authority need not be a judicial authority, but the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy before it is effective.[90]

7.39 Secret surveillance by the state poses particular problems in this regard since, for the reasons adverted to earlier,[91] a person subject to such surveillance may never become aware of the fact and hence may never seek a remedy. Consistently with its conclusion on the matter under Article 8, the Court has held that a person who has been subjected to secret surveillance may not in all cases derive from Article 13 a right to notification of the surveillance. Rather, "an "effective remedy" under Article 13 must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance."[92]

(iii) Article 6

7.40 While the remedy under Article 13 need not be judicial, Article 6 does require that certain proceedings afford the degree of independence and impartiality associated in a democratic society with the judicial process. Article 6 requires a fair trial where a person's civil rights and obligations, or a criminal charge against a person, are being determined, and the Article has been interpreted by the Court to include access to a tribunal.[93] The first sentence of paragraph 1 of Article 6 sets forth the general guarantee:

> "In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law."[94]

Paragraphs 2 and 3 itemise some specific rights of a person faced with a criminal

---

90 *Klass and Others*, Court Judgment, 6 September 1978, Series A, No. 28, para. 67, 2 E.H.R.R. 214 at 239.

91 See above para. 7.30.

92 *Klass and Others*, Court Judgment, para. 69, 2 E.H.R.R. 214 at 240. Applying this understanding of Article 13, the Court found that the aggregate of remedies provided for under German law in respect of secret surveillance satisfied the requirements of the Article. These remedies were the opportunity for a person believing herself or himself to be under surveillance of complaining to an independent Commission and to the Constitutional Court, and the various legal remedies before the courts upon notification subsequent to surveillance: namely, an action for a declaration before an administrative court as to the lawfulness of the application of the legislation to the person and the conformity with the law of the surveillance measures ordered; an action for damages in a civil court if the person had been prejudiced; an action for the destruction or, if appropriate, restitution of documents; and an application to the Federal Constitutional Court for a ruling as to whether there had been a breach of the Basic Law. See paras. 24 & 70-72 of the Court's Judgment, 2 E.H.R.R. 214 at 224 & 240-241.

In the *Malone* case, the Court, having regard to its decision on Article 8, did not consider it necessary to rule on whether there had also been a violation of Article 13: see the Court's Judgment, para. 91, 7 E.H.R.R. 14 at 48, and cf. the Opinion of the Commission on this matter.

93 See *Golder*, Court Judgment, 21 February 1975, Series A, No. 18, paras. 28-36, 1 E.H.R.R. 524 at 532-536.

94 The paragraph continues:

> "Judgment shall be pronounced publicly but the press and the public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

charge. They include the presumption of innocence and address such matters as legal assistance, the preparation of the defence, the examination of witnesses and the use of language in court.[95]

7.41 If an issue pertaining to the interception of communications or surveillance is being decided and if it concerns the civil rights or obligations of a person or a criminal charge, then the guarantees of Article 6 apply. In a case of surveillance, whether covert or overt, by a non-state actor, an issue pertaining to the civil rights, that is, private rights,[96] of the person subject to surveillance may not infrequently arise. For example, if a newspaper publishes information which was obtained by the use of a scanning device, without the knowledge or consent of the person to whom the information relates, that person may plead an infringement of private rights to secure compensation for the unauthorised publication and any detriment suffered as a result. Similarly, if an individual is followed everywhere by another person who attempts continually to observe the subject, the latter may want to invoke private rights to put an end to the observation. A case of surveillance by a public authority may also raise an issue relating to the private rights or obligations of the subject, but is less likely to do so since the Strasbourg organs have held that relations between a public authority and an individual are not usually to be regarded as belonging to the civil or private field.[97] Whether the surveillance be state or non-state, a "right" under national law must be involved.[98] Under the "criminal" head, a person charged with unlawful surveillance should be afforded the same specific entitlements under Article 6 as are enjoyed by persons facing other criminal charges.

---

95 Paragraph 2 provides:

> "Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law."

Paragraph 3:

> "Everyone charged with a criminal offence has the following minimum rights;
>
> (*a*) to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
>
> (*b*) to have adequate time and facilities for the preparation of his defence;
>
> (*c*) to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
>
> (*d*) to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
>
> (*e*) to have the free assistance of an interpreter if he cannot understand or speak the language used in court."

96 On the meaning of 'civil rights and obligations', see, e.g., J.E.S. Fawcett, *op. cit.*, pp.133-145; and P. van Dijk and G.J.H. van Hoof, *op. cit.*, pp.295-305.

97 The Court at times weighs the 'public law' aspects of a right against its 'private law' aspects, and if the latter outweigh the former, categorises the right as a civil right: see, e.g, *Feldbrugge v. The Netherlands*, Court Judgment, 29 May 1986, Series A, No. 99, paras. 26-40, 8 E.H.R.R. 425 at 431-435, and *Deumeland v. Germany*, Court Judgment, 29 May 1986, Series A, No. 120, paras. 60-74, 8 E.H.R.R. 448 at 462-466.

98 See, e.g., *Fayed v. United Kingdom*, Court Judgment, 21 September 1994, Series A, No. 294-B, para. 65, 18 E.H.R.R. 393 at 429.

7.42 As with regard to Article 13, secret surveillance by the state poses particular problems regarding the applicability and scope of Article 6. The Court has held that, on the assumption that Article 6 applies:

> "As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6; as a consequence, it of necessity escapes the requirements of that Article."[99]

7.43 A particular issue which may arise in the context of either civil or criminal proceedings is the admissibility of evidence which has been obtained by surveillance. The Court has held that the admissibility of evidence is primarily governed by the rules of domestic law, and that, as a general rule, it is for the national courts to assess the evidence before them. The task of the Court is "to ascertain whether the proceedings, considered as a whole, including the way in which the evidence was submitted, were fair."[100]

7.44 Article 6 does not require that evidence which has been unlawfully obtained should always be excluded. The Court has specifically considered the admission in a criminal trial of evidence which was unlawfully obtained by a person who recorded a telephone conversation with the applicant.[101] The recorded conversation was subsequently used in evidence at the trial of the applicant for incitement to murder. The applicant argued, *inter alia*, that the use of unlawfully obtained evidence was enough to make the trial unfair. The Court disagreed:

> "While Article 6 of the Convention guarantees the right to a fair trial, it does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law.
>
> The Court cannot therefore exclude as a matter of principle and in the abstract that unlawfully obtained evidence of the present kind may be admissible. It has only to ascertain whether [the applicant's] trial as a whole was fair."[102]

The International Covenant On Civil And Political Rights

7.45 The International Covenant on Civil and Political Rights entered into

---

99 *Klass and Others*, Court Judgment, 6 September 1978, Series A, No. 28, para. 75, 2 E.H.R.R. 214 at 241-242.

100 *Ludi v. Switzerland*, Court Judgment, 15 June 1992, Series A, No. 238, para. 43, 15 E.H.R.R. 197 at 200. See also *Vidal v. Belgium*, 22 April 1992, Series A, No. 235-B, para. 33.

101 *Schenk v. Switzerland*, 12 July 1988, Series A, No. 140, 13 E.H.R.R. 242.

102 Para. 46 of the Judgment, 13 E.H.R.R. 242 at 265-266. The Court found in this case that the use of the recording in evidence did not deprive the applicant of a fair trial. The rights of the defence had not been disregarded; the applicant had been aware of the unlawfulness of the recording and had been able to challenge its authenticity and to oppose its use in the domestic proceedings; he had obtained an investigation of and could have examined the persons involved in the making of the recording; and the recording was not the only evidence on which the applicant's conviction was based.

force for Ireland on 7 March 1990.[103] The Covenant attempts to enunciate a universally agreed catalogue of human rights in the civil and political fields and, under it, there was established the Human Rights Committee to monitor states' Parties compliance with the standards set forth therein.[104] Article 17 deals with privacy, and follows much more closely than its European counterpart the wording of the equivalent provision in the Universal Declaration of Human Rights.[105] It provides:

> "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks."

7.46 Clearly, Article 17 permits interference with privacy, family, home or correspondence provided the interference is neither "arbitrary" nor "unlawful". The use of the word "unlawful", as well as the recognition in paragraph 2 of the right to the protection of the law against interference suggests that, like under the European Convention, there must exist a legal basis for any interference. The word "arbitrary" is undefined but echoes the requirement under the European Convention that safeguards should exist against any power to authorise or conduct interference and against unauthorised interference. Unlike Article 8 of the European Convention, however, Article 17 of the Covenant does not give an exhaustive, or even illustrative, list of the grounds on which interference may be regarded as legitimate. The Human Rights Committee itself has merely commented, "As all persons live in society, the protection of privacy is necessarily relative."[106]

7.47 As to the legal basis for any interference, the Committee has stated that "it is precisely in State legislation above all that provision must be made for the protection of the right set forth"[107] in Article 17, and that the term "unlawful"

---

103 In accordance with Article 49(2), which reads:

> 'For each State ratifying the present Covenant or acceding to it after the deposit of the thirty-fifth instrument of ratification or instrument of accession, the present Covenant shall enter into force three months after the date of deposit of its own instrument of ratification or instrument of accession.'

The Covenant entered into force on 23 March 1976, three months after the date of deposit with the Secretary-General of the United Nations of the thirty-fifth instrument of ratification: see Art. 49(1). Ireland deposited its instrument of ratification on 7 December 1989.

104 As of 1 January 1994, there were 125 states Parties to the Covenant.

105 Article 12, which reads:

> 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.'

106 General comment 16(32) (art. 17) of 23 March 1988, para. 7, U.N. Doc. CCPR/C/21/Add.6. For the competence of the Committee to make 'such general comments as it may consider appropriate' to states Parties and to the Economic and Social Council of the United Nations, see Art. 40(4) of the Covenant. The Committee's general comments, although providing useful guidance as to states Parties' obligations under the Covenant, are not legally binding.

107 General comment, para. 2. See also para. 1 where the obligations imposed on states Parties are described as including 'other measures' as well as legislation.

means that "no interference can take place except in cases envisaged by the law."[108] Moreover, "[i]nterference authorised by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant."[109] The "relevant legislation must specify in detail the precise circumstances in which ... interferences may be permitted",[110] and a "decision to make use of such authorised interference must be made only by the authority designated under the law, and on a case-by-case basis."[111]

7.48 As to the meaning of the expression "arbitrary interference", the Committee has said that an interference provided for under the law may nonetheless by arbitrary. In its opinion:

> "The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."[112]

On the face of it, the criterion of "reasonableness" employed here by the Committee in gauging the acceptability of an interference would appear to be less strict than the test of "necessity" explicitly laid down in paragraph 2 of Article 8 of the European Convention; but, in considering the balance to be drawn between an individual's interest in privacy and a competing public interest, the Committee has also said that:

> "... the competent public authorities should only be able to call for such information relating to an individual's private life, the knowledge of which is essential in the interests of society as understood under the Covenant."[113]

Evaluating an interference by reference to what is essential is close to the European test of what is necessary.

7.49 Whether Article 17 protects against interference with a person's privacy not only by the State but also by non-State actors has been directly addressed by the Committee. In its view, the right to privacy must 'be guaranteed against all interferences whether they emanate from State authorities or from natural or legal persons.'[114] More precisely:

> "States parties are under a duty themselves not to engage in interferences inconsistent with Article 17 of the Covenant and to provide the legislative framework prohibiting such acts by natural or legal

---

108 *Ibid.*, para. 3.
109 *Ibid.*
110 General comment, para. 8.
111 *Ibid.*
112 General comment, para. 4.
113 Para. 7.
114 General comment, para. 1.

persons."[115]

7.50 With particular reference to interference with correspondence and surveillance, the Committee has commented that:

> "Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed *de jure* and *de facto*. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited."[116]

Despite the unqualified wording of this statement, read in the context of the "general comment" in which it was made, it must be understood to mean that interference with correspondence and surveillance are in principle to be prohibited both in law and in practice, but that interference may be permitted where the interests of society require it.

7.51 Under Article 40, paragraph 1, of the Covenant, States Parties undertake to submit reports on the measures they have adopted which give effect to the rights recognised in the Covenant and on the progress made in the enjoyment of these rights within one year of the entry into force of the Covenant for the State Party concerned and at intervals thereafter. These reports are considered by the Human Rights Committee, and "shall indicate the factors and difficulties, if any, affecting the implementation of the ... Covenant."[117] In its general comment of 1988 on Article 17, the Committee recommended "that States should indicate in their reports the laws and regulations that govern authorised interferences with private life"[118]; and, more generally, expressed the view:

> "... that the reports should include information on the authorities and organs set up within the legal system of the State which are competent to authorise interference allowed by law. It is also indispensable to have information on the authorities which are entitled to exercise control over such interference with strict regard for the law, and to know in what manner and through which organs persons concerned may complain of a violation of the right provided for in article 17 of the Covenant. In their reports, States should make clear the extent to which actual practise conforms to the law. State party reports should also contain information on complaints lodged in respect of arbitrary or unlawful interference, and the number of any findings in that regard, as well as the remedies provided in such cases."[119]

---

115 Para. 9.
116 Para. 8.
117 Art. 40(2) of the Covenant.
118 At para. 7.
119 Para. 6.

7.52 Ireland submitted its First Report under Article 40 in 1992.[120] In relation to Article 17, the Report quotes Article 40.3.1° of the Constitution which guarantees the personal rights of the citizen and mentions that the superior courts have interpreted this provision to include a right of privacy.[121] The Report also states that, in addition to the constitutional protection of privacy, "the civil and criminal law can provide a means of safeguarding privacy in individual cases."[122] Under the heading, "Correspondence and communications", mention is made of the general prohibition on the opening etc. of postal packets and the interception of telecommunications messages under sections 84 and 98 of the *Postal and Telecommunications Act, 1983*.[123] Mention is also made of the issue of warrants by the Minister for Justice authorising the interception of telephone conversations or the opening of letters and of their implementation under general directions given by the Minister for Communications under section 110 of the 1983 Act.[124] The Report includes information about the conditions and circumstances under which warrants were issued prior to the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* and about pending legislation, which it is claimed:

> "... will place on a statutory basis the conditions under which the existing power of the Minister for Justice to issue warrants authorising the interception of communications is to be exercised and will regulate the procedure for the issue of authorisations. It will also introduce new safeguards against any misuse of the power to issue warrants."[125]

Global Intergovernmental Organisations

7.53 Ireland is a member of the Universal Postal Union (UPU) and of the International Telecommunication Union (ITU), intergovernmental organisations which were established to regulate global communications in their respective fields. Both are specialised agencies of the United Nations.[126]

(i) Universal Postal Union

7.54 The Universal Postal Union was formed in the latter half of the nineteenth century.[127] Its central office, called the International Bureau, is

---

120 The Report was considered by the Committee 12-14 July 1993: see "The Irish Times", 13 and 14 July 1993.

121 Only two cases are explicitly mentioned in para. 166 of the Report: *McGee v. Attorney General* [1974] I.R. 284 (a right to marital privacy) and *Kennedy v. Ireland* [1987] I.R. 587 (a right of individual privacy).

122 Para. 166.

123 Para. 169. On these sections see above paras. 5.38-5.44 & 5.53-5.60.

124 Para. 170.

125 Para. 171. See also para. 170 concerning the former practice; and above ch. 6 concerning this practice and the 1993 Act.

126 Article 57 of the United Nations Charter provides that various specialised agencies shall be brought into relationship with the U.N. in accordance with the provisions of Article 63. Article 63 confers the competence on the Economic and Social Council to enter into agreements with any of these agencies, defining the terms on which the agency concerned shall be brought into relationship with the U.N. Such agreements are subject to approval by the U.N. General Assembly. The UPU became a specialised agency of the U.N. in 1948, the ITU in 1947.

127 Concerning the foundation of the Union, see vol. 1 of the *UPU Annotated Code*, published by the International Bureau, Berne, 1991, pp.viii-ix.

located in Berne, Switzerland.[128] The supreme authority of the Union is Congress. It enjoys legislative powers and comprises a conference of representatives of member countries which meets not later than five years after the Acts of the previous Congress have been put into effect.[129] The present Constitution of the UPU was adopted by the Vienna Congress in 1964,[130] and was subsequently amended at the Tokyo Congress in 1969, the Lausanne Congress in 1974, the Hamburg Congress in 1984, the Washington Congress in 1989 and the Seoul Congress in 1994. The overwhelming number of states in the world today are members of the UPU.[131] Ireland joined in 1923.

7.55 The aim of the Union is "to secure the organization and improvement of the postal services and to promote in this sphere the development of international collaboration."[132] The common rules applicable to the international postal service and the provisions concerning letter-post services are contained in the Universal Postal Convention and its Detailed Regulations.[133] Services other than the letter-post are governed by special Agreements which, in turn, have their own Detailed Regulations.[134] Of these other Agreements, only the Postal Parcels Agreement, together with its Regulations, are of particular interest in the context of the present study.

7.56 No express provision has been made in either the Universal Postal Convention or the Postal Parcels Agreement for the inviolability of the mail, but it has been affirmed on many occasions by various organs of the UPU that the inviolability of postal items is a fundamental principle of the Union. One such recent occasion was the adoption by the Washington Congress of a resolution which stated that it is "the fundamental responsibility of postal administrations to assure the inviolability of postal items", and which urged "members to assess the adequacy of national policies and current legislation governing the security and integrity of mail and to adopt appropriate changes as necessary to achieve improvements in this area".[135]

7.57 Moreover, express provision is made in the basic documents of the UPU

---

128 See Articles 13 and 20 of the UPU Constitution.

129 Unless exceptional circumstances justify the convening of an extraordinary Congress. See Articles 13(1), 14 & 15 of the UPU Constitution and Article 101 of the General Regulations of the UPU. Both the Constitution and the General Regulations are reproduced in vol. 1 of the *Annotated Code*, published by the International Bureau. The last Congress was held in Seoul in 1994. The next Congress will be held in Beijing in 1999.

130 The Constitution came into operation on 1 January 1966: see Article 33.

131 As of 14 September 1994, 189 countries were members.

132 Article 1(2) of the Constitution. See also the Preamble.

133 Article 22(3) of the Constitution.

134 Article 22(4) of the Constitution. These Agreements are the Postal Parcels Agreement, originally agreed in 1880, the Money Orders Agreement, originally agreed in 1878, the Giro Agreement, originally agreed in 1920, and the Cash-on-Delivery Agreement, originally agreed in 1947. The text of the Postal Parcels Agreement and its Regulations are reproduced in vol. 3 of the *UPU Annotated Code*; the text of the other Agreements and their Regulations in vol. 4.

135 Resolution C 12/1989, Action to enhance the security and integrity of international mail, reproduced in Vol. 2 of the *Annotated Code*, at pp.380-382. By this resolution, Congress also instructed:

> "the Executive Council (EC) and the Consultative Council for Postal Studies (CCPS), within their respective areas of responsibility, and with the support of the International Bureau, to convene a group of experts in postal security and to develop and adopt initiatives regarding international policies, standards and programmes which can be undertaken prior to the next Congress."

for freedom of transit for postal items, and implicit in this freedom is the inviolability of these items. Article 1(1) of the UPU Constitution provides that member countries shall comprise, under the title of the Universal Postal Union, a single postal territory for the reciprocal exchange of letter-post items,[136] and that freedom of transit shall be guaranteed throughout the entire territory of the Union. Article 1 of the Universal Postal Convention[137] fleshes out this guarantee by imposing a duty on the postal administration of each member country to forward by the quickest route[138] which it uses for its own items, closed mails and à découvert letter-post items which are passed to it by another administration.[139] Admission in transit à découvert of certain letter-post items may however be refused.[140] Freedom of transit for postal parcels to be forwarded by land and sea routes is limited to the territory of the countries taking part in this service[141]; but freedom of transit for air parcels is guaranteed throughout the territory of the Union.[142]

7.58 Inviolability is of course not absolute. Priority may on occasion need to be given to considerations such as national security, the protection of public safety, including the safety of post office personnel, and the detection and control of contraband. According to an early arbitral award, however, although the principle of inviolability may give way to some extent to the necessities of public order, it may never cede to purely fiscal interests.[143] The requirements of some considerations such as national security and public order are clearly more appropriately determined at the national than at the international level. But, in so far as an aspect of the international postal service is regulated by the UPU, the Union tends to place a high value on the inviolability of the mail. Its practice suggests that, although each country is entitled to inspect mail, closed mail should in general be opened by a competent national authority, such as the customs, rather than by the postal administration and that on occasion the appropriate course of action for a postal administration, in view of the principle of the inviolability of the mail, is e.g. to return an item suspected of containing

---

136 The 1964 Vienna Congress substituted the phrase "envois de la poste aux lettres" ("letter-post items") for the term "correspondances" ("correspondence"): see note 3, p.6, Vol. 1 of the *Annotated Code*. Article 19(1) of the Convention provides:

> "Letter-post items shall consist of:
> a letters and postcards together called "LC";
> b printed papers, literature for the blind and small packets together called "AO"."

The category, small packets, was introduced by the London Congress in 1929 and was created in order to make the rapid means of conveyance of letter post available for small quantities of merchandise with a market value: see vol. 2 of the *Annotated Code*, note 7, p.29. A proposal at the 1989 Washington Conference to include a definition of letters and postcards was rejected.

137 Separate provisions apply according to whether the transit is by land, sea or air: see Art.1(4) and (5). For "postal parcels", see Art. 2 of the Postal Parcels Agreement and vol. 3 of the *Annotated Code*, p.9, note 1.

138 By an amendment made at the Seoul Congress the notion of security was added to that of speed. See *Summary of the main amendments made to the UPU Acts and of the major decisions taken by the 21st Congress* (International Bureau of the UPU, Berne 1995).

139 There are some limits: see Art. 1(2), (4) & (5). See Vol. 2 of the *Annotated Code*, note 6, pp.9-10 for the attempted justification by a country of its interception of a registered letter in transit. The justification was rejected by most other member countries.

140 See Arts. 1(2) & 41(9) of the Convention.

141 Art. 1(4).

142 Art. 1(5).

143 See the summary of published arbitral awards in Vol. 1 of the *Annotated Code*, p.49, no. 1.

prohibited articles to the country of origin rather than to forward it to the national authority.

7.59 Article 41 of the Universal Postal Convention lists letter-post items and articles which shall not be admitted to the post. In particular, paragraph 4 of Article 41 provides:

> "The insertion in letter-post items of the following articles shall be prohibited:
>
> a articles which, by their nature, may cause the dangers or damage mentioned in paragraph 1[144];
> b narcotics and psychotropic substances;
> c live animals[145] ...;
> d explosive, flammable or other dangerous substances[146]; ...
> e obscene or immoral articles[147];
> f articles of which the importation and circulation are prohibited in the country of destination.[148]"

A similar list of prohibitions applying to parcels is contained in Article 20 of the Postal Parcels Agreement. Items containing these prohibited articles which have been wrongly admitted to the post shall be dealt with according to the legislation of the country of the administration establishing their presence.[149] However, items containing certain articles are in no circumstances to be forwarded to their destination, delivered to the addressee or returned to origin.[150] These articles are narcotics and psychotropic substances, explosive, flammable or other dangerous substances, obscene or immoral articles, and additionally, under the Postal Parcels Agreement, radioactive materials.[151] When an item wrongly admitted to the post is neither returned to origin nor delivered to the addressee, the administration of origin shall be notified without delay how it has been dealt with.[152]

7.60 In 1934, at the request of the Bolivian administration, an inquiry was conducted by the UPU whereby the administrations of member countries were asked, *inter alia*, what verification procedures could be taken where the internal legislation of a country prohibits the importation of currency in letters. The administrations replied that they were entitled to apply paragraph 4(f) of Article

---

144 These are items which may expose officials to danger or may soil or damage other items or postal equipment.
145 Some exceptions are specified.
146 The perishable biological substances and radioactive substances mentioned in Article 23 do not fall within this prohibition.
147 It was decided at the Rome Congress in 1906 that it is at the discretion of each administration to decide what constitutes an obscene article.
148 A List of Prohibited Articles is maintained by the International Bureau and member countries should inform the Bureau of their current prohibitions for inclusion in the List.
149 Art. 41(6) of the Convention; Art. 22(1) of the Agreement.
150 Art. 41(7) of the Convention; Art. 22(1) of the Agreement.
151 The admission of radioactive materials to the letter-post is governed by Art. 23 of the Convention.
152 See also the following Articles of the Convention on items wrongly admitted: Arts. 20 (postage charges and limits of weight and size of items), 23 (perishable biological substances and radioactive materials) & 24.

41 of the Convention, but those which replied were also unanimously of the view that, by virtue of the principle of the inviolability of correspondence, the postal service did not possess the necessary powers to carry out an official verification of the content of items and that the discovery of infringements of this kind was merely fortuitous.[153] Some administrations did however state that items suspected of containing currency were submitted to customs control.[154] Article 42 of the Convention now explicitly provides that the postal administrations of countries of origin and destination shall be authorized to submit letter-post items to customs control, according to the legislation of those countries.

7.61 Where a postal administration wrongly diverts an item to the customs or other competent national authority for verification of the content, it may escape liability if the contents are confiscated or destroyed by the authority. An arbitration concerned the passing by the administration of a transit country of a large number of items containing saccharine to the customs. Under the legislation in force in the country, the customs confiscated and destroyed the saccharine. The arbitrators held that it would have been more appropriate for the administration to return the items to the office of origin. However, since the importation of these goods was prohibited not only in the transit country but also in the country of destination and they were therefore contraband goods, and since their illegal character allowed the administration of origin to refuse to pay the indemnity claimed by the sender, the transit administration was relieved of any liability.[155] Both the Universal Postal Convention and the Postal Parcels Agreement now contain provisions expressly exempting postal administrations from liability for certain items confiscated or destroyed by the competent national authority because they contain prohibited articles.[156]

7.62 With the advent of new technology, such as X-ray equipment, and new techniques, such as the use of 'sniffer dogs' for the detection of narcotics, it is of course no longer always necessary to open closed mail in order to check its contents. Some recent decisions of the Washington Congress suggest that, by virtue of the principle of the inviolability of the mail, resort should be had, where possible, to means other than the opening of the mail to combat the improper use of the postal services. The Congress adopted a formal opinion on closed mail in transit suspected of containing narcotics or psychotropic substances.[157] After referring to the importance of the principle of freedom of transit for postal items as guaranteed by Article 1 of the Universal Postal Convention and to the prohibitions listed in Article 41, the opinion invited:

> "postal administrations:
> i - to cooperate in combating the traffic in narcotics and

153 Examples given of fortuitous discovery were accidental opening during handling, claims in respect of correspondence presumed not to have arrived, and undeliverable items.

154 See Vol. 2 of the *Annotated Code*, p.64, note 6.

155 See Vol. 1 of the *Annotated Code*, p.50, no. 9.

156 See Arts. 60(2)(iii) & 61(2)(i)(d) of the Convention, and Art. 41(2)(iii) of the Agreement. See also Arts. 60(2)(ii) & 61(2)(ii) of the Convention and Art. 41(2)(ii) of the Agreement.

157 C 54/1989, reproduced in Vol. 2 of the *Annotated Code*, at pp.389-390.

psychotropic substances whenever they are legally required to do so by their national authorities responsible for this matter;

- to ensure respect for the fundamental principles of the international post, in particular, the freedom of transit (article 1 of the Constitution and of the Convention);

ii to make all appropriate arrangements with the relevant authorities of their countries to ensure that bags of mail in transit suspected of enclosing items containing narcotics or psychotropic substances are not opened, but to advise:

a by the quickest means, at the request of their customs authorities the administration of destination so that the suspected bags can easily be identified on arrival;

b by verification note, the administration of origin of the mail;

iii to approach the legislative authorities, in consultation with the customs services, to ensure that laws and regulations do not prevent the use of the technique known as "controlled delivery"; the customs of the transit country, if necessary with the agreement of the competent authorities, must take appropriate measures to inform the customs authorities of the country of destination and, possibly, of the country of origin of the suspect mails."

Congress also adopted a resolution on the exclusion of dangerous goods from airmail.[158] After referring, *inter alia*, to the prohibition on the transport of dangerous substances, contained in Article 41 of the Universal Postal Convention, the resolution urged:

"postal administrations:

- to strengthen measures aimed at preventing the insertion of dangerous articles in postal items and, where appropriate, at detecting at the time of posting items containing such articles;
- to develop to this end educational measures suited to the local situation, for the benefit of postal users and staff;
- to ensure wide dissemination of these measures and appropriate training of the staff, using the most effective modern technical methods (audiovisual or others)".

By this resolution, Congress also instructed the Executive Council of the UPU to monitor this question closely during the five-year period 1990-1994.[159]

---

158 C 65/1989, reproduced in Vol. 2 of the *Annotated Code*, at pp.393-394.

159 Under the Universal Postal Convention, Article 14(e), the Governments of member countries have undertaken to adopt, or to propose to the legislatures of their countries, the necessary measures, *inter alia*:

"for preventing and, if necessary, for punishing the insertion in postal items of narcotics and psychotropic substances, as well as explosive, flammable or other dangerous substances, where their insertion has not been expressly authorized by the Convention and the Agreements."

(ii) International Telecommunication Union

7.63 Telecommunication services are coordinated and regulated internationally by the International Telecommunication Union, whose seat is at Geneva.[160] The Union is responsible for the regulation, standardization, coordination and development of international telecommunications as well as the harmonization of national telecommunication policies.[161] It dates back to 1865, when it was called the International Telegraph Union.[162] The vast majority of states are today members of the Union.[163] Ireland joined in 1923.

7.64 The main policies of the organisation are decided at Plenipotentiary Conferences held every four years.[164] The ITU was substantially restructured at an Additional Plenipotentiary Conference held in Geneva in 1992, and the present Constitution and Convention of the ITU were adopted at this Conference.[165] Other conferences are convened regularly dealing with specific sectors of telecommunications. Telecommunication Regulations are reviewed and revised at World Conferences on International Telecommunications; and Radio Regulations at Radiocommunication Conferences. Together the International Telecommunication Regulations and the Radio Regulations comprise the Administrative Regulations of the ITU. Both the ITU Constitution, the Convention and the Administrative Regulations are binding under international law on member countries.

7.65 The right of the public to use the international telecommunication service is recognised in the ITU Constitution,[166] and it is provided that the same safeguards shall apply to "all users in each category of correspondence without any priority or preference."[167] Neither the Constitution, the Convention nor the Regulations require any specific safeguards with regard to the secrecy of telecommunications, but the matter is addressed generally. Article 37 of the Constitution reads:

> "1. Members agree to take all possible measures, compatible with the system of telecommunication used, with a view to ensuring the secrecy of international correspondence.
>
> 2. Nevertheless, they reserve the right to communicate such correspondence to the competent authorities in order to ensure the application of their national laws or the execution of international conventions to which they are parties."

---

160 The headquarters of the organisation were transferred in 1948 from Berne to Geneva.

161 See Art. 1 of the ITU Constitution.

162 See, e.g., *The International Telecommunication Union*, published by the ITU, Geneva, 1994, pp.3-4.

163 As at 24 May 1994, 184 countries were members.

164 See Art. 8 of the ITU Constitution and Art. 1 of the ITU Convention.

165 Ireland signed the Constitution and the Convention at the Additional Plenipotentiary Conference in 1992, but, as at 19 August 1994, had not yet ratified them.

166 Art. 33.

167 It is also provided that services and charges shall be the same. The provision must however be read in the light of subsequent provisions which both allow and require priority to be given to certain types of communication, e.g., government communications and distress calls: see Arts. 40, 41 & 46 of the Constitution and Art. 5 of the International Telecommunication Regulations.

The principle of secrecy is therefore endorsed by the organisation, but it seems that the application of this principle has been left largely to national authorities. Paragraph 1 contains a strongly worded obligation in that members must take "all possible measures" to ensure the secrecy of international correspondence. Such measures will of course include the legal, but are not limited thereto. Thus Members should ensure, e.g., that the postal administration is so organised that it is not easy casually to overhear such correspondence. The obligation is tempered by the qualification which recognises that the system of telecommunication used may place limits on the measures which can be taken. Moreover, paragraph 2 allows Member States to monitor international telecommunications. It does however suggest that any interference with the secrecy of such telecommunications should be reserved to a competent national authority and that it should have a basis in either national or international law.

7.66 Article 34 of the Constitution specifically allows Members to interrupt private telecommunications on a number of grounds:

> "1. Members reserve the right to stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage of any such telegram or any part thereof, except when such notification may appear dangerous to the security of the State.
>
> 2. Members also reserve the right to cut off any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency."

The references to Members' "laws" means that the grounds specified, namely, State security, public order and public decency, are not the only grounds on which a Member may intercept a private telecommunication. Rather interception on other grounds is permitted provided legal provision exists in the member country for such interception.

7.67 No specific provision governs the interruption or interception of foreign government telecommunications; but it is provided that "Government telegrams and service telegrams may be expressed in secret language in all relations."[168] Freedom of transit must generally be provided for private telegrams in secret language[169]; but Members may refuse to admit such telegrams which are destined for their territory.[170]

7.68 In addition:

---

168 Art. 40(1) of the Convention.
169 Art. 40(3) of the Convention.
170 Art. 40(2) of the Convention.

"Each member reserves the right to suspend the international telecommunication service, either generally or only for certain relations and/or for certain types of correspondence, outgoing, incoming or in transit, provided that it immediately notifies such action to each of the other members through the medium of the Secretary-General."[171]

Conclusion

7.69 Ireland's international obligations provide some clear pointers as to the measures needed in respect of surveillance and the interception of communications in order to protect individual privacy. They specify the grounds and delineate the scope of permitted state action. The State's obligations under the European Convention on Human Rights are of particular significance in this regard, not only in themselves but also by virtue of the impact of the Convention on the law of the European Union. They require a legal basis for any interference with privacy and that the law be worded with a sufficient degree of clarity and precision to enable persons to discover the circumstances in which they may be subject to surveillance and any conditions pertaining thereto. Moreover, they require the existence of substantial safeguards against any abuse of a power of surveillance. Other international obligations of the State confirm these requirements, though usually in a more general fashion.

7.70 The State's obligations under both the European Convention on Human Rights and the International Covenant on Civil and Political Rights also indicate that some legal protection must exist in respect of surveillance by other actors than the State. The scope and content of this protection has as yet been less well defined by either the European Court and Commission of Human Rights or the Human Rights Committee than that required in respect of surveillance by the State; but a complete lack of any such protection would clearly not accord with Ireland's obligations under these treaties.

7.71 Developments within the European Union are of interest not only for their endorsement of the standards contained in the European Convention, but also because of the emphasis on freedom of goods and services and the detailed regulation of postal and telecommunications equipment and services. As regards the latter, the protection of privacy has been recognised as a ground on which access to and use of networks and services may be restricted, and in delineating the scope of permissible restriction, the European Council has enunciated much the same criteria as has the European Court of Human Rights in respect of interference with privacy - that any restriction should be objectively justified and be proportionate to the aim pursued, i.e. not excessive. The difference is that, whereas the European Court of Human Rights has posited these criteria for restrictions on privacy, the European Council has utilised them in respect of restrictions on access to and use of telecommunications services and networks.

---

171 Art. 35 of the Constitution.

7.72 Developments within the Universal Postal Union and the International Telecommunication Union are also of some interest. In particular, although states members of the UPU are required to prohibit the inclusion in letter-post of certain articles, by virtue of the principle of the inviolability of the post, postal administrations do not generally enjoy freedom to open international post suspected of containing such articles. Rather any such control should be exercised by the customs authorities of the state concerned. Moreover, it appears to be current UPU policy that, whenever possible, other means than the opening of post should be availed of to counter abuse of the postal system.

PART 4: PROPOSALS FOR REFORM

CHAPTER 8: THE ISSUES

Introduction

8.1 In this Chapter we shall review the existing constitutional and legal protection against invasive surveillance, focusing on the gaps and inadequacies in this protection. In the course of our review, we will identify the main issues we will be addressing in the rest of the Paper and give our general approach thereto. But before engaging in this review, we should first give some thought to whether any of the interests which may compete with privacy merit treatment as a special case.

8.2 We stated in Chapter 1 that in this Paper we would be considering the threat posed by surveillance to privacy in general. We are reserving for a later study an examination of the protection of privacy in specific institutional contexts since distinct considerations often apply in such contexts, as when a person is employed in the workplace or has been imprisoned for a criminal offence.[1] Distinct considerations may also apply in some cases of conflict between privacy and a competing interest. As the superior courts have indicated,[2] not all interests carry equal weight.

8.3 We mentioned earlier that privacy is not a value to be upheld at all costs.[3] It may legitimately be restricted to some extent in the public interest or in order to protect the rights and freedoms of others, and there will be circumstances in which a countervailing interest should be afforded priority. The public interests in national security and in the prevention and detection of crime are important interests in any society, and it is usually accepted that the State is entitled to act on behalf of the community, indeed that it should so act, in order

---

1 See above para. 1.8.
2 See above para. 3.11.
3 See above para. 3.10.

to protect these interests. As a consequence, the State also usually enjoys powers which are not given to ordinary citizens in order to fulfil its role as public protector. Such special powers are recognised in Irish law in relation to the interception of communications, and their exercise has been subjected to extensive legal regulation by the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. We shall consider these powers and the applicable legal controls in Chapter 12. State resort to visual surveillance, and to aural surveillance other than in the context of the interception of communications, is not at present specifically regulated by law. Not only is the precise legal basis of such conduct by the State uncertain, but such surveillance is carried out within the parameters of the general law, the agents of the State neither enjoying any special powers in this regard nor being subject to any specific legal constraints. These apparent legal voids will be addressed in Chapter 10 in relation to visual surveillance and in Chapter 11 in relation to aural surveillance.

8.4 In addition to national security and the prevention and detection of crime in relation to which the State plays a special role, there may be sectoral interests which, by virtue of the importance attached to them in a democracy such as Ireland, deserve special treatment. The clearest example of candidacy for special treatment is perhaps the media. The media play an important role in the dissemination and discussion of ideas and information. Moreover, by investigating matters of public importance and informing the public thereof, they can act as watchdogs for society, alert to abuses of power in any quarter and be instrumental in bringing them to public notice. As a judge of the English Court of Appeal has said:

> "The media, to use a term which comprises not only the newspapers but also television and radio, are an essential foundation of any democracy. In exposing crime, anti-social behaviour and hypocrisy and in campaigning for reform and propagating the views of minorities, they perform an invaluable function."[4]

Given the very high value attached to freedom of expression,[5] it is appropriate that we should consider whether the media should be treated as a special case in relation to the use of surveillance and the publication of information obtained thereby or whether the same general rules should apply to them as to everyone

---

4 *Francome v. Mirror Group Newspapers* [1984] 1 W.L.R. 892 at 898; [1984] 2 All ER 408 at 413 (Sir John Donaldson, M.R.). The Constitution explicitly recognises the media as organs of public opinion while requiring the State to ensure that their freedom of expression is not used to undermine public order or morality or the authority of the State: see Article 40.6.1°i.

5 The press has been described as "a vital institution of a free society": see the *Report of the Committee on Privacy*, Cmnd. 5012, 1972, para. 126. See also *Müller and Others v. Switzerland*, Judgment of the European Court of Human rights, 24 May 1988, Series A, No. 133, para. 33, 13 E.H.R.R. 212 at 229, where the Court described freedom of expression as "one of the essential foundations of a democratic society, indeed one of the basic conditions for its progress and for the self-fulfilment of the individual"; and *Informationsverein Lentia v. Austria*, Judgment of the European Court of Human Rights, 24 November 1993, Series A, No. 276, para. 38, 17 E.H.R.R. 93 at 113. The Court has however also stressed that, according to the wording of paragraph 2 of Article 10 of the European Convention on Human Rights, the exercise of this freedom carries with it duties and responsibilities: *ibid.*, para. 34.

else.

The Media

8.5 Public concern has been voiced in recent years about invasions of privacy by the media, particularly by the press. Much of the concern has arisen as a result of the publication of intimate private details of the lives of public figures, including photographs.[6] Concern also stems however from the photographing and interviewing of ordinary citizens in circumstances of great personal tragedy.

8.6 This concern is not new. Over twenty years ago, the Younger Committee on Privacy received more complaints about the activities of the press than on any other aspect of the subject.[7] These complaints showed two general areas of concern. One was that the press sometimes use objectionable means to obtain information. The other was that they give widespread publicity to information, however obtained, which is regarded as private.[8]

8.7 Concern over privacy-invasive media activity has been particularly strong in Britain. The Younger Committee considered the press and broadcasting in the overall context of a study of the "protection [of] the individual citizen and [of] commercial and industrial interests against intrusions into privacy by private persons and organisations, or by companies".[9] With particular reference to technical surveillance devices, the Committee thought it right to maintain the important principle that the law in this area[10] should apply to those working for the press and broadcasting as it does to all other persons.[11] In more recent years however the press has been picked out for special attention. There had been severe public criticism of sections of the press for intruding upon accident victims and other patients in hospital, for using stolen private correspondence or photographs and for publishing scurrilous details of individuals' private lives.[12] Consequently, a Committee, chaired by David Calcutt Q.C., was appointed in 1989 to consider whether further protection should be afforded privacy in such circumstances; and three years later, in 1992, Calcutt was again asked to undertake a follow-up review of the situation.

8.8 It has frequently been remarked that not everything which is of public interest is in the public interest. Moreover, it has been said of this distinction that it "is of great importance in attempting to set the bounds at which the right

---

6 See, e.g., above paras. 4.55 & 4.67 for examples.

7 See the Committee's *Report*, para. 116.

8 More complaints fell into the latter category than into the former.

9 *Report*, para. 1.

10 And in other matters.

11 See the Committee's *Report*, paras. 186 & 238. It recommended that there should be a new criminal offence of unlawful surveillance by surreptitious means: *ibid.*, paras. 562-563. This recommendation was not implemented, largely because of the difficulty of defining the act which it was intended to prohibit: see *Report of the Committee on Privacy and Related Matters (Calcutt I)*, Cm 1102, 1990, para. 6.9.

12 See *Calcutt I*, para. 1.5.

to be informed should give way to the right to privacy."[13] Like privacy, freedom of expression is not an absolute value, and there will be circumstances in which the latter should cede precedence to the former. Given the importance in a democracy of both privacy and freedom of expression, the task of balancing these interests will however often be a difficult one. What we examine here is whether, in the context of surveillance, special rules should apply to this balancing of interests or whether the same rules should apply to the balancing of these interests as to the balancing of privacy and other interests.

(i) Regulation of broadcasting

8.9 Broadcasting is regulated by statute in Ireland and additionally, in the independent sector, by contract and licence. As part of this regulation, substantial legal obligations have been placed on the broadcasting authorities in order to safeguard various public interests. Among the interests explicitly protected is that of privacy. Both RTE and independent broadcasting contractors must respect persons' privacy in the making and transmission of programmes.

8.10 Section 18(1B) of the *Broadcasting Authority Act, 1960*[14] provides that RTE "shall not, in its programmes and in the means employed to make such programmes unreasonably encroach on the privacy of the individual."[15] Similarly, with respect to independent broadcasting, sections 9(1)(e) and 18(1) of the *Radio and Television Act, 1988* require every sound broadcasting contractor and television programme service contractor to ensure that "in programmes broadcast by [the contractor], and in the means employed to make such programmes, the privacy of any individual is not unreasonably encroached upon."[16]

8.11 RTE has spelt out its understanding of this statutory duty and its implications for staff in its *Broadcasting Guidelines for RTE Personnel*.[17] Its "very firm guidelines"[18] on privacy recognise that "[t]he problems of intrusion into personal privacy have become a major issue with the development of very sensitive surveillance and recording devices",[19] and specifically address the covert use of such devices as follows:

> "3. The use of surreptitious recording and filming devices that would be altogether outside normal recording and filming practice is ruled out, except in the most exceptional cases where

---

13 *Report of the Committee on Privacy*, para. 157. Cf. *Calcutt I*, paras. 3.19-3.23; and *Review of Press Self-Regulation (Calcutt II)*, Cm 2135, 1993, paras. 4.13, 34f. & 56. See also the reference in *Calcutt II*, at para. 5.18, to the distinction drawn by Viscount Astor between the public right to know and what the public delights to know.

14 As substituted by s.3 of the *Broadcasting Authority (Amendment) Act, 1976.*

15 See also s.17(b), as substituted by s.13 of the *Broadcasting Authority (Amendment) Act, 1976.*

16 See also s.18(3)(b).

17 Published by RTE, 1989.

18 *Broadcasting Guidelines*, p.32.

19 *Ibid.*

compelling reasons may be advanced for suspending the general prohibition and where the means proposed to be employed would not, in the circumstances, be regarded as constituting unreasonable encroachment on privacy.

4. The criteria to be used in determining such cases are as follows:
   - 4.1 The activity to be recorded by such means must be widely accepted as gravely anti-social.
   - 4.2 The broadcasting of the information or event so obtained must be recognised as serving a really important public purpose which could not be achieved by other means.
   - 4.3 The use of such methods or devices must be shown to be indispensable to the achievement of this purpose.
   - 4.4 Such use must not contravene the law.
   - 4.5 The matter is so important in itself and one in which consistency of judgement is so vital that the prohibition on the use of such methods and devices can be lifted only by the personal decision of the Director General, to whom the matter should be referred by the appropriate Divisional Head."[20]

The *Guidelines* are also of interest for what is considered by RTE to fall outside its legal, including its statutory, obligations in respect of privacy:

> "RTE would not consider it is obliged under law to ensure the privacy of individuals in a street scene or whilst attending a public event such as a sports meeting, parade or demonstration and it would be wholly impracticable to obtain the permission of every individual televised. Individuals included in such recordings are seen to be part of the general public and can reasonably be expected to have assumed their presence there and participation might be recorded for broadcasting and other publication. Where, however, as in documentaries recorded in such public institutions as hospitals, Government offices, factories and other public and private places where individuals attend for their private purposes, the identity of an individual is materially relevant to the subject matter of the programme, and editorially significant, then it is reasonable that as a general rule the individual's consent should be obtained. It is for the programme maker to be satisfied that an individual's presence in any place and his activities there are sufficiently in the public domain to justify his inclusion in a recording without the individual's express permission being obtained. If in doubt the programme maker can seek the advice of senior colleagues. The recording of what is clearly an uninvited attendance by a reporter at an individual's home for the purposes of obtaining an interview or comment

---

20 *Ibid.*

and an attempt to interview or get comment from an unwilling individual at his office, as he enters his car or as he walks along the pavement all require sensitive consideration. There may be circumstances when aggressive techniques could reasonably be construed as harassment and an unreasonable encroachment on an individual's privacy."[21]

The Independent Radio and Television Commission is empowered by the *Radio and Television Act, 1988* to draw up codes of practice, *inter alia*, in relation to the statutory obligations of broadcasting contractors regarding privacy,[22] but has not to date done so.[23]

8.12 A member of the public may complain to the Broadcasting Complaints Commission about an alleged breach of these statutory duties by RTE or a broadcasting contractor.[24] Decisions of the Commission receive some publicity. Apart from being reproduced in the Commission's *Annual Reports*, they are forwarded to the Government Information Services for circulation to the national newspapers and, where relevant, are published in the *RTE Guide*. The Commission has to date decided only one complaint of an invasion of privacy, which complaint did not involve surveillance or the intrusive use of aural or visual devices.[25] Also, the Independent Radio and Television Commission has the power to suspend or terminate the contract of an independent broadcaster for serious or repeated breaches of its obligations under the Radio and Television Act.[26]

(ii) Regulation of the press

8.13 In contrast to broadcasting, the print media are not subject to specific statutory regulation, but rather are governed by the general law of the State. The National Union of Journalists produces a Code of Conduct for its members, and the Code has been accepted by many of the Irish national newspapers as part of a house agreement with the Union.[27] Two provisions of the Code in particular

---

21 At p.33.

22 Sections 9(3) & 18(1).

23 However the contract between the Independent Radio and Television Commission and a broadcasting contractor contains a term relating to privacy: see above para. 4.68.

24 Section 18B(1)(d) of the *Broadcasting Act, 1960*, as substituted by s.4 of the *Broadcasting Authority (Amendment) Act, 1976* and regulations made by the Minister for Tourism, Transport and Communications under ss.11(3) and 18(1) of the *Radio and Television Act, 1988*. The Radio and Television (Complaints by Members of the Public) Regulations, 1992 (S.I. No. 329 of 1992) extend the remit of the Broadcasting Complaints Commission to the independent broadcasting services provided under the 1988 Act. On the handling of complaints by the Commission see, in general, E.G. Hall, *The electronic age*, Oak Tree Press, Dublin, 1993, ch. 22.

25 The complaint related to a television programme during which some young children were clearly identifiable as having been victims of sexual abuse. The Commission was unanimously of the view that there had been a gross violation of the children's right to privacy. See the *Ninth Annual Report of the Broadcasting Complaints Commission*, 1987, p.2.

Cf. the rejection by the British Broadcasting Complaints Commission, on 28 September 1994, of a complaint, brought by a woman on her own behalf and on behalf of her young daughter, that the secret use of sound recording equipment by journalists in her home and the showing on television of a film of her house infringed their privacy: see (1995) 145 *New Law Journal* 226. The broadcast concerned the work of detectives in tracking down and arresting the girl's father, a paedophile, who was convicted of indecency involving young boys.

26 Sections 14(4)(a)(ii) and 18(1).

27 The Code is reproduced at Appendix A of the *NUJ Rule Book 1994*.

deal with matters of privacy. Provision 5 states:

> "A journalist shall obtain information, photographs and illustrations only by straight-forward means. The use of other means can be justified only by over-riding considerations of the public interest. The journalist is entitled to exercise a personal conscientious objection to the use of such means."

Provision 6 reads:

> "Subject to the justification by over-riding considerations of the public interest, a journalist shall do nothing which entails intrusion into private grief and distress."

An Ethics Council considers alleged breaches of the Code of Conduct.[28] Where the Ethics Council is of the opinion that a member is guilty of a breach of the Code, it may deliver a reprimand and/or recommend to the National Executive Council of the Union that one or more of a number of penalties be imposed.[29] These penalties are a fine not exceeding the sum of £1,000, suspension from the Union for a period not exceeding 12 months, censure and expulsion from the Union.[30] Complaints about alleged contravention of the NUJ Code of Conduct may only be entertained by the Ethics Council when they are made by NUJ branches or individual NUJ members.[31] In addition, each national newspaper has in recent years appointed a person to deal with readers' complaints. These complaints are dealt with internally by the newspaper itself. Irish newspapers do not have standing editorial instructions on the conduct of reporters, and it seems that complaints are therefore assessed and processed in accordance with practice and tradition.

(iii) Calcutt I

8.14 In 1989 in Britain, in the light of public concern about intrusion by the press into the private lives of individuals, a Committee was appointed to consider:

> "... what measures (whether legislative or otherwise) are needed to give further protection to individual privacy from the activities of the press and improve recourse against the press for the individual citizen, taking account of existing remedies, including the law on defamation and breach of confidence",[32]

and to make recommendations. The Committee looked at two distinct categories of intrusion into privacy: (i) physical intrusion by reporters and/or

---

28 See Rules 18(c) and 22 of the *NUJ Rule Book 1994*.
29 Rule 22(l).
30 See Rule 18(a).
31 Rule 22(c).
32 *Calcutt I*, para. 1.1.

photographers, and (ii) publication of intrusive material.[33] Since the Committee's terms of reference specified intrusion by the press, it did not specifically examine intrusion in the context of broadcasting, but it did seek to take account of existing controls and remedies in the broadcasting field and of the possible impact of its conclusions on other media.[34]

8.15 The Committee recognised that physical intrusion by the press can take a variety of forms and thought that there was, and could be, no single remedy to tackle the various forms of intrusion. Rather each should be tackled individually.[35] It singled out for attention three particular forms of intrusion: harassment, surveillance and trespass.

8.16 In addressing harassment, it considered s.7 of the *Conspiracy and Protection of Property Act, 1875*.[36] In its view, the offence created by this Act could cover besieging a person's house or following a person from place to place with the aim of making the person give an interview when she or he did not wish to. In theory it could be committed by journalists following someone or surrounding a person's house. However, the Act had largely fallen into disuse and, in practice, it was unlikely that it would be invoked against the press. The police normally limited themselves to moving the press aside so that other persons could pass. Referring directly to *Raffaelli v. Heatley*,[37] the Committee also mentioned that in Scotland many forms of harassment would be covered by the common law offence of breach of the peace, and that to constitute a breach of the peace it was not necessary that an act have been committed in a public place.[38] Entering someone's house and refusing to leave, or taking photographs through a person's window, could constitute a breach of the peace if the person could reasonably be expected to be alarmed, upset or annoyed or if the conduct was calculated to result in a public disturbance. If the presence of journalists was offensive, the police could remove them on the basis of a threatened breach of the peace. The Committee also considered and rejected the creation of a statutory tort of harassment.[39] It was not persuaded that a general tort of harassment would provide a practical solution to the problem of harassment by the press. It remarked that press harassment often occurs at times when persons are at their least resilient, as during bereavement, and that, to be of practical value, any remedy would need to be capable of immediate invocation.[40]

8.17 With regard to covert surveillance, the Committee pointed out that resort to this method of obtaining information was not peculiar to the media.[41] It is used in industrial espionage, marital disputes, for security in shops and offices

---

33 *Ibid.*, para. 2.4 and ch. 4.
34 *Ibid.*, para. 2.5.
35 *Ibid.*, para. 6.1.
36 See above paras. 5.21-5.22; and para. 6.2 of *Calcutt I*.
37 [1949] J.C. 101, and see above para. 5.2.
38 Citing *McMillan v. Normand* [1988] S.C.C.R. 269.
39 *Calcutt I*, para. 6.23-6.25. There is no tort of harassment in English law: see *Patel v. Patel* [1988] 2 F.L.R. 179.
40 It was also of the view that, while such a tort might protect an individual against a particular intrusive reporter, it was difficult to see how it could reasonably be applied to a crowd of reporters or photographers whose conduct collectively but not individually amounted to harassment: *ibid.*, para. 6.25.
41 *Ibid.*, para. 6.9.

and might include casual eavesdropping by neighbours. In its opinion, the worst forms, such as planting secret bugging devices, are more likely to arise in connection with industrial espionage than with press investigations. The surveillance devices normally used by the press are long range cameras and concealed microphones carried by reporters.[42]

8.18 As regards trespass, the Committee noted that there is no general criminal offence of trespass to land in either England, Scotland or Wales, and that there is little protection under the criminal law against intrusion on private property.[43] The torts of trespass and nuisance, in particular trespass, can be used to protect an individual's privacy from unjustified intrusion.[44] They can theoretically provide a remedy against physical harassment both directly, through unauthorised presence on someone's land, and indirectly, for instance by telephone.[45] On the principle of vicarious liability, the law would apply not merely to reporters and photographers but also to any employers they might have. In practice, however, these remedies are little used. Moreover, the law of trespass is designed primarily to protect a person's land and enjoyment of it rather than to protect privacy as such.[46] It does not generally protect a person from harassment or surveillance from outside his or her property. Unless an actual trespass is or is about to be committed, merely to approach a person's house does not constitute grounds for an injunction. The civil law of trespass, therefore, has little impact on the intrusion caused by the press massing outside a house in the hope of securing a story.

8.19 The Committee considered extending the law of trespass to include any unauthorised entry or surveillance of premises without the occupant's consent.[47] It thought that this might offer a solution to a number of abuses. It might provide a remedy in 'foot in the door' cases, where a reporter camped outside someone's premises, where a photographer used a long range lens, and the use of long range listening devices. It also considered extending the tort of nuisance to cover watching or besetting an individual with a view to pressuring the individual into altering his or her lawful conduct (e.g. refusal to grant an interview) or which had that effect (e.g. preventing a person from sunbathing in the garden). The Committee did not recommend a statutory extension of either of these torts. It was not persuaded that they would provide any effective additional recourse for an individual against harassment by the press.[48]

---

42 The Committee was however made aware of one allegation concerning the planting of a bugging device to obtain information about a well-known actor: *ibid.*

43 *Ibid.*, para. 6.10.

44 See *ibid.*, paras. 6.12-6.19 on civil remedies.

45 See above p.77, n.24.

46 See further above paras. 4.4-4.8.

47 *Ibid.*, para. 6.26.

48 Also, as with its rejection of the creation of a general tort of harassment, the Committee was of the opinion that while such extensions might provide some protection against a particular intrusive reporter or photographer, they wouldn't necessarily afford protection against the collective conduct of a number of reporters or photographers, and that, anyway, it was rare for any action to be brought where one or other of the torts was available under the present law against reporters or photographers: *ibid.*, para.6.28. The Committee also considered and rejected the creation of a statutory tort of infringement of privacy, in particular, by the publication of personal information, including photographs: see ch. 12 of *Calcutt I.*

8.20 Instead the Committee recommended the creation of three new criminal offences which would be targeted specifically at abusive physical intrusion by the press. The Committee took the view that only the criminal law can guarantee prompt relief to the victim and provide a sufficient deterrent to the intruder.[49] It identified the main concern of a victim of physical intrusion, whether of harassment, surveillance or trespass, as being for the intrusion to be stopped immediately as by the police arresting or removing those who are intruding. A civil remedy cannot be described as instant and requires action by the victim who may not be in a state to take it or who may be deterred by the legal process. The offences it recommended are:

> "a. entering private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication;
>
> b. placing a surveillance device on private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication; and
>
> c. taking a photograph, or recording the voice, of an individual who is on private property, without his consent, with a view to its publication with intent that the individual shall be identifiable."[50]

8.21 The Committee further recommended that it should be a defence to any of the proposed offences that the act was done:

> "a. for the purpose of preventing, detecting or exposing the commission of any crime, or other seriously anti-social conduct; or
>
> b. for the protection of public health or safety; or
>
> c. under any lawful authority."[51]

8.22 It also considered and rejected the creation of a further offence of publishing any photograph, recording or information obtained by any of the forms of intrusion to be penalised, knowing or having reason to believe that it had been so obtained.[52] While it was not as such against the creation of an offence which would catch the publisher and editor as well as the journalist, it was wary of

---

49 *Ibid.*, para. 6.30.

50 *Ibid.*, para. 6.33. "Private property" would be defined as any private residence, together with its immediate curtilage (garden and outbuildings), but excluding any adjacent fields or parkland. It would also cover hotel bedrooms (but not other areas in a hotel) and those parts of a hospital or nursing home where patients are treated or accommodated.

51 *Ibid.*, para. 6.36.

52 *Ibid.*, para. 6.37.

creating an offence of publishing material in a newspaper where the point at issue would be how the material was obtained rather than the content. It also bore in mind that, in appropriate circumstances, a proprietor or editor could be prosecuted as an accessory to the offences it was proposing or for conspiracy. The Committee did however favour the creation of a statutory right of action against the publisher of material so obtained. In its view, "anyone having a sufficient interest"[53] should be able to apply for an injunction or, if the material had already been published, for damages or an account of profits. It considered that "such a tightly-drawn civil remedy, closely linked to acts that most people would regard as clearly wrong, would tackle many of the worst forms of infringement of individual privacy"[54] by members of the press.

(iv) Calcutt II

8.23 Consequent on the *Report of the Committee on Privacy and Related Matters (Calcutt I)*, a new regulatory body, the Press Complaints Commission, was established on a non-statutory basis. When this new body had been in operation for some 18 months, the Secretary of State for National Heritage asked Calcutt to assess the effectiveness of press self-regulation and to consider whether any further measures might be needed to deal with intrusions into privacy by the press. His review of self-regulation was submitted to the Secretary early in 1993.[55]

8.24 In this context Calcutt reconsidered the criminal offences proposed by the Committee in 1990 and the associated civil remedy, none of which had been implemented by the Government. He remained of the view that the most blatant forms of physical intrusion - practices involving doorstepping, bugging and the use of long-range cameras - should be outlawed, and accordingly recommended that the offences and the attendant civil remedy should, with modifications, be enacted.[56] He recommended that the offence of entering private property be extended to remaining on private property.[57] This was to catch the reporter or journalist who, having lawfully entered private property, failed to leave when asked to do so.[58] He proposed that the offence of placing a surveillance device on private property be supplemented by the addition of an alternative offence of using a surveillance device (whether on private property or elsewhere) in relation to an individual who is on private property, without the consent of the individual

---

53 *Ibid.*, para. 6.38.

54 *Ibid.*, para. 12.33.

55 *Review of Press Self-Regulation (Calcutt II)*, Cm 2135, 1992.

56 See *Calcutt II*, paras. 5.37 & 7.4. To the argument that it was odd that the offences would apply to those who collect information, but not to those who may subsequently make use of it by publishing it, he reiterated and endorsed the view of the earlier Committee that the case had not been made out for an additional offence of publication. He also pointed out that, under the Committee's proposals, the individual concerned would be able to apply for an injunction restraining the publication of any material obtained by means of any of the criminal offences or, if the material had already been published, for damages for any loss suffered or an account of profits: see *ibid.*, para. 7.6.

57 *Calcutt II*, para. 7.25.

58 *Ibid.*, para. 7.10. He pointed out that a reporter who walks up the path to the front door of a house to make proper inquiries would not thereby commit a criminal offence, simply because she or he had not first obtained express permission to do so. In the absence of any notice to the contrary, householders give their implied consent to anyone to knock on the door for any proper purpose.

to such use, with intent to obtain personal information about that individual with a view to its publication.[59] This extension was intended to meet criticism that the limitation of the offence to the placing of a surveillance device on private property would not meet the nub of the problem since it is possible for a surveillance device to be used effectively at a considerable distance from the target.[60] "Surveillance device" should be defined to mean "any equipment which enables personal information to be obtained without the knowledge of the person concerned or the lawful occupant, as the case may be."[61] As to the third category of offence, the taking of a photograph or recording the voice of an individual, he suggested that the wording be tightened to make clear that the individual's lack of consent related to the taking of the photograph or recording of the voice.[62] The offence was not meant to cover circumstances in which a journalist might record a telephone conversation she or he had with another person, who might be on private property, even though consent had not been obtained.[63] Rather the act to be outlawed was the surreptitious recording of a conversation to which the person making the recording was not party.[64] "Publication" should generally be defined as meaning publication by the media.[65] It should not cover the simple act of passing the material from one person to another. In the specific context of recording, "publication" should be defined to mean making generally available the soundtrack of part or all of the recording. It should not extend to publication of the transcript of a recording.[66] Also, the definition of "private property" should be extended to include school premises.[67]

---

59 *Ibid.*, para. 7.25.

60 See *ibid.*, para. 7.14.

61 *Ibid.*

62 *Ibid.*, para. 7.25.

63 See *ibid.*, para. 7.16.

64 *Ibid.* These intentions would appear however not to be reflected in the actual wording of the proposed offence which is broad enough to catch a person who is party to a conversation, and even tighter wording would seem to be required to exclude such situations. Moreover, it is not altogether clear whether or not criminal liability attaches in some circumstances. If a journalist has a conversation with someone, and the conversation is secretly recorded by a third party who is an associate of the journalist, e.g. sitting in a car parked some distance away, is that person exempt from criminal liability because she or he acted in tandem with the journalist, or is the person guilty of a criminal offence, and if the person is guilty of an offence, is the journalist also guilty by way of complicity in the offence?

On participant monitoring (recording a conversation to which one is party) see further below paras. 11.37-11.44.

65 *Calcutt II*, para. 7.13.

66 *Ibid.*, para. 7.13.

67 *Ibid.*, para. 7.9. The proposed offences, as modified, are:

> "(a) entering or remaining on private property without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication; or
>
> (b) (i) placing a surveillance device on private property without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication; or
>
> (ii) using a surveillance device (whether on private property or elsewhere) in relation to an individual who is on private property, without the consent of the individual to such use, with intent to obtain personal information about that individual with a view to its publication: or
>
> (c) taking a photograph, or recording the voice, of an individual who is on private property, without his consent to the taking or recording, with a view to its publication and with intent that the individual shall be identifiable.": para. 7.25.

8.25 As well as proposing that the offences should be extended, Calcutt recommended that there be two additional defences. These are that the act was done "for the purpose of preventing the public from being misled by some public statement or action of [the] individual"[68]; or "for the purpose of informing the public about matters directly affecting the discharge of any public function of the individual concerned."[69] Calcutt also recognised that the defence of publication for the purpose of exposing seriously anti-social conduct might pose difficulties of interpretation and application in particular cases and that it may in fact prove "too difficult a concept for criminal legislation".[70] Nevertheless he retained it among the proposed defences.[71] He recommended that the offences should be summary only, punishable with a fine but not imprisonment.[72] Moreover, in spite of the view of the earlier Committee that the main concern of a victim of physical intrusion is that the intrusion be stopped immediately as by the police arresting or removing those who are intruding,[73] he proposed that the offences should not carry a power of arrest. In his opinion, if the police had reason to believe that a journalist was committing an offence, they could report the person, and existing powers of enforcement would probably be adequate.[74] He also recommended that a prosecution for any of the offences should be brought only with the consent of the Director of Public Prosecutions.[75]

8.26 Calcutt also reiterated the recommendations of the Committee on Privacy and Related Matters with respect to applications for an injunction and for damages or an account of profits in the event of publication.[76] These civil remedies should be available if the commission of an offence could properly be inferred. It should not be necessary "to prove the offence to conviction".[77] Moreover, they should be available if the act set out in any of the proposed offences took place outside the jurisdiction, if it was done with a view to publication within the jurisdiction.[78] The same defences should be available as

---

68 *Ibid.*, para. 7.26.
69 *Ibid.*
70 *Ibid.*, para. 7.21.
71 He recommended that the burden of proving a defence should fall on the defendant, but would be discharged on a balance of probabilities: para. 7.23. The modified list of proposed defences reads:

> "(a) for the purpose of preventing, detecting or exposing the commission of any crime or other seriously anti-social conduct; or
>
> (b) for the purpose of preventing the public from being misled by some public statement or action of that individual; or
>
> (c) for the purpose of informing the public about matters directly affecting the discharge of any public function of the individual concerned; or
>
> (d) for the protection of public health or safety; or
>
> (e) under any lawful authority.": para. 7.26.

72 *Ibid.*, para. 7.24.
73 See above para. 8.20.
74 *Calcutt II*, para. 7.24.
75 *Ibid.*, para. 7.22. No specific reason was given for this view.
76 *Ibid.*, para. 7.27.
77 *Ibid.*, para. 7.28.
78 *Ibid.*, para. 7.29.

in the case of the proposed criminal offences.[79]

8.27 He pointed out that the offences he was proposing would not apply only to journalists.[80] It was true that they would only apply where there was an intent to obtain material 'with a view to its publication'; but, within that limitation, the offences would be of general application and could be committed by anyone who made the physical intrusion.

(v) A special case?

8.28 While neither the Younger Committee on Privacy nor the later Committee on Privacy and Related Matters and Calcutt Review of Press Self-Regulation recommended that the media be treated as a special case in relation to the acquisition of personal information or its publication, *Calcutt I* and *Calcutt II* did favour the creation of new criminal offences and torts which might be described as media-oriented in that they would impact most significantly on this sector.

8.29 We too shall be recommending the introduction of a number of criminal offences and statutory torts to counter the threats posed to privacy by surveillance.[81] We believe that the criteria we shall propose for balancing the interests of privacy and freedom of expression should apply irrespective of who claims to be exercising this freedom and that the criteria allow account to be taken of the important investigative and informative roles of the media in a democracy. In balancing these interests, the judiciary would apply the statutory criteria we propose and can be expected to afford a high value to the freedom of the press and other media in evaluating the respective claims to privacy and freedom of expression. *We provisionally recommend that there should be no special rules applying to the media. We welcome submissions on this. We reiterate the recommendation in our* Report on Non-Fatal Offences Against the Person *that there be a general offence of harassment, as follows:*

> *"Every person who harasses another by persistently following, watching or besetting him or her in any place, by use of the telephone or otherwise, shall be guilty of an offence.*
> *For the purposes of this section a person harasses another when his or her acts seriously interfere with another's peace or privacy."*[82]

We also welcome submissions on whether there should be a "group" offence of collective besetting.

---

79 *Ibid.*, para. 7.30. Calcutt also proposed a fall-back position in the event his recommendations for the creation of criminal offences and associated civil remedies were not accepted by the Government. Since he was also recommending the introduction of a statutory press complaints tribunal, he suggested, as a less preferred alternative, that the substance of the proposed offences should be incorporated into the statutory code of practice which the tribunal would administer: see para. 7.32.

80 Para. 2.11. See also para. 7.5.

81 See below chs. 9-12.

82 *Report on Non-Fatal Offences Against the Person* (LRC 45-1994), recommendation 10.

8.30 We think that there is room for a greater degree of self-regulation of the media within the parameters of the law we shall be proposing. We note that the broadcasting media are under a statutory duty to respect privacy in the making and transmission of programmes,[83] whereas, in contrast, no such duty applies to the print media. Moreover, in its *Broadcasting Guidelines for RTE Personnel*, RTE clearly states its understanding of this duty and details the criteria to be applied in deciding whether or not the use of surreptitious recording and filming devices is permissible. There is a general prohibition on the use of these devices and the exceptions permitting their use are narrowly drawn. In particular, the criteria that there must be compelling reasons for their use, that it must not be possible to obtain the information by other means and that the use of such devices must be indispensable to achieve the intended purpose seem to us to be not only desirable but also sufficient to meet Ireland's international obligations in this regard.[84] That the prohibition should be lifted in a particular case by a personal decision of the Director General of RTE is an additional safeguard. *We would therefore recommend that the Independent Radio and Television Commission should, in the exercise of its statutory powers,[85] give thought to including comparable guidelines in a code of practice for independent broadcasters. Likewise, with regard to the print media, we would suggest that the NUJ might consider formulating more detailed provisions on respect for privacy for insertion in its Code of Conduct for members. Individual newspapers and other publications might also consider issuing explicit editorial instructions to staff on this matter.*

Review Of Constitutional And Legal Protection

(i) The Constitution

8.31 Judges have identified a number of constitutional provisions as affording a degree of protection to aspects of privacy. In addition, it is now accepted that one provision affords protection of a more general kind. Article 40.3.1° states:

> "The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen."

It is now clear that these personal rights include a right of privacy and that telephone conversations fall within the protected realm of privacy, or at least that the provision protects against deliberate, conscious, covert and unjustified interference by servants of the State with one's telephone conversations. Logically there would seem to be no good reason why the protection should not extend to other types of covert surveillance, as by a telephoto lens, but in such cases the respective locations of the person subject to the surveillance and of the person conducting it may be relevant to whether or not the former enjoys a privacy interest in the circumstances. *Kane*[86] proceeded on the basis that an

---

83 See above paras. 8.9-8.12.
84 See above paras. 7.17-7.50.
85 See above para. 8.11.
86 [1988] I.R. 757.

individual may enjoy a right to privacy in a public place. The question whether or not this assumption is correct was expressly left open by the Supreme Court. Some pronouncements by the High Court in the context of overt surveillance suggest that not only location but also conduct i.e. whether one places oneself in the public view - may be significant. Thus, in *Nason*,[87] the Court seems to have regarded as relevant both the failure of the subject of the photographs to draw the curtains and the fact that the photographer took the photographs from the street.

8.32 Even if an intrusion is accepted by the court as impinging upon the privacy interest of a person, protection will only be afforded if no weightier countervailing interest exists. The latter may either be a community interest or an individual interest, and the list of such interests is not closed.[88] In balancing an interest in privacy against a countervailing interest, the courts have looked both at the nature of the latter and at the nature of the State and have applied a criterion of proportionality in assessing the impact on privacy of the invasion in question. In particular, they have stated that the right to life takes priority over the right to privacy,[89] that reference should be had to the sovereign, independent, democratic and Christian nature of the State,[90] and that the adverse consequences for the person whose privacy has been threatened or invaded of upholding a countervailing interest must not be excessive.[91]

8.33 The criteria used by the superior courts in weighing privacy and competing interests echo those applied by international human rights bodies in assessing the international obligations of states, including Ireland, with respect to the protection of privacy. There is some indication in the case law of the European Commission and European Court of Human Rights that they attach greater weight to some interests than to others. These bodies seem to afford a particularly heavy weight to freedom of expression and have described this freedom on several occasions as fundamental in a democracy.[92] In contrast to the present position under the Irish Constitution, the list of acceptable competing interests under the European Convention on Human Rights is limited. Article 8 gives an exhaustive list of the grounds on which privacy may legitimately be invaded, but this list is extensive and contains the somewhat open-ended objective of the protection of the rights and freedoms of others.[93] Article 8 also requires that the balance between competing interests be drawn by reference to democratic values, and these values have been interpreted by the Commission and the Court as those of a liberal, democratic state. Moreover, in order for a competing interest to be afforded priority over privacy, the invasion must be "necessary in a democratic society" for the attainment of the competing objective, and in determining the question of necessity, the Commission and the Court look

---

87 Unreported, 12 April 1991 (Keane J.).
88 See above paras. 3.10-3.11.
89 See above para. 3.11.
90 See above paras. 3.18-3.19.
91 See above para. 3.16.
92 See above n.5.
93 For comment on this objective see, e.g., A. Connelly, "The Protection of the Rights of Others", (1980) 5 *Human Rights Review* 117.

not only to the nature of the competing interest but also require that the impact on the complainant of upholding this interest would be "proportionate to the aim pursued".[94]

8.34 Where privacy is afforded protection by the Constitution, it extends beyond the surveillance itself to ancillary conduct. In *Kennedy and Arnold*,[95] the privacy of the plaintiffs was infringed not only by other persons listening to their telephone conversations but also by the recording of the conversations, their transcription and the making available of transcriptions to other persons. How far beyond this protection extends has yet to be decided, in particular, whether it extends to publication by the media, at least where the editor or publisher was aware of how the information was obtained.

8.35 It is clear that the fundamental rights provisions of the Constitution may be invoked against intrusive State action. The extent to which they also afford protection against intrusive conduct by non-State actors is less clear. While some guarantees may be directly enforced against private bodies and individuals,[96] others may only indirectly afford protection against intrusive private conduct. In this connection, the wording of the guarantee may be important. Article 40.3.1° expresses an undertaking by the State to protect the personal rights of the citizen. Moreover, it is "in its laws" and "by its laws" that the State is to implement this undertaking. The wording of the provision therefore suggests that it may not be directly invoked against a private body or individual. Nevertheless, it has been successfully invoked against private conduct on at least one occasion.[97] Furthermore, it may provide indirect protection against conduct on the part of private actors in that the State must respect, defend and vindicate the personal rights of the citizen in and by its laws; and this obligation may require legal protection against not only intrusive State conduct but also such conduct by non-State actors. In *Hanrahan v. Merck Sharp & Dohme*, Henchy J. said, *obiter*:

> "The implementation of those constitutional rights [*inter alia*, in Article 40.3.1°] is primarily a matter for the State and the courts are entitled to intervene only when there has been a failure to implement or, where the implementation relied on is plainly inadequate, to effectuate the constitutional guarantee in question... A person may of course, in the absence of a common law or statutory cause of action, sue directly for breach of a constitutional right...; but when he founds his action on an existing tort he is normally confined to the limitations of that tort. It might be different if it could be shown that the tort in question is basically ineffective to protect his constitutional right."[98]

8.36 Certainly, as regards privacy, compliance by Ireland with its international

---

94 See above para. 7.22.

95 [1987] I.R. 587, [1988] I.L.R.M. 472.

96 See, e.g., *Murtagh Properties Ltd. v. Cleary* [1972] I.R. 330, and *Meskell v. C.I.E.* [1973] I.R. 121.

97 See *Murtagh Properties Ltd. v. Cleary* [1972] I.R. 330.

98 [1988] I.L.R.M. at 636.

obligations requires it to afford a degree of protection against invasive private conduct as well as against such public action. The European Commission and European Court of Human Rights have stated that, at times, compliance by a state with its obligations under Article 8 requires it to take positive action to protect an individual's privacy, not merely to refrain from unjustifiable intrusion into it, and that such positive action may include legal protection against privacy-invasive conduct by private individuals.[99] Precisely what degree of legal protection for privacy against invasion by non-state actors is required by Ireland's obligations under the European Convention has yet to be determined. As regards Ireland's obligations under the International Covenant on Civil and Political Rights, the Human Rights Committee has explicitly stated that compliance by a state with its obligations under Article 17 of the Covenant requires it "to provide the legislative framework prohibiting [privacy-invasive] acts by natural or legal persons".[100]

8.37 Not only do Ireland's international obligations require that there exist in domestic law a measure of protection against privacy-invasive conduct whether by the State or by non-State actors, they further require that the law affording this protection be accessible to the persons concerned and formulated with sufficient precision to enable them to foresee, to a degree that is reasonable in the circumstances, what legal consequences may flow from their conduct. It must specify in detail the circumstances in which interference is permitted and, where State interference is concerned, it must designate the authority or authorities entitled to interfere. Where the law confers a discretion, the scope and permitted manner of exercise of this discretion must be clearly set out.[101]

8.38 Although the Constitution may afford general protection in cases of surveillance, of its nature, it cannot fulfil these international criteria. The fine print of legislation is needed to specify the circumstances in which and the conditions under which privacy may lawfully be infringed, as well as the persons who may legitimately intrude upon the privacy of another. Legislation, whether primary or secondary, will meet the criterion of accessibility in that it is published and, with careful phrasing, should meet the criteria of clarity and precision. Moreover, as regards intrusion by non-State actors, on at least one interpretation of Article 40.3.1°, legislation is required by the State's undertaking in and by its laws to respect, defend and vindicate the personal rights of the citizen. We are therefore of the view that *the first line of protection against surveillance by both private and public actors should be provided by the civil and the criminal law. The constitutional protection of privacy provides a backdrop for this law as well as an alternative avenue of redress for some grievances. It may also provide supplementary protection if gaps appear in the régime of civil and criminal protection.*

---

99 None of the surveillance cases decided by the Court has in fact yet concerned purely private behaviour, but the Court has accepted that, under Article 8, a person is entitled to the protection of the national legal system against the clandestine recording of his or her telephone conversations by private individuals: see above paras.

100 General comment of the Committee on Article 17, 23 March 1988: see above para. 7.49.

101 See above paras. 7.20-7.21 & 7.46-7.49.

8.39 We are reinforced in this view by other considerations pertaining to the legal system. A constitutional action may only be initiated in the High Court, and constitutional actions are expensive. Civil legal aid is not generally available in such cases, nor does the Attorney General's scheme of legal aid specifically cover actions for invasion of one's privacy. In our opinion, remedies and sanctions should be available in the Circuit and District Courts for invasions of one's privacy. While there may be an appeal from the decisions of these courts to the higher courts, and, in such event, expense may be unavoidable, it is desirable that remedies and sanctions be readily available in the first instance in cases of unjustifiable surveillance.[102]

(ii) The criminal law

8.40 It is at present mainly through the sanctions of the criminal law that surveillance is regulated. However, while a number of offences may be committed in the course of surveillance, most are not directed at such conduct, but merely happen to catch within their ambit instances of surveillance. One exception is the interception of communications, which has been specifically targeted for the application of penal sanctions.

8.41 It is an offence under s.84(1) of the *Postal and Telecommunications Services Act, 1983* to open or attempt to open a postal packet addressed to another person without the agreement of that person.[103] Unlike earlier offences under the *Post Office Act, 1908*, the offences under s.84(1) are not expressly limited to postal packets in the course of transmission by post or being transmitted by An Post.[104] In Chapter 12, we will consider whether this broad sweep of the law is desirable or whether the relevant criminal offences should be more narrowly framed. Also, since there is no clear legal definition of what constitutes a postal packet, we will examine the meaning of this expression and will suggest the adoption of a new term in order to secure in the criminal field the degree of precision which is desirable. Disclosure of the contents of a postal packet addressed to another person and use for any purpose of any information obtained from any such postal packet are also offences under the 1983 Act.[105] We accept the principle that it is appropriate to criminalise such conduct. Civil remedies alone would not be sufficient in such cases. The deterrent effect and moral sanctioning of the criminal law are necessary to signal society's disapproval of interference with correspondence in general. Our inquiry will therefore be limited to an assessment of whether the present law in this area is satisfactory or not. In this connection, we will also examine the statutory exemptions from criminal liability.[106]

---

102 In their *Consultation Paper on Infringement of Privacy*, published in July 1993, the Lord Chancellor's Department and the Scottish Office expressed the view that, for plaintiffs to be able to obtain adequate relief for infringement of their privacy, it is important that the procedures available should be accessible, quick and cheap: para. 6.1.

103 Or to authorise, suffer or permit another person to open or attempt to open a postal packet addressed to someone else: s.84(1)(a).

104 See above paras. 5.37 & 5.42.

105 Section 84(1)(b) and (c) respectively.

106 Section 84(2) of the *Postal and Telecommunications Services Act, 1983.*

8.42 As in the case of the post, in the telecommunications field it is an offence under s.98(1) of the 1983 Act to intercept or attempt to intercept telecommunications messages.[107] Unlike the comparable offences in relation to the post, however, these offences apply only to messages transmitted by Bord Telecom Éireann and only while a message is "being transmitted". In Chapter 12, we will consider whether it is desirable to extend the scope of these offences, particularly in view of the worldwide deregulation of telecommunications services. Since there is also a lack of clarity surrounding the definition of "telecommunications messages", we will likewise examine the meaning of this expression and suggest some legislative clarification. We will also examine the meaning of "intercept", particularly in view of the recent legislative exclusion of participant monitoring from the definition of this word.[108] Disclosure not only of the "substance" but also of the "purport" of an intercepted message are likewise offences under s.98(1), as is using for any purpose any information obtained from any such message. Again, we accept the principle that it is appropriate to criminalise such conduct, and will limit our inquiry to examining whether or not the present law is satisfactory. In the course of this examination, we will also consider the statutory exemptions from criminal liability.[109]

8.43 The offences under the 1983 Act concern the interception of postal packets and telecommunications messages, and the question should be asked whether there is any other form of communication the interception of which is not presently penalised but which should be penalised. Advances in technology have revolutionised communications, and one of these advances has been the marriage of computers and telecommunications to produce electronic mail. Electronic mail is increasingly used for a wide range of purposes, including personal communication. There is no specific offence of intercepting electronic mail. When such mail is carried by Bord Telecom Éireann, it constitutes a "telecommunications message" and is therefore protected by s.98(1) of the 1983 Act. There are also a number of offences pertaining to the unauthorised accessing and disclosure of computerised data, and since electronic mail comprises computerised data, the privacy of this mail is further protected by these offences. In Chapter 12, we will further consider whether adequate protection is afforded the privacy of electronic mail by the aggregate of these telecommunications and computer offences and will pay some attention to the use of encryption techniques as a means of protecting the privacy of such communications.

8.44 Aural surveillance, where there is no interception of a telecommunications message, is not specifically prohibited or regulated by law. Wireless telegraphy is however extensively regulated by law, and in that the devices used for aural surveillance constitute "apparatus for wireless telegraphy", there is a considerable body of law applicable to them. This body of law has

---

107 Or to authorise, suffer or permit another person to intercept telecommunications messages, or to do anything that will enable him or another person to intercept telecommunications messages: s.98(1)(b) & (c).

108 See s.13(3) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*, and above paras. 5.52-5.53.

109 Section 98(2) of the *Postal and Telecommunications Services Act, 1983*.

however developed in response to a need to regulate the use of the airwaves, not to regulate the use of aural devices, and again only incidentally affords protection against intrusive aural surveillance.

8.45 A person using an aural device may commit an offence if she or he does not possess a licence for the device or contravenes the terms and conditions of any licence.[110] Where a person is incidentally privy to a communication not intended for receipt by him or her while lawfully using apparatus for wireless telegraphy, licensing regulations make it an offence for that person to disclose the content of the communication or even on occasion the fact of the communication to another person except in limited circumstances. Also, it is an offence improperly to divulge the purport of any message or communication sent by wireless telegraphy.[111] Furthermore, an offence may be committed if a device is used in such a way as to interfere with licensed wireless telegraphy.[112] For the purpose of preventing and reducing the risk of interference with wireless telegraphy, the Minister for Transport, Energy and Communications has made an order requiring a licence for the sale, letting on hire, manufacture or importation of certain radio transceivers. It is an offence to sell, let on hire, manufacture or import these transceivers without the required licence.[113] In Chapter 11, we will consider whether the various wireless telegraphy offences are, in tandem with telecommunications offences, sufficient to control the abusive use of aural devices.

8.46 Similarly, visual surveillance is not specifically prohibited by law. This is perhaps the greatest gap in the protection presently afforded privacy by the criminal law in respect of invasive surveillance. Technological developments have clearly outstripped the law in this area. Nor is there any ready explanation for this legislative omission since, although some use of the technology is covert, much is readily visible, as demonstrated by the growing ubiquity of video cameras and closed circuit television in banks, stores, post offices and elsewhere. We do not favour the criminalisation of all abuses of such surveillance but, in our view, it is right that society should mark its disapproval of the worst invasions of privacy by the application of penal sanctions, and these we shall address in Chapter 10.

8.47 Also in Chapter 10 we shall consider whether there are circumstances in which even extensive invasion of an individual's privacy by means of visual surveillance may be justified, and shall suggest safeguards to ensure that, in cases where a legitimate reason exists for such surveillance, this reason does not afford a blanket justification for excessive or unnecessary surveillance.

---

110 See above paras. 5.30-5.32 concerning licensing.
111 See above para. 5.33.
112 See above para. 5.32 for this offence.
113 See above para. 5.34.

(iii) Civil remedies

8.48 A range of civil remedies are available to victims of surveillance. Thus one may get an injunction to stop photographers trespassing on one's land or may claim damages if any photograph taken was published in such a way as to be defamatory of the person. These remedies have however not been fashioned specifically to protect privacy. Any protection they afford is limited and incidental to the protection of other interests.

8.49 There appear to be few, if any, remedies specifically targeted at invasions of privacy. One such remedy in relation to the interception of communications may be an action for breach of a statutory duty arising from the legislative endorsement of the principle of the inviolability of the post,[114] but we are not aware of any such action ever having been taken. Some faith has been placed in the courts extending the law on breach of confidence to catch unauthorised disclosure of information obtained by the interception of communications, but such extension is uncertain and, as we have noted, confidentiality and privacy are in fact two distinct interests.[115] There is no specific cause of action protecting against unwanted surveillance, whether aural or visual.

8.50 In that a victim of unwanted surveillance has no specific civil remedy but must, to gain redress, seek among a range of general civil actions in the hope that the circumstances will come within the ambit of one of them, and in that it will often be uncertain whether the action covers the situation or not, there is a huge deficiency in the civil law. This deficiency could probably be rectified by the creation of a single action for breach of privacy. The law of several countries, including both civil law and common law jurisdictions, recognises a right of privacy, breach of which entails civil liability. In the next Chapter, we will address the question whether it is desirable that a statutory tort of invasion of privacy be created in Ireland. Since, in this Paper, we are particularly concerned with the threats posed to privacy by surveillance, we will also consider whether the creation of a more narrowly drawn tort designed to afford a remedy specifically for privacy-invasive surveillance would be a more appropriate way of filling the gap. In addition, we will look at whether there should be, as there is in a number of other countries, a specific tort of appropriation of the name, likeness or voice of another person.

---

114 See above p.68, n.64.
115 See above paras. 4.35-4.37.

CHAPTER 9: CIVIL REMEDIES

9.1 In this Chapter we will consider the creation of the following statutory torts as means of affording protection and a remedy to victims of invasive surveillance:

(i) invasion of privacy;
(ii) invasive surveillance; and
(iii) unauthorised use of one's image, name or voice.

A Tort Of Invasion Of Privacy?

9.2 **France**: The French courts have for very many years recognised a right of privacy, breach of which entails civil liability.[1] The courts accepted a right of privacy as one of a number of rights of personality and also imposed civil liability for breach of this right under a provision of the Civil Code, Article 1382, which deals generally with responsibility for delicts. This Article requires anyone who by her or his fault causes damage to another to make good the damage.[2] In 1970 a right of privacy, modelled on Article 8 of the European Convention on Human Rights, was specifically incorporated into the Civil Code. Paragraph 1 of Article 9 of the Code provides that everyone has the right to respect for her or his private life. Paragraph 2 then states that judges may, without prejudice to reparation for any damage suffered, prescribe any appropriate measure, including sequestration and seizure, to prevent or bring to an end an attack on the intimacy

---

1 See, e.g., P. Kayser, *La Protection de la vie privée*, 2nd ed., Economica, Presses universitaires d'Aix-Marseille, 1990, pp.75-81.

2 Article 1382 provides:

> "Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer."

of private life.[3] The saver in paragraph 2 with respect to reparation for damage suffered has the effect that the legal basis for reparation remains Article 1382 whereas other measures are authorised by Article 9 itself.

9.3 The wording of Article 9 has led to some uncertainty of interpretation since the right itself is phrased in terms of respect for private life, whereas the measures in respect of prevention and cesser authorised by paragraph 2 refer to 'the intimacy of private life', a somewhat narrower concept. This has led some judges and commentators to conclude that it is only this narrower field which is protected by Article 9 in general, but the better view would appear to be that it is the broader field of private life which is so protected,[4] and certainly the broader interpretation accords with Article 8 of the European Convention.

9.4 A distinction has been drawn in the case law between private life and public activities, though it is not always clear into which category a particular matter will fall. Linked as the concepts of private life and public activities are to the social custom of the day, the line between the two will not necessarily be drawn in the same place over time.[5] Persons have generally been regarded as giving tacit consent to the making of inquiries about their public activities and to publication thereof whereas express consent is needed if inquiries and publications relating to private life are to be accepted as lawful. Privacy is reduced in public places. The taking and publication of a person's photograph in a public place is lawful when the photograph is incidental to the overall context of the picture being taken, as when a person is photographed in a crowd or visiting a national monument.[6] However consent is generally required if a person is singled out from others.[7] Persons in the public eye are entitled to respect for their private lives as are ordinary citizens, but the scope of this respect will be somewhat less in their case since the public is regarded as having a legitimate interest in greater information about them than about the ordinary citizen.[8] Thus, a Paris court held that the publication of a photograph of a well-known person piloting a speedboat did not infringe her right to respect for her private life.[9]

9.5 **Germany**: In Germany, in addition to constitutional protection, an invasion of privacy is actionable in the civil courts as an aspect of the right of

---

3 Article 9 reads:

> "Chacun a droit au respect de sa vie privée.
>
> Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée; ces mesures peuvent, s'il y a urgence, être ordonnées en référé."

4 See, e.g., P. Kayser, *op. cit.*, pp.158-160.

5 See in general P. Kayser, *op. cit.*, p.161ff.

6 See, e.g., *X v. Commandant Y and Others*, Tribunal de grande instance, Lyon, Référés, 29 August 1980, D.1981, J:507.

7 See, e.g., Tribunal de grande instance, 2 June 1976, D.1977.364; and 11 February 1987, *Gaz. Pal.* 1987.1.138.

8 On the lesser entitlement of public figures see Kayser, *op. cit*, p.191f.

9 *S.A. the Begum Aga Khan v. Buttafava and Others*, Tribunal de grande instance, Paris, First Chamber, 26 June 1974, *Gaz. Pal.* 1974.2.901.

personality.[10] Section 823(1) of the German Civil Code provides:

> "A person is obliged to pay compensation for either negligently or intentionally violating the life, health, freedom, property or any other right of another where:
>
> (i) there has been an act that has violated an interest and caused damage;
> (ii) the violation of the right is unlawful and not justified;
> (iii) it was caused by intentional or negligent fault."

In 1957, the Supreme Court held that the general right to one's personality is an "other right" within the meaning of this subsection.[11] It is "to be recognised as a civil right to be respected by everyone in daily life, in so far as that right does not impinge upon the rights of others and is not repugnant to constitutional order or the moral law."[12] The meaning and scope of this right have been defined on a case-by-case basis. It has been described as a "source right" (*Quellrecht*) from which a number of discrete rights of personality derive, one of which is a right to one's own image or likeness, and another the right to one's spoken word.[13]

9.6 As in France, public figures are afforded some protection, but the courts will take into account the public profile of a plaintiff in assessing whether or not the person's right to personality has been infringed. Among the examples given by the Younger Committee of situations accepted by the courts as encompassed by the right of personality are the use of the plaintiff's "wedding photograph to advertise marriage advertisements in a newspaper; the secret recording of conversations; and the disclosure of the content of confidential letters without the author's consent."[14] According to this Committee, in 1972 the decided cases showed "that the right of personality is primarily a right of freedom from publicity (whether or not defamatory) by mass communication."[15]

9.7 Subsequent case law has broadened the scope of the right, and while the courts formerly required proof of monetary loss, they are now prepared to award damages for non-pecuniary loss.[16] Damages for non-pecuniary loss caused by unlawful surveillance may be awarded where (i) the infringement of the right is

---

10 See, e.g., B.S. Markesinis, *The German Law of Torts*, 3rd ed., pp.376-416.
11 24 BGHZ 72 (1957).
12 26 BGHZ 349 (1958).
13 See further below para. 9.61 on these rights.
14 *Report*, Appendix J, para. 17, p.311.
15 *Ibid.*, para. 23, p.312.
16 See, e.g., 26 BGHZ 349, *Neue Juristische Wochenschrift* 1958, 827; and 35 BGHZ 363, *Neue Juristische Wochenschrift* 1961, 2059.

serious, and (ii) there is no other means of satisfaction for the plaintiff.[17] Further remedies include an order for the seizure of the surveillance equipment used and an injunction.

9.8 A recent decision of the Cologne Court of Appeal illustrates the present scope of this action in the context of visual surveillance.[18] A man attached one video camera to a rotating antenna and another to a birdhouse in order permanently to watch a neighbouring estate where his mother-in-law lived. She won a legal order against him to stop the surveillance, but he continued. In a further action, the Court awarded her damages although she had suffered no material loss. She had, said the Court, been forced to live for over a year in "an optically cordoned-off prison", and because of this, the normal legal measures, such as seizure of the cameras, would not be sufficient by way of redress. An award of damages was the only way she could now get satisfaction for the infringement of her right of personality.

9.9 **U.S.A.**: A right of privacy distinct from the Constitution has also been recognised in the United States of America over the last century both by way of statute[19] and case law. As in France, the writings of jurists were influential in this development. In particular, the article by Warren and Brandeis in the *Harvard Law Review* of 1890 on "The Right to Privacy" has often been referred to with approval by the courts.[20] Four distinct types of conduct are generally identified as grounding an action in tort under the heading of privacy. Indeed leading commentators on the U.S. law of torts have said of breach of privacy:

> "... it is not one tort, but a complex of four. To date the law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff 'to be let alone.'"[21]

The four types of conduct are:

(i) appropriation of a person's name or likeness for commercial purposes;

---

17 E.g., the Hamburg Court of Appeal said in a 1987 case:

> "The Supreme Court has always held that where there has been an unlawful and culpable invasion of the right of personality, the victim can claim money damages for immaterial harm only when the gravity of the invasion makes such a *solatium* absolutely necessary. Whether such an invasion is sufficiently grave depends on all the facts of the case, including the seriousness and intrusiveness of the invasion, the dissemination of the publication, the duration of the harm to the victim's interests and reputation, the nature of and reasons for the defendant's conduct and the degree to which he was to blame."

Neue Juristische Wochenschrift 1988, 737: reproduced in B.S. Markesinis, *op. cit.*, p.407f.

18 Cologne Court of Appeal, *Neue Juristische Wochenschrift* 1989, 720.

19 See Neb. Rev. Stat. ss.20-201 to 211 & 25-804.04; N.Y. Sess. Laws 1903, ch. 132, ss.1-2, as amended 1921; Okla. Code Ann. 1953, 76-9-401 to 406; Va. Code 1950, ss.2.1-377 to 386; and Wis. Stat. Ann. 895.50.

20 See, e.g., *Pasevich v. New England Life Insurance Co.*, 1905, 122 Ga. 190, 50 S.E. 68.

21 *Prosser and Keeton on Torts*, 5th ed., p.851.

(ii) unreasonable and highly offensive intrusion upon the seclusion of another person;
(iii) public disclosure of private facts; and
(iv) putting someone in a false light.

9.10 Of particular interest in the context of this Paper are the first three types of conduct. The first, the appropriation of a person's name or likeness will be considered below. Intrusion upon the seclusion of another person has been interpreted by the courts to cover activities such as eavesdropping upon private conversations by wire-tapping and microphones, the conduct of "peeping Toms", and the use of telescopic lenses.[22]

9.11 For a claim in relation to the public disclosure of private facts to succeed four elements must be proven:

(i) the disclosure must be public, not private;
(ii) the facts disclosed to the public must be private facts, not public facts;
(iii) the matter made public must be one which would be highly offensive and objectionable to a reasonable person of ordinary sensibilities; and
(iv) the public must not have a legitimate interest in having the information made available.[23]

As regards the latter, great weight is often afforded by the courts to the competing value of freedom of expression, and public figures in particular are often regarded as legitimate subjects of public interest with the consequence that their entitlement to privacy is usually much less than that of the ordinary citizen.

9.12 **Canada:** In the last twenty to twenty-five years, a number of Canadian provinces have enacted a tort of breach of privacy. The Manitoba *Privacy Act* of *1970* provides:

> "A person who substantially, unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person."[24]

A violation may occur without proof of damage.[25] The tort is phrased in identical terms in the British Columbia and Saskatchewan Privacy Acts, both of 1979:

> "It is a tort, actionable without proof of damage, for a person, wilfully

---

22 See, e.g., *Rhodes v. Graham*, 1931, 238 Ky. 225, 37 S.W.2d 46; *Roach v. Harper*, 1958, 143 W.Va.869, 105 S.E.2d 564; *La Crone v. Ohio Bell Telephone Co.*, 1961, 114 Ohio App. 299, 182 N.E.2d 15; *Dietemann v. Time Inc.*, 1971, 449 F.2d 245.

23 *Second Restatement of Torts*, §.652D.

24 Section 2(1).

25 Section 2(2).

and without claim of right, to violate the privacy of another person."[26]

9.13 The various Acts do not contain a definition of privacy, but they do stipulate that certain actions are *prima facie* breaches of privacy; and among the illustrative lists given in the legislation are invariably instances of visual and aural surveillance.[27] The Acts also typically give some guidance to the courts as to the scope of the protection to be given privacy,[28] and specify a number of defences.[29]

9.14 It is clear then that in a number of both civil law and common law countries privacy-invasive conduct of the type we are considering in this Paper may constitute the tort of breach of privacy. The publication of information obtained by means of such surveillance may also constitute a tort, but often the public interest in freedom of expression will outweigh the individual's interest in privacy, especially where public figures are concerned.

9.15 The creation in Ireland of a statutory tort of invasion of privacy would therefore provide broad-ranging protection against invasive surveillance. A range of civil remedies are available for breach of privacy in all the jurisdictions mentioned and, as in the Canadian legislation,[30] the Irish statute could specify the available remedies. The creation of such a general tort would however also capture other conduct than that we are examining here, and we are of the opinion that it would only be appropriate to recommend such a course of action after considering many other issues than those addressed in the present Paper. Accordingly, and without prejudice to any view of the matter we may subsequently adopt, we make no recommendation in this regard for the moment. On the other hand, it is appropriate for us to consider whether the enactment of a more restricted tort relating specifically to surveillance is desirable.

A Tort Of Invasive Surveillance?

9.16 Included in the illustrative list of activities which constitute *prima facie* evidence of violation of privacy in the Canadian legislation is a number of forms of surveillance. The Saskatchewan Act is typical. It provides that proof of, *inter alia*, the following conduct, without the consent (express or implied) of the person concerned or of some other person who has the lawful authority to give consent, is *prima facie* evidence of a violation of the privacy of the former:

---

26 Section 2 of the British Columbia Privacy Act and s.1(1) of the Saskatchewan Privacy Act. See also s.3(1) of the Newfoundland *Privacy Act, 1981*. The Canadian provincial statutes mentioned here are reproduced at Appendix D below.

27 See s.1(4) of the British Columbia Privacy Act; s.3 of the Manitoba Privacy Act; s.4(a) & (b) of the Newfoundland Privacy Act; and ss.3(a) & (b) of the Saskatchewan Privacy Act.

28 See s.1(2) & (3) of the British Columbia Privacy Act; s.3(2) of the Newfoundland Privacy Act; s.6 of the Saskatchewan Privacy Act; and cf. s.4(2) of the Manitoba Privacy Act (considerations to be taken into account by the court in awarding damages). See further below para. 9.26.

29 See s.2 of the British Columbia Privacy Act; s.5 of the Manitoba Privacy Act; s.5 of the Newfoundland Privacy Act; and s.4 of the Saskatchewan Privacy Act. See further below paras. 9.17, 9.42 & 9.45.

30 See s.4(1) of the Manitoba Privacy Act; s.6(1) of the Newfoundland Privacy Act; and s.7 of the Saskatchewan Privacy Act.

"(a) auditory or visual surveillance of a person by any means including eavesdropping, watching, spying, besetting or following and whether or not accomplished by trespass;

(b) listening to or recording of a conversation in which a person participates, or listening to or recording of messages to or from that person passing by means of telecommunications, otherwise than as a lawful party thereto."[31]

9.17 There are several exceptions and defences to the action some of which are designed to protect the freedom of the press and other media.[32] Again, the exceptions in the Saskatchewan Act are representative:

"An act, conduct or publication is not a violation of privacy where:

(a) it is consented to, either expressly or impliedly by some person entitled to consent thereto;

(b) it was incidental to the exercise of a lawful right of defence of person or property;

(c) it was authorized or required by or under a law in force in the province or by a court or any process of a court;

(d) it was that of:

(i) a peace officer acting in the course and within the scope of his duty; or
(ii) a public officer engaged in an investigation in the course and within the scope of his duty;

and was neither disproportionate to the gravity of the matter subject to investigation nor committed in the course of trespass; or

(e) it was that of a person engaged in news gathering:

(i) for any newspaper or other paper containing public news; or
(ii) for a broadcaster licensed by the Canadian Radio-Television Commission to carry on a broadcasting transmitting undertaking;

and such act, conduct or publication was reasonable in the

---

31 Section 3(a) & (b).

32 It should be noted that these defences are available in all cases of alleged violation of privacy, not merely in cases of privacy-invasive surveillance.

circumstances and was necessary for or incidental to ordinary news gathering activities."[33]

Moreover, there is further protection for freedom of expression in that:

> "A publication of any matter is not a violation of privacy where:
>
> (a) there were reasonable grounds for belief that the matter published was of public interest or was fair comment on a matter of public interest; or
>
> (b) the publication was, in accordance with the rules of law relating to defamation, privileged."[34]

This provision does not however "extend to any other act or conduct whereby the matter published was obtained if such other act or conduct was itself a violation of privacy."[35]

9.18 An option in terms of remedying the deficiency in civil remedies in Ireland would be to create a statutory tort of invasion of privacy by means of surveillance and to provide a number of defences or exceptions as has been done in some Canadian provinces. The disclosure or publication of information obtained by such means might also be rendered tortious.

9.19 We are attracted by this option. It would catch within its scope all instances of abusive surveillance irrespective of type. It would also target the specific problem so that a plaintiff would not have to seek among a range of civil actions fashioned to protect interests other than privacy in the hope of finding one or more which would fit the circumstances of her or his particular case. In tandem with the criminal sanctions and safeguards which we recommend in the following chapters, it would constitute a comprehensive legal régime for the protection of privacy in cases of invasive surveillance.

9.20 On the other hand, it may seem inappropriate to create civil liability in respect of only one means whereby privacy may be infringed. The creation of such torts might also be seen as running contrary to a branch of the law which has traditionally been concerned with failure to comply with a duty rather than the enforcement of a right.[36]

9.21 We do not however find these countervailing considerations convincing and, on balance, favour the creation of a tort, or rather torts, of invasion of privacy by or as a result of surveillance. The sophistication of aural and visual

---

33 Section 4(1). See also s.2(1) of the British Columbia Act; s.5 (a)-(e) of the Manitoba Privacy Act; and s.5(1) of the Newfoundland Privacy Act.

34 Section 4(2). See also s.2(2) of the British Columbia Act; s.5(f) of the Manitoba Privacy Act; and s.5(2) of the Newfoundland Privacy Act.

35 *Ibid.*

36 See, e.g., B.M.E. McMahon and W. Binchy, *Irish Law of Torts*, 2nd ed., p.684.

devices, as well as the ease of acquisition and use by reason of recent technological and economic developments, pose a real threat to privacy. The creation of a tort to counter this threat would be timely and could indeed be regarded as overdue. While this may be described as a piecemeal approach to the protection of privacy, if successful, it might in due course be extended to other privacy-invasive conduct. *We accordingly recommend the creation of a statutory tort which will afford a range of civil remedies to a person whose privacy has been infringed by surveillance. We also recommend the creation of a statutory tort of disclosure or publication of information or material obtained by means of privacy-invasive surveillance.* We consider below how these torts might be phrased, the defences thereto, and ancillary matters such as the particular remedies which would be available and who should be entitled to sue.

9.22 *In the event that our recommendations in this regard are not accepted, an alternative would be to create civil liability in respect of the conduct to which we recommend below that criminal liability should attach, and we so recommend*, but as a much less preferred option. We recommend criminal sanctions only in the more serious cases of invasion of privacy, and adoption of our alternative recommendation with respect to civil liability would leave gaps in the protection under the civil law for victims of surveillance.

The New Torts

(i) Formulation of the torts

9.23 *First*, it is necessary to decide whether there should be specific reference to privacy in the formulation of the tort of invasive surveillance since this is the interest to be protected or whether the conduct to be rendered unlawful should simply be surveillance itself, with the consequence that other interests would be protected along with privacy. For example, in the latter eventuality, business interests would be protected from industrial espionage as well as personal communications from unauthorised eavesdropping.

9.24 We are of the view that, in the context of the present study, the tort should relate only to the protection of privacy. The protection of interests other than privacy from unwanted surveillance raises issues beyond those considered in this Paper. For example, the recording of what is said at a business meeting may raise issues regarding the extent to which the law should protect a business against competitors and the proper balance to be drawn between the public interest in a free market and the business interests of a particular company. These are not matters pertaining to privacy. Moreover, privacy is a universally recognised human right. Not only has Ireland entered into specific international obligations to respect it as such, but, being linked as a human right to the promotion of human dignity, privacy is intrinsically distinct from such other interests. *The tort should therefore be phrased in such a way as to make it clear that the interest being protected is that of privacy.*

9.25 *Secondly*, it is necessary to decide whether, in the wording of the tort,

some indication should be given of what is being protected, that is, the scope and content of privacy, or whether the concept of privacy should be left to be interpreted by the courts on a case by case basis. As we have mentioned, the difficulty of defining the concept of privacy is notorious,[37] and it would probably not be advisable to attempt to define privacy in the legislation or even to give a broad description. The courts of many countries have been asked in interpreting a right of privacy, to decide whether or not particular interests pertain to privacy and have not found the task to lie outside the judicial function. The scope of the concept in general has been defined somewhat differently in different jurisdictions, and in general we think it should be left to the Irish courts, at least in the first instance, to identify the matters properly to be regarded as matters of privacy. We have considered whether a general definition in line with the language used in some of the international treaties to which Ireland is party might be helpful to the courts but have concluded that it would not. For example, Article 8 of the European Convention on Human Rights refers to respect for "private life, family life, home and correspondence"[38]; but, in our view, not all observation of a person's home constitutes an invasion of a person's privacy. We therefore prefer to leave the question of definition entirely to the courts for the time being.

9.26 A separate question is whether the legislation should also afford some guidance to the courts in terms of the considerations which should be taken into account in deciding whether or not there has been an invasion of privacy. The Canadian Acts give some guidance to the judiciary by providing that:

> "The nature and degree of privacy to which an individual is entitled in any situation or in relation to any matter is that which is reasonable in the circumstances, due regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of an individual, regard shall be given to the nature, incidence, and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties."[39]

9.27 Again, in general, we do not think it desirable that the legislation we propose contain such a list of relevant considerations. The courts are well used to taking all the circumstances of the case into account, and the lawful interests of others, as well as the consequences for the plaintiff of the impugned conduct or publication, will be adequately catered for by the balancing of interests and the test of proportionality which we recommend below.

9.28 *Thirdly*, it is necessary to decide whether or not the particular conduct being targeted as unlawful surveillance should be defined in the legislation. We do not think it desirable that a comprehensive definition be given. Rather it

---

37 See above para. 1.1.

38 Article 8(1) of the European Convention on Human Rights. Cf. the wording of Art.17(1) of the International Covenant on Civil and Political Rights.

39 Section 3(2) of the Newfoundland Privacy Act. See also s.1(2) & (3) of the British Columbia Privacy Act, and s.6 of the Saskatchewan Privacy Act; and cf. s.4(2) of the Manitoba Privacy Act.

should be stated in the legislation that surveillance includes certain conduct, without this conduct being regarded as exhaustive of the forms surveillance may take. This would add specificity to the tort without introducing rigidity. The named conduct would clearly be covered by it, but the courts would be free to take account of developments in surveillance technology[40] and to apply the tort to any unusual form of surveillance.

9.29 Accordingly, *we recommend that the word "surveillance" should be defined to include aural and visual surveillance, irrespective of the means employed, and the interception of communications*. This would mean that the tort would catch a person listening at a door or looking through a keyhole as well as someone using a listening device or video camera. The listening and looking inherent in everyday living, as well as the ordinary use of devices such as binoculars and video cameras, would not be covered since another element of the tort discussed below would not be present.[41]

9.30 A particular problem is whether *recording a conversation to which one is party* should come within the meaning of the term "surveillance" or should be explicitly excluded therefrom.[42] There are legitimate reasons for recording such conversations, e.g. to ensure the accuracy of information conveyed or as evidence of the details of an agreement. Moreover, where the fact of the recording is known to the other person, that person has the option not to enter into the conversation or to tailor what she or he says so that nothing is recorded which the person wished to keep secret. Where a recording is made without the knowledge of the other person, although this may be reprehensible, the person whose voice is recorded intended to engage in conversation either with the person making the recording or in the presence of that person. The former was therefore aware that the latter would hear what was said. On the other hand, engaging in a conversation is different from consenting to being recorded. Consent to being recorded implies acceptance that not only one's words but also the way in which they were spoken are on permanent record in the hands of another person. *We welcome submissions on this issue.*

9.31 *Fourthly*, it is necessary to decide whether only surveillance should be a tort or whether disclosure or publication of information obtained by means of surveillance should also be tortious. In our opinion, disclosure or publication of such information often constitutes a greater invasion of the privacy of an individual than the act of surveillance itself in that the individual's control of the information has been lost not only to another person but to a number, and in some cases an unlimited number, of other persons. Moreover disclosure or publication of the purport of the information may be as damaging as disclosure or publication of the substance of the information. Also, in cases such as the taking of photographs, it is important that protection extend to material reproduction. *Disclosure or publication of the substance or purport of information*

---

40 See above paras. 2.1-2.9.

41 Viz., the intention to invade the privacy of another person: see below para. 9.34.

42 See further below paras. 11.37-11.44 concerning participant monitoring.

or material obtained by means of surveillance should therefore *also be torts.*

9.32 *Fifthly*, it is necessary to decide whether it should be sufficient to show invasion of privacy to succeed in an action or whether proof of damage as a result of the invasion should be required. We have noted that the Canadian statutes explicitly exclude the need to prove damage, and that the German courts will award damages for non-pecuniary loss where the invasion is serious and there is no other appropriate means of satisfaction for the plaintiff.[43] While damage may result from surveillance, this is not the essence of the wrong for which it is sought to compensate the victim. Rather it is the affront to human dignity, and it is desirable that the phrasing of the tort should expressly recognise this fact. *We* therefore *recommend that the tort be phrased in such a way as to make it clear that it is not necessary that the plaintiff show that he or she suffered any damage.*[44]

9.33 *Sixthly*, it is necessary in defining the tort of invasion of privacy by means of surveillance to exclude accidental invasions of another's privacy as well as the overhearing and seeing which are incidental to everyday living. Nor do we favour the extension of liability to negligent as opposed to deliberate invasions of privacy.[45] We think that some such requirement as that the invasion be wilful or intentional would achieve this objective. *We* therefore *recommend that it should be a requirement of the tort of invasion of another's privacy by means of surveillance that the invasion be intentional. With respect to disclosure or publication of information or material obtained by means of surveillance, we recommend that the disclosure or publication should also be intentional, but we think it right that, in such cases, liability should extend beyond intentional invasions of privacy to negligent conduct.* To require in all cases, for a plaintiff to succeed, that the plaintiff show that the defendant was aware that the information or material had been obtained by the intentional invasion by means of surveillance of the plaintiff's privacy would, in our view, tip the balance too far in favour of freedom of information at the expense of respect for privacy. Instead, *we recommend that strict liability should attach to the element of the invasion of privacy, but should be subject to the special defences which we propose below in respect of disclosure or publication.*[46] This would in effect mean that where the defendant knew that the information or material had been unlawfully obtained or had been reckless or negligent as to the manner in which it had been obtained, that person may be liable. However, where the defendant has taken reasonable care before disclosure or publication to discover how the information or material was obtained and to ensure that it was not unlawfully obtained by means of surveillance, that person will not be liable. Responsible journalists, broadcasters and publishers should have nothing to fear from such a standard of

---

43 See above paras. 9.7 & 9.12.

44 Cf. Lord Chancellor's Department and the Scottish Office, *op. cit.*, paras. 5.3-5.14, where, in the context of proposing the creation of a general statutory tort of infringement of privacy, it is suggested that the plaintiff should have to show that a person of ordinary sensibilities in the plaintiff's position would have suffered substantial distress as a result of the infringement of privacy, and that the plaintiff has suffered such distress.

45 Cf. *Ibid.*, para. 5.35.

46 See below para. 9.49. This is the approach adopted in the Canadian legislation.

liability.

9.34 In summary, *we recommend that it should be a tort, actionable without proof of damage, intentionally to invade the privacy of another person by means of surveillance. Surveillance should be defined to include aural and visual surveillance, irrespective of the means employed, and the interception of communications. It should also be a tort, actionable without proof of damage, intentionally to disclose or to publish information obtained by means of privacy-invasive surveillance.*

(ii) Defences

(a) Consent

9.35 An interest in privacy may be waived. Persons may willingly reveal the most intimate personal details to another or allow another to photograph them in their own home. In such cases they may be regarded as having waived any interest in privacy, at least as far as the recipient of the personal details is concerned in the former case and as far as the taking of the photographs is concerned in the latter. This waiver may however be partial in that although the persons with the privacy interest may have voluntarily ceded control of personal information to another, they may not have intended to cede control altogether, particularly in respect of release of the information to the world at large, as by publication in the media. Consent to publication may be implied in the circumstances of the initial communication or acquisition of the information, but where consent is neither express nor implied, we think it desirable that some protection be afforded by the law. It is also possible that a person who is secretly photographed or whose words are covertly recorded while the person is at home, on learning of the intrusion into her or his privacy, may, for whatever reason, have no objection to the subsequent publication of the photograph or recorded words. In such cases, it is right that the individual should have a civil remedy in respect of the taking of the photograph and the recording of words should the individual wish to avail of it, but that no remedy should be available in the event of subsequent publication in the event the individual is not opposed thereto. *We* therefore *recommend that consent, express or implied, should be a defence to the proposed actions in tort.* In many cases the required consent will be that of the person with the interest in privacy, but in some cases the person may not be capable of consent, e.g. a minor or a person who is mentally handicapped, or the person may have yielded a competence to consent on his or her behalf to another, e.g. by contract. In these cases *the consent of another person legally entitled to give consent on behalf of the plaintiff should be sufficient.*

(b) The exercise of legal duties, powers and rights

9.36 There are clearly circumstances in which it should be lawful not only to conduct surveillance, e.g. as a security measure in a bank or shop, but also to conduct it in a way which is invasive of the privacy of another person, e.g. state interception of communications in the interests of national security. The law

recognises such situations, and it should be a defence to the actions we propose that a person was acting in the exercise of a legal duty, power or right. For example, parents have a duty to care for and 'to keep an eye on' their children; the police have a duty to maintain public order and to prevent and investigate crime; employees of An Post may intercept an individual's post by virtue of a direction by the Minister for Transport, Energy and Communications under s.110 of the *Postal and Telecommunications Services Act, 1983*; individuals have a right to protect their property and their persons. A legal basis exists for resort to surveillance in such cases.

9.37 Duties, powers and rights may however be abused. The security camera in the shop may in fact be used for purposes other than or in addition to protecting the premises; in investigating a robbery, the police may plant listening devices not only in a suspect's home but also in that of a friend of the subject, or in listening to conversations in the subject's home may record and store the most intimate personal details of the suspect's life out of curiosity rather than relevance to the investigation. It should therefore not be sufficient by way of defence to show merely that the person was acting in the exercise of a legal duty, power or right. Safeguards are needed against the privacy-invasive abuse of duties, powers and rights. If licensing were to be introduced for the installation and use of aural and visual devices, then privacy might be protected in the granting of licences and in the terms and conditions attached to any licence.[47] But, in the absence of a system of licensing, more general safeguards are desirable.

9.38 A balance needs to be drawn between the interest protected by the duty, power or right on the one hand and the interest of the individual whose privacy is invaded on the other. Indications of the proper balance to be drawn are to be found both in the constitutional case-law on privacy[48] and in the international texts and cases pertaining to privacy.[49] Both sources have employed a criterion of proportionality: in other words, the impact of the surveillance on the person whose privacy has been invaded should not be disproportionate to the attainment of the objective pursued, be it the protection of property, national security, or whatever. Both sources also suggest that, in weighing and balancing the competing interests, regard should be had to the nature of the society which is envisaged by the relevant texts, that is, the Constitution and the international treaties to which Ireland is party. This society is a democracy which subscribes to the rule of law, the independence of the judiciary, a free press and individual liberty and whose institutions reflect these values.

9.39 In summary, *it should be a defence to the proposed torts to show that the defendant acted in the exercise of a legal duty, power or right and that the surveillance, disclosure or publication was not disproportionate having regard to the*

---

47 See below paras. 10.28-10.36 for an example of the control of optical surveillance by means of a system of licensing.

48 See above para. 3.24.

49 See above paras. 7.22, 7.29 & 7.48.

values of a sovereign, independent, democratic state.[50]

(c) The media

9.40 Given the high value attached to freedom of expression in democracies such as Ireland,[51] it is necessary to consider whether any additional defence/s should be available to members of the media.

9.41 The Saskatchewan Privacy Act provides that an act, conduct or publication is not a violation of privacy where:

> "it was that of a person engaged in news gathering;
>
> (i) for any newspaper or other paper containing public news; or
> (ii) for a broadcaster licensed by the Canadian Radio-Television Commission to carry on a broadcasting transmitting undertaking;
>
> and such act, conduct or publication was reasonable in the circumstances and was necessary for or incidental to ordinary news gathering activities."[52]

The other Canadian statutes do not provide such a defence and this is the only statutory provision of which we are aware to address specifically the matter of news gathering. We do not believe that the tests of reasonableness in the circumstances and being incidental to news gathering activities draw the proper balance between the privacy of the individual and the public interest in news. Nor would they satisfy the international criteria to which Ireland subscribes.[53] The criterion of necessity would accord with Ireland's international obligations, but would not add anything to the criteria we have proposed above for the balancing of competing interests. Moreover, we take the view that journalists and broadcasters should not have any special privileges in the gathering of information. They should be subject to the same rules as everyone else with respect to aural and visual surveillance and the interception of communications. The general criteria we propose should afford responsible journalists a sufficient defence, while protecting the privacy of the individual from the irresponsible.

9.42 In this connection, we recall that the *Broadcasting Guidelines for RTE Personnel* contain directions on the use of surreptitious recording and filming devices.[54] These directions would seem to accord with the defences we propose. In particular, they specify that "compelling reasons" must exist for encroaching on another's privacy, the broadcast must serve "a really important

---

50 Article 5 of the Constitution provides: "Ireland is a sovereign, independent, democratic state."
51 See above para. 8.4.
52 Section 4(1)(c).
53 See above paras. 7.22, 7.29 & 7.48.
54 See above para. 8.11.

public purpose which could not be achieved by other means", any encroachment on privacy must not be "unreasonable", and such recording or filming must be "indispensable to the achievement" of the public purpose. Moreover, such recording and filming must be personally authorised by the Director General.

9.43 A separate question is whether the media should have any special immunity in respect of the publication of information obtained by means of surveillance, especially where the information has been unlawfully obtained. In this regard, it should be remembered that, under our proposals, consent will provide a defence, even where the information has been unlawfully obtained.

9.44 All the Canadian statutes contain a special defence in relation to publication. The Saskatchewan Act is representative. Section 4(2) of this Act provides:

> "A publication of any matter is not a violation of privacy where:
>
> (a) there were reasonable grounds for belief that the matter published was of public interest and was fair comment on a matter of public interest; or
>
> (b) the publication was, in accordance with the rules of law relating to defamation, privileged;
>
> but this subsection does not extend to any other act or conduct whereby the matter published was obtained if such other act or conduct was itself a violation of privacy."[55]

9.45 Such a defence would obviously provide the media with extensive protection as regards the publication of any matter pertaining to a person's privacy. It would suffice that the matter was published in the belief that it was of public interest or was fair comment on a matter of public interest provided reasonable grounds existed for the belief. It would also suffice that the publication would be privileged, should the action have been one for defamation. This defence clearly tips the scales in favour of freedom of expression.

9.46 It seems to us that the wording of this defence has been substantially influenced by the law relating to defamation and seeks to align the defences available in an action for breach of privacy which those which are available in an action for defamation. As we have noted, there is indeed an overlap between privacy and the interests protected by an action for defamation.[56] The interests are nevertheless distinct.[57] We believe that the law should reflect this difference, and that any reference to defamation in a law designed to protect

---

55 See also s.2(2) of the British Columbia Act; s.5(f) of the Manitoba Privacy Act; and s.5(2) of the Newfoundland Privacy Act.

56 See above para. 4.19 and n. 37 (Chapter 4).

57 See above para. 4.19 and n. 38 & 39 (Chapter 4).

privacy may blur the distinction. We are also of the opinion that a belief, even on reasonable grounds, that a matter is of public interest would afford too broad a justification for an invasion of privacy. As has been pointed out on many occasions, publication of a matter which is of public interest does not mean that publication is in the public interest, that is, publication may not serve any particular common good. Indeed it may simply pander to prurient interest or curiosity.[58] We are further of the opinion that where it is in the public interest that a certain matter be published, the defences which we recommend should afford adequate protection. Consent may be sought to publication. In the event that consent is unobtainable or is refused, the publisher may plead exercise of the right of freedom of expression, and the criteria of proportionality and reference to democratic values would apply. We think it appropriate that, in the context of surveillance, the courts should be allowed, at least initially, to draw the proper balance between the interest of an individual in privacy and the public interest in freedom of expression by applying these criteria.[59]

9.47 Our proposals in this regard are without prejudice to any defence of absolute privilege which may otherwise be available under the law or the Constitution in respect of publications generally.[60]

9.48 Although we are opposed, in the particular context of surveillance, to any special defences in respect of publication which echo the law on defamation, we appreciate that in some situations where information which has been unlawfully obtained by means of surveillance is published, the publisher may not be aware of the way in which the information was acquired, and it would be unjust to make such a publisher strictly liable in all circumstances for the resultant invasion of privacy. *We* therefore *recommend that it should be a defence to the tort of disclosure or publication that the defendant did not believe and had no reasonable grounds to believe that the information had been obtained by means of privacy-invasive surveillance.*

(d) Constitutional rights

9.49 *The defences which we propose* will have a statutory basis and *are without prejudice to any defence which may be available under the Constitution, in particular, any constitutional rights which the defendant may enjoy.*

(iii) Remedies

9.50 We consider that the full range of civil remedies should be available to a person in respect of privacy-invasive surveillance and the publication of material obtained by means of such surveillance. For example, a person should be able to seek a court order to stop the surveillance or to prevent publication,

---

58 See above para. 8.8.

59 Cf. Lord Chancellor's Department and the Scottish Office, *op. cit.*, paras. 5.56-5.67.

60 See, e.g., Art. 15.12 of the Constitution and our *Consultation Paper on the Civil Law of Defamation*, 1991, paras. 94-106.

and to obtain damages or an account of profits where the invasion has occurred. The person should also be able to obtain the delivery up of any prints of unlawful surveillance, such as film, including both negatives and any prints, or a tape recording. *We* therefore *recommend that the legislation should provide for a full range of civil remedies.*

9.51 With reference to the granting of a court order to stop surveillance or to prevent publication, it will be necessary specifically to confer on the lower courts this power since in general only the High and the Supreme Courts have the competence to give injunctive relief. We have taken as our model in this regard the provisions of the *Family Home (Protection of Spouses and Children) Act, 1981* dealing with barring orders.

(iv) Level of court

9.52 We have already indicated that we believe *a civil remedy should be available in the Circuit and District Courts in respect of privacy-invasive surveillance.*[61] An action should usually be initiated in the District Court, but may need to be initiated at the higher level where the amount of damages sought exceeds the jurisdiction of the lower court. We would emphasise that the actions we propose have a statutory basis and are without prejudice to any constitutional action which may be brought or to any constitutional defence which may be raised.

9.53 Where the defendant pleads a constitutional right by way of defence and an issue arises as to the proper balance to be drawn between the privacy interest of the plaintiff and the right of the defendant, the issue will have to be determined by the High Court or, on appeal, by the Supreme Court. Cases in which this is most likely to occur are those where the defendant pleads a constitutional right to freedom of expression,[62] the defendant in such cases probably often being a member of the media. Given the present court system and, in particular, the exclusive competence of the High and Supreme Court in matters of interpretation of the Constitution, it is unavoidable that a certain

---

61 See above para. 8.39.

62 Article 40.6.1° of the Constitution provides:

> "The State guarantees liberty for the exercise of the following rights, subject to public order and morality:-
>
> i. The right of the citizens to express freely their convictions and opinions.
>
> The education of public opinion being, however, a matter of such grave import to the common good, the State shall endeavour to ensure that organs of public opinion, such as the radio, the press, the cinema, while preserving their rightful liberty of expression, including criticism of Government policy, shall not be used to undermine public order or morality or the authority of the State.
>
> The publication or utterance of blasphemous, seditious, or indecent matter is an offence which shall be punishable in accordance with law."

The other rights listed in this subsection are the right to freedom of assembly and the right to freedom of association.

number of cases will be heard and determined by these Courts. By our proposals, we seek to ensure that, in so far as is possible within the existing court system and the competence of the respective courts, a civil remedy is readily available to a person whose privacy is threatened, or whose privacy has been infringed, by or as a result of surveillance.

(v) Right of action

9.54 The actions which we recommend are designed to protect human dignity. It is therefore appropriate that *the actions should be limited to natural persons and* that *the person to whom any right of action should accrue is the person whose privacy is threatened or has allegedly been infringed.* We are aware that some persons such as minors or the mentally incapacitated may not be capable of taking an action on their own behalf and think that *the legislation should make it clear that the right of action also extends to any person who is legally entitled to act on behalf of the person whose privacy has or is about to be infringed.*

9.55 *For the purpose of obtaining a privacy order but not for the purpose of obtaining damages, a right of action should survive the death of the person whose privacy is alleged to have been infringed.*

(vi) Limitation period

9.56 There are limits to the period of time during which an action in tort may be taken. In general an action founded on tort may not be brought after the expiration of six years from the date on which the cause of action accrued.[63]

9.57 As to the length of this period, it is questionable whether six years may not in fact be too long in relation to an alleged invasion of privacy. Shorter periods apply in Ireland to certain types of action, e.g. an action claiming damages for negligence, nuisance or breach of duty where the damages consist of or include damages in respect of personal injuries.[64] The Saskatchewan *Privacy Act* of *1979* provides that an action for violation of privacy "shall be commenced within two years from the discovery of the alleged violation of privacy by the person who claims his privacy has been violated."[65] The Newfoundland *Privacy Act* of *1981* also provides a general limitation period of two years from the time when the violation of privacy first became known, but adds a cut-off limit of seven years from the date on which the violation of privacy occurred.[66] The Lord Chancellor's Department and the Scottish Office have proposed a period of only one year in England and Wales and of three years in Scotland in the context of the creation of a statutory tort of infringement of

---

63 See s.11(2(a) of the Statute of Limitations, 1957. On limitation periods in tort generally see, e.g., W.Binchy and B.M.E. McMahon, *Irish Law of Torts*, 2nd ed., ch. 46; and J. Brady and T. Kerr, *The Limitation of Actions in the Republic of Ireland*, Incorporated Law Society, 1984, ch. 3.

64 See s.11(2)(b) of the *Statute of Limitations, 1957.*

65 Section 9.

66 Section 10.

privacy.[67] It can be argued that the torts which we are recommending are designed essentially to protect human dignity and that a person whose sense of dignity has been affronted or whose feelings have been injured by an invasion of their privacy can be expected to take action promptly to secure redress for affront or injury to their feelings. On the other hand, the full effects of some of the conduct with which we are dealing will not be immediate even if the plaintiff is aware of the surveillance or the disclosure or publication at the time they occur. For example, the full implications for the plaintiff of the disclosure of personal information obtained by means of unlawful surveillance may not become apparent until some time after the disclosure, and the plaintiff may only be prompted to take action when she or he becomes aware of these implications. Consequently we think that a period of one year or even two years is too short. However, a period of six years does seem to us to be somewhat over long in relation to the type of actions we are proposing. *We* therefore *recommend a limitation period of three years for the new torts.*

9.58 As to the date on which the cause of action accrues, in relation to the new torts which we are proposing, where a person is aware of the surveillance, disclosure or publication, the date would be that of the surveillance, disclosure or publication, as the case may be. Disclosure or publication may of course occur some time, even years, after the invasive surveillance itself. However, where the surveillance is covert and unknown to the subject of the surveillance at the time, it would be unjust if time were to run from the act of surveillance itself, and the law is less clear as to the date on which a cause of action accrues in cases where the plaintiff is unaware at the time of the commission of the alleged tortious act. When considering the issue of limitation of actions in respect of latent personal injuries, we recommended that time should run from the date the plaintiff became aware, or ought reasonably to have become aware, that she or he had sustained a personal injury.[68] In line with this earlier recommendation, *we recommend that the date on which the cause of action accrues in relation to the torts we are proposing here should be that on which the plaintiff became aware or ought reasonably to have become aware of the surveillance, disclosure or publication, as the case may be. There should be no absolute cut-off limit for the taking of an action.*

(vii) Right of action and other remedies

9.59 Since the same act may ground an action in respect of the new torts we are proposing and in respect of an existing tort, we should consider the relationship between such actions and their attendant remedies. For example, surveillance which is invasive of another's privacy may also constitute a trespass to land or a private nuisance; disclosure of information obtained by means of surveillance may also constitute a breach of confidence. We think it right that *in such cases the plaintiff should be entitled to take either or both actions, but* that,

---

67 *Consultation Paper on Infringement of Privacy*, paras. 6.29-6.35.

68 See our *Report on the Statute of Limitations; Claims in Respect of Latent Personal Injuries*, LRC 21-1987, pp.42-43.

in the event that more than one action is successful, the court in the later action should be entitled to take account of any remedy afforded in the other action. The same should apply where the plaintiffs in the separate actions are different persons as, e.g., where an owner of land takes an action in trespass in respect of surveillance on her premises and a house-guest takes an action for invasion of privacy by means of the surveillance.

(viii) Legal aid

9.60 Privacy is a human right, and it is important that no person be unable, through lack of financial means, to gain protection from the courts against a threatened invasion of privacy or redress in the event of an actual violation. *We* therefore *recommend that*, for the avoidance of any doubt, *the Scheme of Civil Legal Aid and Advice should expressly be extended to these actions.*

(ix) Conclusion

9.61 *We recommend that a statute be enacted along the following lines*:

An Act To Protect The Privacy Of The Individual From Intrusive Surveillance

Definitions

1. In this Act -

"the Court" means the Circuit Court or the District Court;

"privacy order" has the meaning assigned to it by ***section*** *5 of this Act;*

"surveillance" includes aural and visual surveillance, irrespective of the means employed, and the interception of communications.

Causes of action

2. It is a tort, actionable without proof of damage, for a person intentionally -

(i) to invade the privacy of another person by means of surveillance; or

(ii) to disclose or publish the purport or substance of information or material obtained by means of privacy-invasive surveillance.

Defences

3. (1) It is a defence to an action under ***subsections*** *(i) and* ***(ii)*** *of section 2 of this Act to show that -*

(i) *the plaintiff, or some other person legally entitled to give consent on behalf of the plaintiff, consented, either expressly or impliedly, to the invasion, disclosure or publication, as the case may be; or*

(ii) *the defendant was fulfilling a legal duty or exercising a legal power or right* ***and*** *the impact of the surveillance, disclosure or publication on the privacy of the plaintiff was not disproportionate to the legal interest pursued, having regard to the values of a sovereign, independent, democratic state.*

(2) It is also a defence to an action under ***subsection (ii)*** *of* ***section*** *2 of this Act to show that the defendant did not believe and had no reasonable grounds to believe that the information had been obtained by means of privacy-invasive surveillance.*

(3) The defences under ***subsections*** *(1) and (2) of this section are without prejudice to any constitutional rights of the defendant.*

Remedies

4. In an action under ***section*** *2 of this Act, the Court may grant such relief as it considers appropriate in the circumstances, including any or all of the following:*

(a) damages;

(b) an account of profits;

(c) a privacy order;

(d) delivery up to the plaintiff of all material that has come into the defendant's possession by reason or in consequence of the tort.

Privacy order

5. (1) The Court may, if it is of opinion that there are reasonable grounds for believing that a tort is being or is about to be committed contrary to ***section*** *2 of this Act, by order (in this Act called a "privacy order"), prohibit the defendant from invading the privacy of the other person or disclosing or publishing the information or material, as the case may be, until further order by the Court or until such other time as the Court shall specify.*

(2) A privacy order may be varied by the Court on the application of either the plaintiff or the defendant.

(3) A privacy order may be discharged by the Court on the application of either the plaintiff or the defendant if the Court is satisfied that the privacy of the individual on whose behalf the order was made does not require that the order shall continue in force.

(4) A privacy order made by a court on appeal from another court shall be treated as if it had been made by that other court.

(5) A privacy order shall take effect on notification of its making being given to the defendant.

(6) Oral communication to the defendant by or on behalf of the plaintiff of the fact that a privacy order has been made, together with production of a copy of the order, shall, without prejudice to the sufficiency of any other form of notification, be taken to be sufficient notification to the defendant of the making of the order.

(7) If the defendant is present at the sitting of the Court at which the privacy order is made, that person shall be taken for the purposes of ***subsection*** *(5) of this section, to have been notified of its making.*

(8) An order varying or discharging a privacy order shall take effect on notification of its making being given to the plaintiff or defendant, being the person other than the person who applied for the variation, and for this purpose ***subsection*** *(6) and (7) of this section shall apply with the necessary modifications.*

(9) The Court, on making, varying or discharging a privacy order, shall cause a copy of the order in question to be given or sent as soon as practicable to the plaintiff and the defendant.

(10) Non-compliance with ***subsection*** *(9) of this section shall not affect the validity of the order.*

(11) An appeal from a privacy order shall, if the court that made the order or the court to which the appeal is brought so determines (but not otherwise), stay the operation of the order on such terms (if any) as may be imposed by the court making the determination.

Right of action

6. *(1) A right of action under* ***section*** *2 of this Act accrues to the person whose privacy is alleged to have been or to be about to be invaded and to any other person who is legally entitled to act on behalf of that person.*

(2) An action or right of action under ***section*** *2 of this Act is extinguished by the death of the person whose privacy is alleged to have been invaded.*

Limitation period

7. *An action under* ***section*** *2 of this Act shall be commenced within three years from the date on which the person who claims his or her privacy has*

been invaded became aware or ought reasonably to have become aware of the surveillance, disclosure or publication, as the case may be.

Right of action and other remedies

8. *(1) The rights of action and the remedies under this Act are in addition to, and not in derogation of, any other right of action or remedy available otherwise than under this Act.*

(2) This section shall not be construed as requiring any damages awarded in an action under ***section*** *2 of this Act to be disregarded in assessing damages in any other proceedings arising out of the same act as gave rise to a cause of action under* ***section*** *2.*

Title

9. *This Act may be cited as the Surveillance Privacy Act.*

9.62 These causes of action should provide a civil remedy in most cases where a person's privacy has been infringed by or as a result of surveillance. For example, a person whose telephone conversations are unlawfully recorded may sue the person responsible and succeed in an action for breach of privacy without the need to show any particular loss as a result of the invasive recording. Similarly, a person who is photographed in a private garden and whose photograph is published without her or his consent may sue for the invasion of privacy. The need for consent to publication in such circumstances will place some constraint on the media in that consent will probably need to be obtained in situations where it is presently not sought, but we think that it is not an unduly onerous condition to impose in seeking to protect individual privacy. In many situations, as at public functions, privacy will not be in issue or, if it is, consent may be implied. For example, consent to surveillance would be implied where persons attending a race-meeting or other sporting, cultural or social occasion normally covered by television - where shots of the attendance are a regular feature of such coverage - were "caught" on camera exchanging intimacies. The adoption of our proposals would ensure that the hospital patient would have a remedy against the journalist who photographed her or him without consent while hospitalised and against any newspaper which published the photograph without the patient's consent. A courting couple would however not have a remedy against the birdwatcher who accidentally saw them through binoculars, even if they were on private premises, since the element of "intention" would not be present - not, that is, unless the birdwatcher was to focus the binoculars on the couple and start watching them instead of birds - in which case it is right that a civil remedy should be available to the couple.

Unauthorised Use Of One's Image, Name Or Voice

9.63 We mentioned earlier that it has been accepted in the United States of

America that one has an interest in the use to which one's name or likeness is put and that this interest has been protected under the heading of privacy.[69] The tort originally comprised the appropriation, for the defendant's benefit or advantage, of the plaintiff's name or likeness[70] and has been extended by the courts to other indicia of identity such as a person's nickname[71] or vocal style.[72] It is crucial to the success of an action that the plaintiff be identifiable and that the defendant have appropriated the identifying characteristic or material to her or his advantage, although it is not always necessary that the advantage be pecuniary. Of the four privacy torts in the U.S.A., it is this one which is litigated most often and "which generates more successful claims that the other three branches combined."[73]

9.64 The Canadian Privacy Acts also protect the use of one's voice as well as of one's name and likeness. Among the examples of violations of privacy given in the Saskatchewan Act is

> "use of the name or likeness or voice of a person for the purposes of advertising or promoting the sale of, or any other trading in, any property or services, for any other purposes of gain to the user if, in the course of the use, the person is identified or identifiable and the user intended to exploit the name or likeness or voice of that person"[74],

without the consent, express or implied, of the person or of some other person with the lawful authority to give consent.

9.65 Nor are such actions peculiar to common law jurisdictions. Comparable causes of action exist in a number of civil law jurisdictions. For example, a right to one's portrait was established and protected in Germany by s.22f. of the *Act on Copyright in Artistic Creations, 1907*. As the First Civil Division of the German Supreme Court said in a landmark decision of 1958 involving the dissemination of a poster with a touched-up picture of a show-jumper on it advertising a pharmaceutical preparation reported to increase sexual potency:

> "... the protection afforded by s.22, according to which portraits may be distributed or shown publicly only with the subject's consent, rests in essence on the fundamental principle of a person's freedom in his highly personal private life, in which the outward appearance of human being plays an essential part. The unauthorised publication of a portrait constitutes, as has long been recognised in legal literature, an attack on the freedom of self-determination and the free expression of the

---

69 See above paras. 4.27 & 9.9.

70 See, e.g., *Pasevich v. New England Life Insurance Co.*, 1905, 122 Ga. 190, 50 S.E. 68; *Flake v. Greensboro News Co.*, 1938, 212 N.C. 780, 195 S.E. 55; *Kerby v. Hal Roach Studios*, 1942, 53 Cal. App. 2d 207, 127 P.2d 577; and *Flores v. Mosler Safe Co.*, 1959, 7 N.Y. 2d 276, 196 N.Y.S. 2d 975, 164 N.E. 2d 853.

71 See *Hirsch v. S.C. Johnson & Son Inc.*, 1979, 90 Wis. 2d 379.

72 See *Midler v. Ford Motor Co.*, 1988, 849 F. 2d. 460.

73 B.S. Markesinis, *op. cit.*, p.423.

74 Section 3(c). See also s.3 of the British Columbia Privacy Act; s.3(3) of the Manitoba Privacy Act; and s.4(c) of the Newfoundland Privacy Act.

personality. The reason why a third party's arbitrary publication of a portrait is not allowed is that the person portrayed is thereby deprived of his freedom to dispose by his own decision of this interest in his individual sphere."[75]

The provisions of the 1907 Act were originally understood to relate to the right to one's own portrait or likeness. This right however came subsequently to be regarded as an aspect of the general right of personality, and the provisions were interpreted to apply also to the representation of a person by an actor on stage, and the use of one's name and opinion for advertising purposes.[76] In one case which concerned the publication in a major news magazine of the plaintiff's picture along with allegations that he had been involved in the illegal granting of residence permits to a number of persons, including Syrian terrorists, the court held that such publication of the plaintiff's picture constituted a more serious interference with his right of privacy than had he been mentioned by name alone.[77]

9.66 French law also protects persons against the exploitation of their personality, that is, the unauthorised use for gain of elements of personality such as a name, image or voice.[78] Most of the cases deal with exploitation in the context of advertising. When a picture of President Pompidou on board a motor-boat was reproduced in an advertisement for the motor in a weekly magazine, a Paris court held that this constituted an infringement of Pompidou's right to his own image.[79] Protection in the case of one's image covers not only exploitation for gain but also the unauthorised taking of one's picture and publication generally.[80] Protection in these cases had in fact first been afforded in respect of the publication of a picture of a well-known actress on her deathbed and was only subsequently extended to living persons.[81]

9.67 It has been queried whether such interests are in fact properly regarded as privacy interests. Some U.S. courts have described the right to one's name or likeness as a "right to publicity" and have drawn attention to the commercial nature of the right. One commentator has recently remarked:

> "... the right to publicity is not really a 'privacy' right at all. The plaintiffs in publicity cases ... regularly exploit their names and images for profit. How are these celebrities to explain to the jury their 'hurt feelings' that this supposedly unwanted publicity has given them when

---

75 26 BGHZ 349, *Neue Juristische Wochenschrift* 827, reproduced in B.S. Markesinis, *op. cit.*, p.380, at p.384.

76 See, e.g., 35 BGHZ 363, *Neue Juristische Wochenschrift* 1961, 2059, reproduced in B.S. Markesinis, *op. cit.*, p.386, 35 BVerfGE 202, reproduced in Markesinis, p.390; *Neue Juristische Wochenschrift* 1987, 2682, reproduced in Markesinis, p.398; and *Neue Juristische Wochenschrift* 1988, 737, reproduced in Markesinis, p.407.

77 Cologne Court of Appeal, *Neue Juristische Wochenschrift* 1987, 2682.

78 See P. Kayser, *op. cit.*, pp.117-120.

79 *Juris-classeur périodique* 1980, II, 16328.

80 See P. Kayser, *op. cit.*, pp.120-133.

81 Decision of Paris court, 16 June 1858, D.1858.3.62. For a more recent decision relating to the publication of a picture of a well-known French actor on his deathbed, *Marcelle Fournier and Others v. Société COGEDI-Presse*, D.1977, J.83.

they spend most of their working hours trying to sell themselves to the highest bidder? The true ancestor of this right is not the right to be left alone, but rather the law of copyright and trademarks."[82]

Similarly, other commentators have said of the U.S. decisions that

> "Although the element of protection of the plaintiff's personal feelings is obviously not to be ignored ..., the effect of the appropriation decisions is to recognise or create an exclusive right in the individual plaintiff to a species of trade name, his own, and a kind of trade mark in his likeness."[83]

9.68 It certainly seems that in the U.S.A. the tort is usually aimed at commercial exploitation. Moreover it has been pointed out that, unlike the interests protected by the other forms of privacy tort, which are personal to the victim and cannot be assigned or enforced after death, the right to control commercial exploitation is assignable *inter vivos* and has been held in most states to be a descendible interest enforceable after the victim's death, at least for a number of years.[84] The wording of the tort in the Canadian provincial statutes also suggests that it is concerned with the unauthorised use for gain of material closely linked to the identity of the plaintiff. Indeed, in one of these statutes, it is treated as a distinct tort.[85] Although the element of gain is also present in many of the German cases, it would seem that this is not essential to the success of an action in that jurisdiction, and the courts have stated that the interest being protected is that of personality as such rather than merely the commercial exploitation of one's personality by another person. Similarly, in some of the French cases, the prejudice which was suffered was material, in some moral, and in others both material and moral. Also, in some, protection has been afforded against misrepresentation or being placed in a false light and has applied to one's public activities as well as one's private life, but, in others, the object has been to protect individual privacy.

9.69 We note that in all four countries, although the right may often be invoked by persons in the public eye since it is their name, likeness or voice which is most likely to be misappropriated by another for reasons of profit, it is enjoyed by everyone. The photograph of a handsome person may be used to advertise a product merely because the person is handsome, not because she or he is well-known. Moreover, where the person does not consent to such use of the photograph, she or he may feel offended or embarrassed simply because they dislike publicity or because they dislike being associated with the product. In such cases, the protected interest is not necessarily proprietary or commercial. It is human dignity.

---

82 D. Bedingfield, "Privacy or Publicity? The Enduring Confusion Surrounding the American Tort of Invasion of Privacy", (1992) 55 M.L.R. 111 at 114.

83 *Prosser and Keeton on Torts*, 5th ed., p.854.

84 See B.S. Markesinis, *op. cit.*, p.423.

85 See s.3 of the British Columbia Privacy Act.

9.70 It seems to us therefore that, in some cases, the interest protected by these causes of action is indeed privacy. In other cases, however, perhaps the majority of cases, the interest is essentially commercial. The actions have a dual character. In the context of this Paper, in which we are considering only the protection of privacy in cases of surveillance, we do not think it appropriate to make any recommendation as to whether or not a comparable cause of action should be introduced in Ireland. The actions deal with interests which have no connection with privacy, e.g. the unauthorised publication of a photograph of a politician at a public function as part of a campaign to promote jackets of the type the politician is wearing. In so far as they protect privacy interests, they go beyond the protection of privacy merely from abusive surveillance. Moreover, while they may afford a remedy for an individual in respect of the use made of personal material obtained by surveillance, they do not address the surveillance itself. We have already recommended that everyone should be under a duty not to invade the privacy of another by means of surveillance and not to disclose or publish information obtained by such means. If this recommendation is implemented, it should provide a remedy in cases of privacy-invasive surveillance, including, e.g., the publication for commercial purposes of a photograph of an individual covertly taken on private premises.

CHAPTER 10: VISUAL SURVEILLANCE

Introduction

10.1 For all except the hermit being overseen in one's daily life is an inherent feature of social existence. No law should try to ban or to limit the visual communication by which human beings normally interact with one another and relate to the world in which they find themselves. However there is a point at which such observation becomes unwelcome intrusion, where it is prying and offensive to the dignity of another person. It is this point which a law protective of privacy must seek to identify and which it should only allow to be passed without sanction when there is an overwhelming public interest or greater private interest to be upheld.

10.2 Most visual observation by unassisted human eyesight[1] is unobjectionable. If a person living in a flat undresses in a room overlooked by an adjacent block of flats, there is an understood possibility of being seen by someone in the adjoining building. It is reasonable to expect persons undressing to draw the curtains if they wish to screen themselves from the view of others. After all, that is the main purpose of curtains, blinds and shutters. The mere fact that the person is in his or her own home does not mean that there should, or that there can be, a blanket prohibition on the person's activities being seen by others. The location of the activity may however be relevant to whether there is an issue of privacy and to whether an individual's privacy has been infringed or not. For example, if persons are sunbathing in their garden, they may reasonably object if passersby climb onto a boundary wall to ogle. The point at which visual observation becomes intrusive and offensive to the dignity of another person has been reached. It would not however be reasonable to object if the persons were sunbathing in a public place such as a beach. Conversely, the mere fact that an

1 Including the use of spectacles and contact lenses.

activity occurs in public does not mean that a person's dignity may not be affected, although commonsense suggests that one must accept the likelihood, and often the certainty, of being viewed by others while in a public place but need not accept anything like a comparable likelihood while at home or on other private premises. Casually being seen on the street by passersby is one thing. Being subjected to close visual surveillance is another.

10.3 The greatest risk to privacy comes of course nowadays from technologically-assisted vision rather than the use of normal human eyesight. Even when the technology is not concealed, those observed may be unaware of its existence, for example, because it is situated a great distance away, or they may have little choice as to whether they are viewed or not as, for example, in a bank or supermarket where all tills and cashdesks are monitored by camera. Where the technology is concealed, those observed are unlikely to be aware of the surveillance and are therefore unlikely to be in a position to take precautions against being observed should they so wish.

10.4 The challenge in formulating a law to protect individuals from unwanted surveillance is to permit surveillance for legitimate purposes and to provide safeguards where the surveillance is legitimate while outlawing surveillance for purposes which are not acceptable and the abuse of surveillance which is otherwise lawful. We have already recommended the creation of a number of statutory torts as a means of affording a remedy to an individual in respect of privacy-invasive surveillance. What we consider in this Chapter is whether the sanctions of the criminal law should also attach to such conduct and, in the case of authorised surveillance, what legal safeguards are desirable to ensure that the legal authority is not exceeded or abused.

10.5 The State's international obligations require that any interference with privacy have a legal basis and that the law contain safeguards for the individual where there is a legitimate ground for interference.[2] Therefore, to the extent that surveillance impacts on privacy, it should be legally regulated. Moreover, since video surveillance has become so much part of everyday life, regulation and legal guarantees against abuse are in any event highly desirable and somewhat overdue.

10.6 Few states have as yet adopted legislation specifically regulating video surveillance, but many penalise the intrusive use of optical devices. We shall briefly review some of this legislation as well as other measures and legislative proposals for pointers as to how this legal vacuum might be filled in Ireland.

---

2 See above paras. 7.17-7.22 & 7.45-7.48.

The Law In Other Jurisdictions

(i) Australia

10.7 Law enforcement agencies conduct covert optical surveillance under warrants issued in accordance with Commonwealth legislation. Otherwise there is no specific regulation by law of the use of optical devices in Australia and therefore no specific legal safeguards in relation to their use.[3]

10.8 Some safeguards of a formal kind do however exist in the context of the operation of the office of the Privacy Commissioner. This office was established by the *Privacy Act 1988* which deals mainly with information privacy.[4] One of the matters of concern to the Commissioner has been the use by Commonwealth agencies of covert optical surveillance for investigating a wide range of activities, e.g. by the Australian Customs Service for intercepting prohibited goods, especially illicit drugs, and by the Australian Tax Office and Department of Social Security to investigate suspected fraud. The Privacy Act specifies a number of Information Privacy Principles which are applicable to records of personal information concerning an individual,[5] and the Commissioner is empowered by the Act:

> "to prepare, and to publish in such a manner as the Commissioner considers appropriate, guidelines for the avoidance of acts or practices of an agency that may or might be interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals."[6]

10.9 In 1992 the Commissioner drew up *Guidelines* on the application of the information privacy principles where Commonwealth agencies conduct covert optical surveillance, the results of which are recorded in some form.[7] Optical is defined to include photography, video cameras or direct observation (including the use of binoculars); covert surveillance as the secretive, continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals which is then recorded in material form, including notes and photographs. The *Guidelines* are advisory rather than mandatory, but adherence or otherwise by the agencies to the standards set forth therein is taken into account by the Commissioner in the event of a complaint or audit relating to their compliance with the Information Privacy Principles. They are applicable to all Commonwealth agencies other than national security organisations and agencies using covert surveillance for law enforcement purposes. They are intended to provide a framework for the agencies to develop their own detailed guidelines taking into account their role, their priorities and

---

3 In its *Report on Privacy*, the Australian Law Reform Commission recommended that, outside public places, the use of optical devices to observe people who could otherwise reasonably expect to be safe from observation should be prohibited: para. 1188.

4 On this office see Part IV of the Act.

5 The 11 principles are listed in s.14 of the Act.

6 Section 27(1)(e).

7 *Covert Optical Surveillance in Commonwealth Administration - Guidelines*, Human Rights and Equal Opportunity Commission, Sydney, Australia, February 1992. The *Guidelines* are reproduced below at Appendix E.

other operational factors, when conducting covert surveillance. In situations where covert surveillance does not lead to the creation of a record, agencies are encouraged to adopt the *Guidelines* where relevant.

10.10 With respect to the decision to undertake covert surveillance, the *Guidelines* provide:

1. Covert surveillance may only be undertaken for a lawful purpose which is related to the function and activity of the agency.

2. Each agency should identify the circumstances or offences for which covert surveillance may be used and the Acts which may justify the agency undertaking the practice.

3. Approval to conduct covert surveillance in any particular case should be made at a senior level, taking into account procedures in place for the conduct of such activities.

4. In deciding to conduct covert surveillance agencies should consider the following factors:

   (a) That there be reasonable suspicion to believe that an offence or an unlawful activity is about to be committed, is being committed or has been committed;

   (b) That other forms of investigation have been considered and have been assessed to be unsuitable, or other forms of investigation have been tried and have been found to be inconclusive or unsuitable;

   (c) The benefits arising from obtaining relevant information by covert surveillance are considered to outweigh to a substantial degree the intrusion on the privacy of the surveillance subject/s.

10.11 As regards the actual conduct of the surveillance, the *Guidelines* state that the agencies should be mindful of the following:

1. The collection of personal information using a covert surveillance operation should be conducted in a lawful manner. Any covert surveillance operation which may involve the commission of a criminal offence or which may give rise to civil action, for example, trespass to land or goods, cannot be sanctioned;

2. The collection should not involve entrapment of the surveillance subject. Hence, passive observation is permissible. However, any attempts actively to induce the surveillance subject into a situation in which that person would not ordinarily and voluntarily enter should not be

permitted;[8]

3. Agencies should avoid any actions which may unreasonably impinge on the privacy and rights of other people;[9]

4. Where practicable, only material relevant to the purpose of conducting the covert surveillance should be collected. There should be a clear separation of facts from opinions and only relevant personal information should be included in records resulting from the surveillance.[10]

10.12 In addition to these general *Guidelines*, the Privacy Commissioner has also produced *Specific Guidelines* for agencies investigating compensation claims, this being an area in which covert surveillance is most used in Commonwealth administration.[11]

(ii) Denmark

10.13 Denmark was one of the first countries to subject video surveillance to legislative regulation. The Act of 1982 is short and deals only with surveillance by private persons.[12] Video surveillance is defined as constant or regular surveillance of the person using a remote-controlled or automatic video camera, photographic camera or similar equipment.[13]

10.14 There is a general prohibition on the surveillance of streets, roads, squares and similar areas used by ordinary traffic,[14] but there are two exceptions to this prohibition. It does not apply to:

1. Video surveillance of petrol stations, factory areas, enclosed shopping centres and similar areas in which business is conducted, provided the surveillance is carried out by the person or persons in charge of the area;[15] and

2. Video surveillance which is not connected with the recording of pictures on videotape or film when the surveillance is carried out as part of a surveillance of private entrances, housefronts, fenced-in or cordoned-off areas, etc.[16]

---

8 The *Guidelines* give the example that, whilst an investigator could pose as a patient in cases of investigations for overservicing by a doctor to afford an opportunity for the doctor to commit a crime if the doctor is so minded, the investigator should not induce a doctor into a crime the doctor is otherwise unwilling to commit.

9 The *Guidelines* give the example that, where practicable, including other individuals such as relatives and friends in photograph should be avoided.

10 The *Guidelines* also contain a section on the handling of records arising from covert surveillance: see below Appendix E.

11 These *Specific Guidelines* are reproduced below at Appendix E.

12 We are grateful to the Danish Ministry of Justice and to the Royal Danish Embassy in Dublin for supplying us with the text of this Act and information relating thereto.

13 Para. 1(2) of the Act.

14 Para. 1(1).

15 Para. 2(1).

16 Para. 2(2).

Moreover, any private person who undertakes video surveillance of places or rooms to which the public has free entry must explicitly publicise on signs that surveillance is taking place.[17] Under the legislation, the Minister for Justice is empowered to make rules in relation to these signs,[18] but as of February 1995 had not done so. The requirement to inform the public of surveillance by way of signs does not apply where the camera is not connected to recording equipment and the surveillance is carried out as part of a surveillance of a private entrance, housefront, fenced in or cordoned off area, etc.[19] Persons who contravene the prohibition on the surveillance of certain areas or who do not comply with the public notification requirement are liable to a fine.[20]

10.15 The Danish law therefore recognises the reality of resort to video surveillance by private actors in the modern world and accepts that it should be regarded as lawful in certain areas. It further acknowledges that in some of these areas safeguards are needed. It operates by way of a general prohibition on the surveillance of public places with exceptions.

10.16 In general the areas in which surveillance is permissible are private places and business areas. Where the private place is a room or other place to which members of the public have free access, the safeguard is that the public should be put on notice by means of a sign that they are subject to surveillance. Implicit in the general prohibition of video surveillance of public places by private persons is the view that such surveillance, if it is to be permitted at all, is only acceptable if carried out by a public authority.

10.17 The Danish Penal Code also penalises unauthorised photography of persons on private property, the latter being defined as a place to which the public is not admitted.[21] Thus the following are offences: taking photographs of people on private property without their consent, spying on people on private property with telescopes, binoculars and other such optical devices, making use of information so obtained, and printing in a newspaper a photograph of a person taken on private property without that person's consent.

(iii) France

10.18 From 1970-1994 it was an offence under Article 368 of the French Penal Code for anyone deliberately to interfere with the intimacy of the private life of another person by, *inter alia*, taking by means of any device, or communicating, the picture of a person in a private place, without the consent of that person.[22] When the pictures were taken in the course of a meeting, with the knowledge of all the participants, their consent was to be presumed. Anyone found guilty of this offence was liable to a term of imprisonment, a fine, or both. The same

---

17 Para. 3(1).
18 Para. 4.
19 Para. 3(2).
20 Para. 5.
21 See *Calcutt I*, para. 5.23 & 24.
22 Art. 368.2[0].

penalties applied in respect of the keeping, disclosure to the public or a third person, permitting the disclosure to the public or a third person, or use, whether public or otherwise, of every recording or document obtained in this way.[23] In case of conviction, the court could order the confiscation of the device by which the picture was taken and of any associated recording or document.[24]

10.19 The protection afforded by these provisions only applied if the person whose picture had been taken was at the time in a private place. The meaning of "a private place" has been elucidated by case law. A photograph taken of a person in the street falls outside the protection since a street is, by its nature, a public place.[25] Also, a place to which everyone has access, without any special authorisation, whether or not access is subject to certain conditions, is not a private place.[26] Thus the person who photographed a bare-breasted woman on a beach to which holiday-makers had free access committed no offence under Article 368.[27] He would however have committed an offence had the woman been sunbathing on the deck of a boat out at sea -provided the boat was not close to shore or an embarkation point. While out at sea, she was entitled to believe that she was sheltered from the gaze of others.[28] A hospital room is a private place,[29] as is one's home. Some places are by their nature always regarded as private, but the same place may be either public or private depending on its use at the time. Thus a shop to which the public has access during the day is not a private place during the day, but may be after closing hours.[30] The photograph need not be taken in a private place. It is sufficient if the person photographed is in such a place. Thus taking the picture of a person in a flat without the person's consent from outside the window of the flat may be an offence.[31] Protection applies even in death, provided the corpse is in a private place. Thus the unauthorised taking of photographs of an actor on his deathbed and their subsequent publication in a weekly magazine fell within the prohibition.[32]

10.20 It should be noted that a "private" element featured twice in the definition of the offence of unauthorised visual surveillance. In fact the essence of the offence was infringement of the intimacy of the private life of another. There would appear to be a tendency in some of the case-law to assume that if a person was caught on camera without their consent in a private place, there had been an infringement of the intimacy of their private life. On other occasions however the courts explicitly distinguished the two private elements of

---

23 Art. 369. See also Arts. 285 (proceedings against the press), 370 (photomontage) and 372 (attempt).
24 Art. 372.
25 See, e.g., Tribunal, chambre correctionnelle, Toulouse, 26 February 1974, D.1974.736.
26 See, e.g., Tribunal de grande instance, Paris, 23 October 1986, *Gaz. Pal.* 1987.1.21.
27 Tribunal de grande instance, Paris, 18 March 1971, D.1971.447; *Gaz. Pal.* 1972.1.59.
28 Tribunal de grande instance, Paris, 5 February 1979, *Juris-classeur périodique* 1980.II.19343.
29 See, e.g., Tribunal de grande instance, Paris, 14 March 1965, *Juris-classeur périodique* 1965.II.14223; 29 January 1986, *Gaz. Pal.* 1987 *Recueil des Sommaires* 127; and 17 March 1986, *Gaz. Pal.* 1986.2.429.
30 Tribunal de grande instance, Paris, 7 November 1975, D.1976.270. See also Court of Cassation, Criminal Division, 8 December 1983, *Bull. crim.* No. 333, *Gaz. Pal.* 1984.1; and 14 March 1984, *Bull. crim.* No. 110, D.1985.IR.17.
31 Court of Cassation, Criminal Division, 25 April 1989, *Bull. crim.* No. 165.
32 Court of Cassation, Criminal Division, 21 October 1980, *Bull. crim.* No. 262, D.1981.72. See also Tribunal de grande instance, Paris, 17 March 1986, *Gaz. Pal.* 1986.2.429.

the offence.[33]

10.21 Article 368 has been replaced by a comparable, but not identical, provision in the New Penal Code,[34] which came into force on 1 March 1994. This provides that it is an offence, by means of any conduct deliberately to infringe the intimacy of the private life of another person, *inter alia*, by taking, recording or communicating the image of a person who is in a private place without the consent of that person. The penalties have been increased, and the competence of a court to order confiscation remains. The significant changes are that the offence has been extended to include the recording of a picture and the means has been changed from that of any device ("*appareil*") to that of any conduct ("*procédé*"). The presumption of consent has also been tightened somewhat. It has been uncoupled from the situation of a meeting and only applies whenever pictures are taken with the knowledge of all the persons concerned, without them objecting thereto when they are in a position to do so. The new penalties also apply to the keeping, disclosure or permitting the disclosure to the public or a third person, or using in any way of every recording or document obtained in a manner contrary to the new provision of the Code.[35] When the latter offences are committed by members of the press or broadcasting, liability is determined by the law particularly relating to these media.[36] Earlier case law on the interpretation of Article 368 will continue to be relevant in so far as the new provisions overlap with the old.

(iv) Norway

10.22 Since 1 July 1991 it has been an offence in Norway punishable by fine for a person to engage in video surveillance in a public place without having clearly indicated by way of a notice that the place is under such surveillance.[37] Video surveillance is defined in the relevant provision of the Criminal Code as constant surveillance of persons effected in a regular manner by means of automatic television cameras, photographic devices or any other similar device. Complicity is likewise punishable with a fine.[38]

10.23 There is an exception for the police who may engage in covert video surveillance subject to a number of conditions.[39] These conditions are:

- there must exist reasonable grounds to suspect the commission of one or more criminal acts which are punishable with at least 6 months' imprisonment;

---

33 E.g. the two elements were distinguished by the Paris Police Tribunal, 25 May 1984, *Gaz. Pal.* 1984.2.632.
34 Article 226-1.
35 Art. 226-2.
36 *Ibid.*
37 Art. 390b of the Criminal Code.
38 Questions have been raised in the literature about the sufficiency of some notices which have been posted. Thus, Kaspersen has pointed out that notices about traffic surveillance in Trondheim have been placed on the access routes to the town and not on each route or street in which traffic is actually monitored: see K.B. Kaspersen, "Secret Video-Surveillance and Photography", (1992) *Norwegian Law Review.*
39 Art. 202 of the Code of Criminal Procedure.

- the surveillance must be of essential importance for the investigation;

- the surveillance must be authorised by a tribunal;

- authorisation must be given for a specific period which may not exceed 4 months at any one time and must not in any event be any longer than is strictly necessary.

A tribunal may decide to authorise such surveillance without the person who is to be the subject of the surveillance or any person affected by the decision having the possibility to be heard or the decision being communicated to such person.

10.24 In addition, the *Personal Data Registers Act* of *1978* was amended in 1993 to include two new provisions specifically dealing with the use of video cameras for the purpose of surveillance in both the private and the public sectors: ss.37a and 37b.[40] This Act, as its title suggests, concerns the keeping of personal data registers. Personal data is defined as information and opinions which directly or indirectly can be linked to identifiable persons, to groups or to institutions[41]; personal register as a register where information is systematically stored in such a way that information on a given person can be retrieved therefrom.[42]

10.25 Section 37a allows video surveillance and picture recordings if there are reasonable grounds for them. In the case of surveillance of an area which is regularly used by only a limited number of people, exceptional grounds must be shown. Video surveillance is defined as continual or regular repeated surveillance of persons by means of a distantly operated or automatically functioning television camera, picture camera or similar apparatus. Any recording must be erased when there is no longer any reasonable ground for keeping it.

10.26 Section 37b regulates the release, storage and use of recorded pictures and film. The pictures and film may only be handed over to others if this is provided for by law or if those who have been filmed agree. Also, subject to any statutory duty of professional secrecy, they may be handed over to the police in connection with criminal offences or accidents. In the event that a recording is not erased in accordance with s.37a, the Data Commission may order its erasure. The King is also empowered by the section to make regulations for the securing, use, release and erasing of recorded film or pictures, and for a right of a person to view those parts of a film or picture in which she or he appears.

10.27 A regulation based on s.37b came into force on 15 October 1994. The main provisions of this regulation are that:

---

40 We are grateful to the Norwegian Department of Legislation, Royal Ministry of Justice and the Police, Oslo, and to the Norwegian Embassy in Dublin for copies of this legislation and the regulation discussed below, and for assistance in translating these documents.

41 Art. 1.

42 *Ibid.*

- the recorded film and pictures must be properly stored;

- only those may have access to the recordings who have reasonable grounds for it in their work;

- the recordings may only be used for the purpose for which they were obtained. The police may however use recordings in their possession in the prevention or investigation of crime, as evidence in criminal cases, or to verify the facts of an accident;

- the recordings may only be handed over to others if this is in accordance with the Constitution or if those who have been filmed consent thereto. Also, if not precluded by a statutory duty of professional secrecy, recordings may be given to the police for the purpose of investigating crime or accidents;

- the recordings may not be kept for more than 7 days. There are a number of exceptions to this time-limit in the case of banks, post offices, the police and national defence. Recordings should however always be erased when there are no reasonable grounds for keeping them;

- if the recordings are kept for more than 7 days, those who have been filmed may see the parts of a recording where they themselves appear.

Contravention of the regulation is punishable with imprisonment or a fine.

(v) Sweden

10.28 Legislation has also recently been passed in Sweden to regulate the use of video cameras.[43] It came into force on 1 July 1990, replacing earlier legislation of 1977. It applies to remote-controlled cameras and other optical electronic devices, including equipment for the treatment and preservation of pictures taken by remote camera. The law is targeted at installed cameras and requires a degree of permanency in the location of the camera for its application. It does not apply to cameras which are manually operated. It would not therefore apply to the personal use of a handheld video camera.[44] Nor does it apply to equipment used temporarily, e.g. as part of a marketing demonstration.

10.29 A licence is required for surveillance of a place to which the public has access.[45] It is sufficient if there is general access even though members of the public do not usually frequent the place. Indoor areas are covered as well as

---

43 *Lagen om övervakningskameror* (Act on Surveillance Cameras), 1990:484. We are grateful to the Swedish Department of Justice, Stockholm, and to the Swedish Embassy in Dublin for providing us with a copy of this Act and of the administrative ordinance applicable to the granting of surveillance licences and for assistance in translating these documents. We are also grateful to Dr. Iain Cameron, Faculty of law, Uppsala University, for a summary of the main provisions of the legislation.

44 Section 1.

45 Section 4.

outdoor areas. Thus, places in shops and banks are covered by the requirement as are common areas in an apartment block such as a communal laundry. Also covered are forestry areas, rivers and lakes. Staff, storage and maintenance areas are not covered. Police cameras used only for monitoring the speed of traffic and cameras used to monitor an area officially classed as a defence area under the Act on Protection of Defence Installations[46] are also excepted from the requirement of a licence. In exceptional circumstances, the police may instal a camera and seek a licence within the next 14 days.[47] Provided an application for a licence is made, the camera may be operated pending the decision on the application.

10.30 The use of video cameras must respect the integrity of the person.[48] The basic principle is that an individual should know she or he is subject to surveillance. Easily visible signs alerting persons to the surveillance must be displayed.[49] There are exceptions for police cameras used only for monitoring the speed of traffic and cameras used to monitor an area classed as a defence area. Other dispensations from the notice requirement may be granted where there are special reasons, for example, if there is concern about public safety or about the safety of a visiting foreign dignitary, and dispensation may be granted subject to conditions.

10.31 Licences and dispensations from the notice requirement are granted by the relevant county administrative board.[50] Applications must be in writing, and copies of the board's decisions are given to the office of the Chancellor of Justice which monitors the local authorities in Sweden.[51] In making its decision, the county administrative board must consult with the municipality concerned and take account of its view.[52] In the event a licence is refused, appeal may be made to the district administrative court.[53] An appeal against a decision to grant a licence may be made by the Chancellor of Justice, the municipality in whose area the camera is installed or, where the camera is located in a workplace, the relevant trade union/s.

10.32 A licence may be granted only if the applicant has a legitimate interest in the use of a surveillance camera and that interest cannot be met in any other way.[54] In deciding whether or not to grant a licence, the county administrative board must have regard to the implications for individuals' personal integrity. If the implications are minimal considering the type of equipment to be used and the area to be subjected to surveillance, a licence may be granted. Surveillance in such places as shops, banks, department stores and post offices are regarded as fulfilling a legitimate interest. However, even where licences are granted,

---

46 1990:217.
47 Section 4.
48 Section 2.
49 Section 3.
50 Section 7. An administrative ordinance of 7 June 1990, SFS 1990:487, applies to applications for a licence.
51 See para. 3 of the administrative ordinance.
52 Section 9.
53 See s.18 of the Act and para. 4 of the administrative ordinance.
54 Section 5 of the Act.

zoom lenses must not be used to take close-up pictures. Where the risk to personal integrity is more than minimal, the board must balance the individual interest in personal integrity against the interest in surveillance and may only grant a licence where the latter completely outweighs the former. In practice, the balance will often be drawn in favour of the prevention of crime or of an accident.[55]

10.33 Licences may be granted subject to conditions and for a limited period of time.[56] For example, a licence may specify where a camera is to be mounted. A licence may also specify rules to be observed in the use of the camera and may, for example, specify who is entitled to use the camera and the way the camera may be used. The Secrecy Act[57] applies to the use of cameras, thereby safeguarding from unauthorised disclosure personal information obtained by such surveillance.[58]

10.34 A separate licence is required for the retention or editing of still pictures or video film.[59] A licence will only be granted where this is necessary to prevent crime or there is some other special need to preserve the pictures or film as, e.g., for security purposes.

10.35 The county administrative boards monitor compliance with the conditions of a licence.[60] They have a right of access to camera installations and a licence may be withdrawn or modified in appropriate cases. Where the conditions justifying the camera installation no longer apply, a licence must be withdrawn.

10.36 A person who deliberately or by negligence fails to notify the public of surveillance or breaches the conditions of a licence commits an offence and is liable to a fine or term of imprisonment.[61] In cases of minor infringement, no fine or imprisonment may be imposed. Also, the surveillance equipment used in connection with the crime may be confiscated if confiscation would not be unreasonable in the circumstances.[62] A fine may be imposed for refusing the county administrative board access to the installation.[63]

(vi) United Kingdom

10.37 There is no specific legislation in the United Kingdom governing the use of optical devices, but the Younger Committee on Privacy considered the creation of an offence of surreptitious surveillance which would apply to the use both of listening and optical devices.[64] The Committee took the view that to

---

55 As regards the latter, it is common in Sweden for escalators in a department store to be monitored by camera.
56 Section 10.
57 *Lag om ändring i sekretesslagen* (1980:100) SFS 1980:485.
58 Section 14 of the Act on Surveillance Cameras.
59 Section 6.
60 See ss.11-13 of the Act.
61 Not exceeding one year: see s.15.
62 Section 16.
63 Section 17.
64 See the Committee's *Report*, para. 560-563.

observe, by means of a device, persons who had put themselves in, or otherwise established, a situation in which they would be justified in believing that they could not be observed was significantly offensive and should be made an offence. It identified three considerations of which, in its opinion, any statement of the offence should take particular account:

(i) There should be an intention to use the device with the object to which exception is taken. Where the person observed has created, or put herself or himself in, a situation of normally adequate protection against being observed, and a technical device is employed with some other object in view, there should be no offence;

(ii) The complainant should have to show that she or he had taken precautions against being observed, which, but for the use of the device, would have been adequate; and

(iii) Use of a device with the consent of the person observed should be excluded.

The Committee therefore recommended the enactment of a criminal offence of surreptitious surveillance by means of a technical device which would comprise the following elements:

"a. a technical device;

b. surreptitious use of the device;

c. a person who is, or his possessions which are, the object of surveillance;

d. a set of circumstances in which, were it not for the use of the device, that person would be justified in believing that he had protected himself or his possessions from surveillance whether by overhearing or observation;

e. an intention by the user to render those circumstances ineffective as protection against overhearing or observation; and

f. absence of consent by the victim."[65]

Incitement to commit this offence would also be an offence and would catch anyone advertising technical devices with reference to their aptness for surreptitious surveillance.[66] The Committee did not recommend the creation of any offence in relation to overt surveillance since, in its view, this type of surveillance is known to persons and they are in a position to do something about

65 Para. 563.
66 Para. 564.

it.[67]

10.38 As we have seen, the later Committee on Privacy and Related Matters recommended the creation of a number of offences in the context of its study of intrusive conduct by the press.[68] Among the offences it recommended were the placing of a surveillance device on private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication, and the taking of a photograph of an individual who is on private property, without the individual's consent, with a view to its publication with intent that the individual be identifiable.[69] It also proposed a number of defences to these crimes.[70] It rejected the creation of a further offence of publishing any photograph or information obtained by the unlawful use of a surveillance device.[71] In his *Review of Press Self-Regulation*, Calcutt endorsed these recommendations and suggested some modifications to them, notably that the offences should be extended to the use of a surveillance device on private property as well as the placing of a device on such property.[72]

Conclusion And Recommendations

10.39 Few countries as yet specifically regulate video surveillance. In most, developments in technology have outstripped the law and the increasing use, both covert and overt, of optical devices, calls for the introduction of legal safeguards, *inter alia*, to protect individual privacy.

10.40 We do not think it appropriate in the context of this Paper to recommend the introduction of a system of licensing in Ireland such as exists in Sweden. Such a recommendation could only be made after consideration of issues other than that of privacy.[73] We do however think that our brief comparative survey of relevant legislation, practice and proposals in other countries gives some indication of the type of measure which is desirable in Ireland.

10.41 We are of the opinion that not all privacy-invasive visual surveillance should attract the sanctions of the criminal law. The private investigator who is paid to trail a person and to report on the person's movements and who does so by sight without infringing the present law should not be subject to criminal sanction. In so far as an investigator intrudes on a person's privacy, the torts of privacy-invasive surveillance which we have proposed will afford a remedy to the victim. The same applies to members of the media. This is sufficient. We do

---

67 Para. 565. It did however recommend the establishment of a cause of action at civil law in relation to both offensive covert and offensive overt surveillance. The new tort would comprise the same elements as the offence of surreptitious surveillance except that use of the device need not be surreptitious: *ibid.*

68 See in general above paras. 8.14-8.22.

69 See above para. 8.20.

70 See above para. 8.21.

71 It did however recommend a civil remedy in such cases: see above para. 8.22.

72 See above para. 8.24.

73 We also note the conclusion of the Younger Committee on Privacy that a system of control by licensing in this area in Britain would probably be unduly cumbersome and probably ineffective: *Report*, para. 570.

not consider most such conduct to be so morally reprehensible as to merit criminal penalties. Certainly the behaviour of passersby who climb onto a boundary wall to ogle at sunbathers is offensive,[74] and it might be thought that persons should be deterred by the criminal law from engaging in such conduct. Under our recommendations, they would be civilly liable, but not criminally liable. We think this is right. Not all irksome behaviour should be rendered criminal, only the more serious instances of such behaviour. If repeated, the sunbathers could seek a privacy order.[75] The situation is however different where sophisticated optical devices are used, particularly where they are used covertly. *We* therefore *recommend that it should be an offence to infringe the integrity of another person by observing the person by means of an optical device or by taking the person's picture by means of an optical device, without the consent of that person or of some other person legally entitled to give consent on behalf of that person. Consent may be express or implied. Taking a picture should be understood to include both taking still pictures and recording a picture on video tape.*

10.42 We favour a formulation of the offence by reference to the integrity of a person rather than to privacy as such. A greater degree of specificity is needed in the formulation of crimes as compared with civil wrongs. Moreover we do not believe that all invasions of privacy should be penalised, only the more serious ones; and use of the word "integrity" to describe what is protected would signify that it is affronts to human dignity which are penalised. The reference to the *intimacy* of private life in the French offences and the requirement in Sweden that the use of video cameras must respect the integrity of the person also seem to indicate that what are principally targeted by the criminal law of those countries are invasions of personal dignity.

10.43 The offence we recommend does not extend to the photographing of a private document or other private property. In our view, such extension of the offence would go too far. Thus aerial photography of a person's home, as occurred in *Bernstein of Leigh (Baron) v. Skyviews and General Ltd.*,[76] would not be caught by the offence. Nor would the photographing of the room of a person's house as such. The offence would start to bite however if the camera lens was focused on a person within the room.

10.44 For the purpose of this offence, a definition of an optical device would be needed. It could be defined narrowly so that only the use of more sophisticated devices would be covered by the offence, or broadly, with the consequence that even the use of an old-fashioned Brownie camera would come within its scope. It seems to us that the threat to privacy stems largely from the use of electronic devices, and *we* therefore *propose that optical device be defined as a video camera or other similar electronic device*. This means that the use of some visual enhancement devices, such as binoculars, would not be covered by

---

74 See above para. 10.2.

75 See above paras. 9.50 & 9.61. Indeed an analogy might be drawn between such cases and the law on trespass, which in this State is not criminal.

76 [1978] 1 Q.B. 479. See above para. 4.8.

the offence.

10.45 Some advertence to the infringement of the integrity of another person should be required. To limit the mental element of the offence to the intentional infringement of another's integrity would, we think, be too restrictive. To extend it to all negligent conduct would be too wide-ranging. Where a person, in using the optical device, is aware of the likelihood of invading another's personal integrity, in our view, it is reasonable to expect that she or he exercise caution in the use of the device so as not to infringe the other's integrity, and where such caution is not taken, that, subject to the defence and exemptions from criminal liability we propose below, any resultant infringement be penalised. *We* accordingly *recommend the offence cover both intentional and reckless infringement of the integrity of another person.*

10.46 We do not find the formulation of the offences by reference to a private place, as in France, particularly helpful, and note that in deciding whether or not a place is private, the French courts have looked to the use of the place at the relevant time so that the same place may be private at one time but public at another. We take the view that even in a public place a person is still entitled to a degree of privacy, and the same view seems to be implicit in the Scandinavian legislation which regulates the use of video surveillance in public places. We also note that it is accepted in the relevant section of the *Broadcasting Guidelines for RTE Personnel* that persons are entitled to a degree of privacy in public places.[77] Location is relevant to the degree of privacy which a person may expect to enjoy, and this will usually be less when a person frequents a public place than when the person is at home. Location may therefore be relevant in deciding whether or not in a particular case there has been an infringement of personal integrity. Thus simply taking a person's picture on the street could not reasonably be regarded as an infringement of that person's integrity, but might well do so if the person was at home, particularly if, for example, the person was undressing. Whatever the formulation of the offence, it will be open to interpretation by the judiciary, but we believe that the formulation we are proposing is sufficiently precise to indicate that only the more egregious cases of invasion of privacy will be caught by it.

10.47 *It should also be an offence to communicate a picture so taken to another person or persons or to the public without the consent of the subject(s) of the picture or the consent of another person legally entitled to give consent on behalf of the subject(s).* Again, *consent may be express or implied; but it should be a defence to this offence that the person communicating the picture did not know and had no reason to believe that the picture had been taken in contravention of the integrity of a person. This offence should cover only the intentional communication of a picture, but should apply where the taking of the picture constituted either an intentional or a reckless infringement of the integrity of the other person.*

---

77 See above para. 8.11.

10.48 We note that the Younger Committee on Privacy recommended the creation of a new criminal offence only where the surveillance is surreptitious.[78] In contrast, the offences we recommend would apply whether the surveillance was covert or overt. We think that even where it is overt, the subject may not be in a position to prevent the surveillance, as in the German case mentioned in the last Chapter where a man subjected his mother-in-law to continuous surveillance.[79] We think that the sanction of the criminal law should apply to such cases. Such surveillance is not possible using normal human eyesight. It has been rendered possible by technological developments, and involves a degree of intrusion into privacy which in a democracy is only acceptable within limits strictly defined by the law.

10.49 The legitimate use of optical devices as, e.g., of video cameras for security purposes in banks, stores, post offices, etc. should not be penalised. Such surveillance would not generally fall within the ambit of the criminal offences we are proposing since, in the ordinary course of events, the filming of customers in such places does not impinge on their personal integrity. But it is right that such surveillance be penalised, if it is abused in order, for example, to film a particular part of the anatomy of a customer or intimate behaviour between two customers and the pictures are subsequently published without the customers' consent.

10.50 Infringements of personal integrity are rarely justified. Many of the grounds on which interference with privacy is permitted under the *European Convention on Human Rights*[80] do not, in our view, afford an acceptable basis for an infringement of the integrity of the person. The integrity of a person is an inner kernel, as it were, of privacy, and neither public safety, the economic well-being of a country, the prevention of disorder, or the protection of health or morals justify the non-consensual invasion of this particular private realm. These interests may afford good reason for the invasion of other aspects of privacy, but when they compete with privacy, they may be adequately protected without sacrificing personal integrity. Similarly it is not in general necessary to infringe a person's integrity in order to protect the rights of and freedoms of others.

10.51 There is one ground on which we believe it to be justified to invade the integrity of a person. This is in order to save human life. We place a very high value on the preservation of human life, and we think that if this objective conflicts with the protection of the integrity of a person, priority should be afforded it. *We* therefore *recommend that it should be a defence to the offences we propose that the surveillance was intended to protect the life of a person*. This would allow surveillance which is invasive of personal integrity to be conducted where the target of the surveillance poses a threat either to his or her own life or to the life of another person or persons. It would permit invasive surveillance of the person from whom the risk to life emanates without the consent of that

---

78 *Report*, para. 563, described above at para. 10.37.
79 See above para. 9.8.
80 See above para. 7.19.

person. It would not justify invasive surveillance of another person whose life is at risk without that person's consent.

10.52 We have also considered whether there should be a general defence relating to the prevention of crime. The investigation of crime is of course primarily a matter for the Gardaí, and we address surveillance by the Gardaí below. What we consider here is whether there should be a defence available to everyone that the invasion of another's personal integrity occurred in the investigation or prevention of crime. Such a defence would be of avail e.g. to private detectives, but would be of especial benefit to members of the media, given its role as public watchdog in a democracy. Investigative journalism is a sign of a healthy democracy and in principle should not be discouraged, but there would have to be limits to what was permissible. A degree of self-regulation already applies within the media in this regard,[81] and we welcome the acceptance of responsibility by the media in their use of surveillance. Nevertheless some of the limits should be set by the law. We believe that it is not necessary in pursuit of a news story to intrude on this inner kernel of a person's dignity. The public interest in the revelation of corrupt or criminal conduct can generally be served without resort to such invasive surveillance. Those cases where the public interest in the detection of crime outweighs respect for the integrity of the person should be tightly regulated, and we think that this can best be achieved by entrusting such cases to the Gardaí and by ensuring that in their use of surveillance the Gardaí are subject to strict control.

10.53 We do not consider that the offences we are proposing would have any significant dampening effect on the freedom of the media to investigate and publish stories which are of public interest. The offences are intended to protect only an inner core of privacy, and while caution will need to be exercised in the use of visual surveillance to ensure respect for this core, the exercise of such caution should not normally result in failure to acquire evidence of the commission of a crime or indeed any newsworthy story.

10.54 Another of the rare circumstances in which violation of the integrity of a person may be justified is in the interests of national security, and as with the detection of crime, we are of the view that only the State should be entitled to invoke national security as justification for such violation. It should not be open to private persons or bodies to excuse their conduct on this ground. Moreover State surveillance of this kind, even when taken in defence of the security of the State, should also be subject to strict control in order to preclude abuse of the power.

10.55 In order to allow for State surveillance which infringes the integrity of the person but which is justified in the interests of the investigation of crime or national security, *we recommend that it should be a defence to the offences we propose that the infringement occurred in the exercise of lawful authority.* By this

---

81 See above paras. 8.11 & 8.13.

we mean that there should be a clear legal basis for the infringement.

10.56 As regards the legal basis for visual surveillance by the State in the investigation of crime and in the interest of national security, we think it somewhat anomalous that the interception of postal packets and telecommunications messages for these purposes is subject by law to specific authorisation, conditions and safeguards[82] whereas other forms of surveillance for these purposes are not. We see no good reason why the former is extensively regulated, but the latter is not. There is of course an historical explanation for the difference in that the post and telegraph have long been in use as methods of communication and have therefore been subject to regulation, *inter alia*, to protect the secrecy of such communications, whereas it is only in recent years that sophisticated aural and visual devices have been invented and become readily available. This explanation does not however provide sufficient justification for the difference in legal regulation. A distinction may be drawn between the interception of communications and other forms of surveillance in that the former necessarily impinges on the secrecy of the communications, whereas the latter does not necessarily impact on the privacy of individuals. The police surveillance van on the streets of Dublin to detect crime[83] does not necessarily infringe individuals' privacy. It may however if the surveillance facilities are abused, and other forms of police surveillance, such as the secret photographing of persons on their own property, may impinge upon their privacy. We will therefore consider whether a régime such as that which applies under the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* should be extended to the use of video surveillance.

10.57 Under the 1993 Act, interception may only be authorised for the purpose of criminal investigation or in the interests of the security of the State.[84] Authorisation is subject to stringent conditions including, in the case of criminal investigation, the seriousness of the offence and the likelihood of failure of other forms of investigation,[85] and in the case of national security, the likelihood of activities endangering the security of the State and of the failure of other methods of investigation.[86] Authorisations may only be given by the Minister for Justice[87] on an application in writing from either the Garda Commissioner or the Chief of Staff of the Defence Forces, as appropriate.[88] The legislation specifies information the warrant must contain,[89] and an authorisation only remains in force for 3 months, unless extended.[90] A judge of the High Court reviews the operation of the Act and considers, *inter alia*, whether its provisions are being complied with, and reports thereon at least once a year to the

---

82 See above ch. 6.
83 See above para. 2.4.
84 Section 2(1).
85 Sections 2(3) & 4.
86 Sections 2(3) & 5.
87 Section 2(1).
88 Section 6(1).
89 Section 2(4).
90 Section 2(5) & (6).

Taoiseach.[91] A copy of this report is laid before each House of the Oireachtas.[92] Failure to comply with the Act's requirements does not give rise to a cause of action.[93] Rather the Act provides for the creation of a special office, that of Complaints Referee, to consider complaints from persons about the interception of their communications.[94]

10.58 We think it desirable that video surveillance by the Gardaí and Defence Forces be subject to specific authorisation when it is directed at a particular individual or individuals or at particular premises. While it might be thought that the most appropriate person or body to grant such authorisation to the police for the investigation of crime is a judge or a court, we do not think that it would be appropriate to seek judicial authorisation for such surveillance where matters of national security are concerned. We are reinforced in this view by the fact that many European countries require judicial authorisation for the interception of communications for the purpose of criminal investigation, but not for national security.[95] We note however that the Government and the legislature have opted in the 1993 Act not to require judicial authorisation even in the case of criminal investigation; and if authorisation is to be required for video surveillance for either purpose, we think it desirable that the same rules and procedure should in general apply to the authorisation of such surveillance as to the interception of communications. *We* therefore *recommend that where the Gardaí wish to subject a particular person or persons or particular premises*[96] *to video surveillance, authorisation by the Minister for Justice upon written application by the Commissioner of the Garda Síochána should be required.*[97] *Similarly where the Defence Forces wish to conduct such surveillance in the interests of national security, authorisation by the Minister for Justice upon written application by the Chief of Staff of the Defence Forces should be required.*

10.59 The extent to which other public bodies in Ireland resort to video surveillance, e.g., in the investigation of suspected tax or social security fraud, is unknown. Such surveillance has given rise to concern in Australia and has prompted the Privacy Commissioner there to issue Guidelines for Commonwealth agencies with respect to the covert use of such surveillance.[98] These Guidelines

---

91 Section 8.

92 Section 8(7) & (8). Certain matters may be excluded from the report laid before the House of the Oireachtas.

93 Section 9(1). There is a saver for constitutional actions.

94 See s.9.

95 For example, in France, a law of 1991 provides for a special extra-judicial procedure in relation to the interception of telecommunications when the object of the interception is to obtain information relating to national security, to safeguard the essential elements of the economic and scientific potential of France, or the prevention of terrorism, organised crime or the regrouping or maintenance of bodies dissolved under a law of 1936 on combat groups and private armies. The law provides safeguards in respect of such interceptions and established a National Commission for the Control of Security Interceptions. The Commission is an independent administrative body which oversees the operation of the legislative provisions. See Arts. 3-19 of Law No. 91-646 of 10 July 1991 concerning the Secrecy of Correspondence by Means of Telecommunications, reproduced in the *First Report of the National Commission for Control of Security Interceptions*, Paris, 1993, at p.159. Article 2 of this Law deals with the judicial authorisation of the interception of telecommunications in the context of criminal investigation and amends the relevant provisions of the Code of Criminal Procedure.

96 It may be necessary to define premises broadly e.g. to allow surveillance of a vessel suspected of engaging in drug trafficking.

97 The British Royal Commission on Criminal Procedure also recommended that the use of surveillance devices by the police should be regulated by statute: see its *Report*, Cmnd 8092, 1981, para. 3.57.

98 See above paras. 10.8-10.12.

were drawn up in the context of specific legislation which deals with information privacy in Australia and which confers on the Commissioner powers in relation thereto. No such legislation or office exists in Ireland. The legislative context in which we are making proposals for law reform is quite different to that pertaining in Australia, and we are not aware of any particular problem in this regard in Ireland. In so far as an offence is suspected, we think it desirable that the relevant body seek the services of the police in the investigation, and in the event that resort is to be had to video surveillance, the conditions and procedures which we recommend above will then apply.[99] Otherwise these bodies and the staff thereof should be subject to the same criminal sanctions as private persons and bodies in respect of surveillance which is invasive of the integrity of the person.[100]

10.60 *Authorisation should be subject to the same conditions as apply mutatis mutandis to the interception of communications.* The conditions presently applying to the interception of communications include respect for individual privacy, and it is worth repeating here that, under our recommendations, one of the conditions for the authorisation of video surveillance by either the Gardaí or the Defence Forces would be:

> "that the importance of obtaining the information or evidence concerned is, having regard to all the circumstances and notwithstanding the importance of preserving individual privacy, sufficient to justify the surveillance."[101]

We would stress that the privacy to be preserved in this context is not merely that of the person who is to be subjected to surveillance but also that of any other person likely to be affected thereby.

10.61 *Authorisation should be by way of warrant, which should contain the same information, mutatis mutandis, as a warrant for the interception of communications.*[102] The warrant should therefore:

- bear the date on which the authorisation is given;
- state
  - (i) that the warrant relates to video surveillance, and
  - (ii) that the requirements of the legislation in relation to the giving

---

99 See above para. 10.49.

100 See above paras. 10.41-10.47.

101 Cf. ss.4(b) & 5(e) of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.* Canada subjects surveillance by the police to judicial authorisation, and the Canadian Criminal Code requires that terms and conditions protective of privacy be attached to any warrant authorising video surveillance. Section 487.01(4) of the Code provides:

> "A warrant ... that authorizes a peace officer to observe, by means of a television camera or other similar electronic device, any person who is engaged in activity in circumstances in which the person has a reasonable expectation of privacy shall contain such terms and conditions as the judge considers advisable to ensure that the privacy of the person or of any other person is respected as much as possible."

102 See s.2(4) of the 1993 Act.

of the authorisation have been complied with; and

- specify the person or persons to whom or the premises to which the surveillance relates.

In our view, there should also be some safeguards in respect of the disclosure to other persons of information and material obtained by means of the surveillance, and this may be achieved in part by the terms of the warrant. *A warrant should be addressed, as appropriate, to a named police officer or officer of the Defence Forces not below a certain rank.* This officer would normally be the person in overall charge of the criminal investigation or national security operation, as the case may be, and might be a superintendent in the case of the Gardaí and a commandant in the case of the Defence Forces.[103] It should be understood that this officer is responsible for the due execution of the warrant and, in particular, for ensuring that the surveillance is not excessive and that the information and material obtained thereby is disclosed only to persons directly involved in the investigation or security measures, or to other persons with a legitimate interest therein, such as the designated judge or Complaints Referee.[104]

10.62 *We* also *recommend that surveillance authorisation should be subject to a time-limit. This limit should be 3 months*, that is, the same as relates to the interception of communications, *but the Minister should be empowered to extend it on the same conditions as under the 1993 Act.*[105]

10.63 *We* further *recommend that the roles of both the designated judge and the Complaints Referee under the 1993 Act should be extended to cases of video surveillance by the Gardaí and the Defence Forces.*

10.64 The procedure and safeguards which we are recommending in respect of the authorisation of video surveillance by the Gardaí and Defence Forces are somewhat simpler than those now pertaining to the interception of communications. Whereas interception is for the most part actually carried out by staff of An Post in the case of postal packets and by staff of Bord Telecom Éireann in the case of telecommunications messages, authorised video surveillance would usually be carried out directly by the relevant force. In that only one body - the Gardaí or the Defence Forces - would be involved as compared to at least two in the case of the interception of communications, it should be easier to maintain control over photographs and film taken and information gleaned therefrom than when more than one body is involved. We have recommended that an officer in the relevant force be specified in the warrant as responsible for exercising this control, and think that at least initially it is not necessary to insert in the legislation provisions limiting disclosure to other specified persons. This should be dealt with operationally within each force, but *we think it desirable that internal guidelines be drawn up by each force*

---

103 Cf. s.8(a) of the *Data Protection Act, 1988.*

104 See below paras. 10.54-10.55.

105 See s.2(5) & (6).

in respect of the implementation of a warrant and the handling, disclosure etc. of material and information obtained thereby. In this connection, the Guidelines produced by the Australian Privacy Commissioner in relation to covert optical surveillance by Commonwealth agencies provide indicators of the matters which should be addressed in any such guidelines. It would be for the designated judge, in the course of reviewing the operation of this legislation, to assess both the adequacy of the guidelines and their actual application. In the event that serious deficiencies were to be found in this regard of other than a once-off kind, consideration might then be given to amending legislation to tighten the safeguards.

10.65 We would emphasise that our recommendations apply only to targeted surveillance, that is, surveillance of a specified person or persons who are suspected of engaging in serious criminal activity or in activity which is prejudicial to the security of the State or of premises suspected of being used for such activities. They do not apply to general video surveillance such as for the purpose of crowd control at a football match, street surveillance in the interests of preventing crime or general safety measures for a visiting foreign dignitary. No authorisation would be required for video surveillance in such cases. *The legislation should* therefore *specify that the requirement of authorisation applies only to the surveillance of a particular person or persons or of particular premises.*

10.66 Implementation of our recommendations would mean that no specific authorisation is needed for general video surveillance by the Gardaí or the Defence Forces, but that where this surveillance is conducted in a way which infringes the integrity of a person, the criminal liability which we propose above would attach to the persons engaging in such conduct. On the other hand, targeted surveillance of a particular person or persons or of particular premises would require ministerial authorisation, and if such surveillance is conducted in a way which infringes the integrity of a person, it would benefit from the defence of lawful authority in that there would exist legislation specifically permitting and regulating it.

10.67 Apart from the criminal offences, defences thereto and safeguards in respect of video surveillance by the Gardaí and members of the Defence Forces which we recommend above, we also think it desirable that some comparable provisions as those in Denmark, Norway and Sweden be enacted in Ireland with regard to the surveillance of public places. The law of these three countries requires that there be some notification to the public that such surveillance is taking place and penalises breach of the requirement. Notification enables members of the public to avoid the place which is under surveillance or to modify their behaviour while in such a place should they wish to conceal something from view. In the event that insufficient precautions are taken or it is not possible to shield something from view, the torts and criminal offences which we recommend above will afford a remedy in cases of privacy-invasive surveillance. *We* therefore *recommend that where a public place is subject to video surveillance, the person responsible for the surveillance should be under a legal obligation to display a notice to this effect at all access points.*

10.68 *The notice should be easily legible, and may be supplemented by further notices at other locations, but this should not be required.* It is important that the notice be placed at access points so that a person knows before entering the place that it is subject to surveillance. Bearing in mind criticism which has been levelled at the Norwegian legislation in this regard,[106] *we recommend that where an area comprises a number of distinct units, each unit should be considered a separate public place for the purpose of the notice requirement.* Thus it would not be sufficient for a local authority to post a sign at an exit from a dual carriageway indicating that the town centre is subject to surveillance. Rather a sign to this effect should be displayed at the entrance to each street and square which is in fact under observation. Similarly, it would not be sufficient to place a sign at the entrance to a shopping-centre stating that the centre is under surveillance. Rather each shop should display its own sign if it avails of this security measure. The term "a public place" is not a new term in the law. Legislative definitions already exist by way of precedent,[107] and *the definition of public place we favour for the purpose of the notice requirement is "any place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission."* Shops, banks, post offices, railway stations and airports would be covered by this definition. Private club premises and hospital wards would not generally come within the definition, but the entrance area of the club and of the hospital would, if the public generally have access thereto. Should an issue arise as to whether or not a place is a public place, the question would be one of fact.[108]

10.69 It would also be necessary to give in the legislation a definition of the type of visual surveillance to which the notice requirement would apply. The Danish legislation applies to video surveillance, but excludes non-recording equipment in some circumstances.[109] The Norwegian legislation also applies to video surveillance which is defined as 'constant surveillance of persons effected in a regular manner by means of television cameras functioning automatically, photographic devices or any other similar device.'[110] The Swedish legislation applies to remote-controlled cameras and other optical-electronic devices but excludes such devices if they are manually held or are used only temporarily.[111] *We* agree that the notice should only be required where there is a degree of permanency or constancy in the surveillance, and *recommend that the notice requirement should apply to constant or regular surveillance by means of an automatically-functioning optical device.* As above,[112] *optical device should be defined as a video camera or other similar electronic device.* The requirement would therefore apply to the surveillance of a public place irrespective of whether or not any recording on film was made of what was viewed.

---

106 See above n. 38.
107 See, e.g., s.3 of the *Road Traffic Act, 1961*; and s.18 of the *English Public Order Act 1986.*
108 See *Attorney General (McLoughlin) v. Rhatigan* (1983) 100 I.L.T.R. 37.
109 See above para. 10.14.
110 See above para. 10.22.
111 See above para. 10.26.
112 At para. 10.42.

10.70 *Failure to comply with the notice obligation should be an offence.* Furthermore, *liability in this regard should be strict.* Thus it should not be open to a defendant to plead, e.g., that she or he did not know or had no reason to believe that the place was a public place.

10.71 Exceptions to the notice requirement should be limited. A notice would not be needed for the surveillance of restricted security areas since the public do not have access thereto. Likewise in the case of the temporary use of surveillance equipment to identify troublemakers in a crowd or robbers in a bank raid of which the police have prior warning. There are however some circumstances in which covert constant or regular surveillance is justified in the public interest, notably by the police in the prevention and investigation of crime; and we note that the Norwegian legislation exempts covert video surveillance by the police provided certain conditions are observed,[113] and that the Swedish legislation allows the county administrative boards to dispense with the requirement of public notification if there is concern about public safety or about the safety of a visiting foreign dignitary.[114] *We* therefore *recommend that the notice requirement should not apply where specific authorisation has been granted to the Gardaí or the Defence Forces as recommended above.*[115] *Exemption should only apply for the duration of such authorisation, but should apply where such authorisation exists, irrespective of whether or not it has been validly given and of whether or not the conditions attaching thereto have been observed. Any question regarding the granting and implementation of the authorisation are properly dealt with by the review and complaints procedures we recommend, that is, by the designated judge and the Complaints Referee.*

113 See above para. 10.23.
114 See above para. 10.30.
115 See para. 10.49.

CHAPTER 11: AURAL SURVEILLANCE

Introduction

11.1 Two distinct bodies of law are applicable to aural surveillance in Ireland: that governing telecommunications and that governing wireless telegraphy. Aural surveillance is directly regulated by the former body of law, indirectly by the latter.

11.2 It is an offence under s.98(1) of the *Postal and Telecommunications Services Act, 1983* to intercept or attempt to intercept, or do anything that will enable oneself or another person to intercept, a telecommunications message being transmitted by Bord Telecom Éireann.[1] It is also an offence under the same provision to disclose the existence, substance or purport of any such message which has been intercepted as well as to use for any purpose any information obtained from any such message.[2] To intercept means to listen to or record by any means a telecommunications message in the course of its transmission.[3] There are a number of exceptions to criminal liability, e.g. to allow for regular maintenance work on a telephone line or the investigation of a criminal offence.[4]

11.3 The wireless telegraphy legislation is designed to regulate the use of the airwaves and deals with such matters as the allocation of frequencies and interference with the regular use of wireless telegraphy. The legislation only incidentally applies to aural surveillance in that a device used for the purpose of eavesdropping will usually fall within the legal definition of "apparatus for

---

1 See above para. 5.53. The limitation of these offences to messages being transmitted by Bord Telecom Éireann is considered below at para. 12.8.

2 See above para. 5.53.

3 *Ibid.*

4 See above paras. 5.55-5.60.

wireless telegraphy".[5] For example, it may be an offence to possess such a device without the required licence or improperly to disclose any message received by means of such a device.[6]

11.4 The two bodies of law may overlap in their application to the facts of a particular case of aural surveillance. For example, use of a radio scanner to intercept an Eircell[7] message may constitute an offence both under s.98(1) of the *Postal and Telecommunications Services Act, 1983* and under s.3(3) of the *Wireless Telegraphy Act, 1926*.[8]

11.5 At first glance it might appear that these two bodies of law, taken together, comprehensively regulate aural surveillance. However, the 1983 Act only applies to the interception of telecommunications messages being transmitted by Bord Telecom Éireann. It does not address the interception of a telecommunications message transmitted other than by BTÉ. Also, the interception of oral communications other than telecommunications messages, e.g. a direct conversation between individuals, is not regulated as such by the wireless telegraphy or any other legislation. Many other countries, including both civil law and common law jurisdictions, have offences relating to eavesdropping. The first question which we shall address in this Chapter therefore is whether a general statutory offence of eavesdropping should be created in Ireland and, if so, what exceptions there should be to it.

11.6 In dealing with this question we shall give special attention to the specific issue of participant monitoring. This monitoring takes two forms. One form is the recording of a conversation by someone party to it. The other is the recording or listening to a conversation by a third party who does so by agreement with one or more of the parties to the conversation. The original definition of "interception" in the *Postal and Telecommunications Services Act, 1983* permitted only limited participant monitoring. To fall outside the definition and hence outside the prohibition on the interception of telecommunications messages, monitoring had to be agreed to by both the person on whose behalf the message was transmitted and the intended recipient of the message.[9] This meant that one party who recorded a telephone conversation with another without that other's agreement to the recording was guilty of an offence under s.98(1) of the 1983 Act unless she or he fell within one of the four categories exempted from criminal liability.[10] This definition was altered by the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. The consent of either of the persons specified to the monitoring is now

---

5 See above para. 5.32 for the meaning of this term and, in general, above paras. 5.31-5.35 for the relevant wireless telegraphy legislation.

6 See above para. 5.31.

7 "Eircell" is the term assigned by Bord Telecom Éireann to the cellular radio telephone system or network for which provision is made under the Eircell Scheme 1985 whereby cellular radio telephone service is provided through the public switched telephone exchange system (the fixed telephone network) and a wireless telegraphy link provided by means of a cellular radio system or network: see S.I. No. 414 of 1985, para. 5.

8 As substituted by s.12(1)(a) of the *Broadcasting and Wireless Telegraphy Act, 1988*.

9 Section 98(5). See above para. 5.54.

10 Section 98(2). See above para. 5.55.

sufficient to exclude the monitoring from being regarded as an interception.[11] The phrasing of this exclusion suggests that it is directed at third party monitoring since where a person records a telecommunications message to which the person is party, it can hardly be required that the person gets his or her own consent to the recording in order to take it outside the prohibition on interception. Probably direct party monitoring is impliedly excluded from the prohibition because it would be anomalous to exclude recording with consent by a third party but not by a party to the telecommunications message itself. We shall consider both forms of participant monitoring in the broader context of aural surveillance in general.

11.7 Finally, we shall discuss regulation of the trade in aural devices as a means of controlling aural surveillance by private individuals. There is presently in force a ministerial order, made under s.7 of the *Wireless Telegraphy Act, 1972*, requiring a licence for the selling, letting on hire, manufacture or import of personal radio (citizen band) equipment.[12] It is an offence under s.10(2) of the 1972 Act to sell, let on hire, manufacture or import this equipment without a licence or to do so other than in compliance with the terms and conditions of any licence applying thereto.[13] Some other countries have also sought to control unauthorised surveillance by controlling the means whereby it is carried out, and we shall try to assess the effectiveness of such a method of control. We shall also examine the compatibility of such a control on imports with Ireland's obligations as a member of the European Union.

A Statutory Offence Of Eavesdropping?

11.8 We noted above that the common law offence of eavesdropping has not been expressly abolished in Ireland, but that it is doubtful whether it has been carried over into the law of the State due to lack of specificity.[14] We also remarked that, if it has been carried over, it affords only very limited protection to privacy interests in cases of surveillance.[15] Hence it is appropriate for us to consider whether a general statutory offence of eavesdropping is desirable in order to give greater protection to privacy from the threat of surveillance.

11.9 Several countries have made it an offence to eavesdrop. Some have a broad offence which applies to such conduct irrespective of what is eavesdropped or the means used. In others the offence is more narrowly framed by reference to what is overheard and/or the means used. Before giving our own view on whether some such offence should be created in Ireland, we shall briefly review the relevant legislation and proposals in a few of these countries, including both civil and common law jurisdictions, to illustrate the range of approaches which

---

11 See above para. 5.53.
12 See above para. 5.35.
13 *Ibid.*
14 See above para. 5.12.
15 *Ibid.*

have been adopted elsewhere.[16]

(i) The law in other jurisdictions

(a) Australia

11.10 Many Australian states regulate the use of listening devices. This legislation does not apply to the use of such devices to intercept telecommunications, this being governed by separate, Commonwealth legislation.[17]

11.11 Regulation is roughly the same in each state. It is an offence to use a device to listen into a private conversation. The latter term is defined in the Victorian *Listening Devices Act 1969* to mean:

> "... any conversation carried on in such circumstances as may reasonably indicate that the parties to such conversation desire it to be confined to such parties but does not include a conversation made in any circumstances in which the parties to the conversation ought reasonably to expect that the conversation may be overheard."[18]

11.12 Conversation, if protected, is protected irrespective of content. Similarly, if protected, it is protected wherever it occurs, that is, irrespective of whether it occurs in a private or in a public place. The context of the conversation determines whether it is protected or not. In general, a conversation addressed to another person or to a limited circle of persons is protected, but not if it is reasonable to expect that it would be overheard. It often would be reasonable to expect that a conversation held in a public place would be overheard, but not necessarily, e.g. where the speakers had purposely placed themselves beyond earshot.

11.13 There are a number of exceptions to the general prohibition on the use of a device to listen into a private conversation. No offence will be committed where consent has been given to the use of the device. The use of listening devices may also be authorised under warrant issued by a court to a police

---

16 See the *Report of the Committee on Privacy, 1972*, pp.319-326 and paras. 5.23-5.25 of *Calcutt I* for examples of such legislation other than those discussed below.

17 *Telecommunications (Interception) Act 1979*. On the state legislation in general see Australian Law Reform Commission, *Report No. 22 on Privacy*, paras. 736-742 & 1125.

18 Section 3. See also the New South Wales *Listening Devices Act 1969*, s.3(1); Queensland *Invasion of Privacy Act 1971*, s.4; South Australia *Listening Devices Act 1972*, s.3; and Western Australia *Listening Devices Act 1978*, s.3: and cf. the following definition of "private communication" in s.183 of the Canadian Criminal Code, as substituted by s.1(1) of the Act to amend the Criminal Code, the *Crown Liability and Proceedings Act* and the *Radiocommunication Act 1993*:

> "'private communication' means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it."

officer for purposes of nationality security[19] or the investigation of narcotic offences.[20] The relevant legislation provides safeguards in respect of an application for a warrant, surveillance carried out in pursuance of a warrant, and the use and disclosure of information lawfully obtained under warrant.

11.14 Where consent is given to the recording of a conversation, this may constitute evidence that the conversation is not "private", that is, that it was not intended that what was said should be confined to the parties. In general the consent of only one party to a conversation to a third party listening to or recording the conversation may be sufficient to take the conversation outside the protected category.[21] Also, the use of a listening device by a party to a conversation is permitted. South Australia has however what appears on the face of it to be somewhat more restrictive legislation. The *Listening Devices Act* of that state contains a broad prohibition on the use of listening devices to overhear or to record private conversations without the express or implied consent of the parties to the conversation.[22] Nevertheless no offence is committed where a party to a conversation records the conversation in the course of duty, in the public interest or for the protection of her or his lawful interests.[23] These broad exceptions mean that in most situations participant monitoring by a party to a conversation is lawful.

(b) France

11.15 From 1970 to 1994, it was an offence under Article 368 of the Penal Code for a person deliberately to invade the intimate, private life of another person by listening, recording or communicating by means of any device words spoken by that person in a private place, without the person's consent.[24] Article 368 is the same provision which penalised visual surveillance by means of a device and which we considered in that context in the last Chapter. As in the case of visual surveillance, consent was presumed when the listening, recording or communicating occurred at a meeting with the knowledge of all the participants. A person found guilty of any of these offences was subject to the same penalties, namely, a term of imprisonment or a fine, or both. These penalties applied also to anyone who knowingly kept, brought or deliberately let be brought to the knowledge of the public or of a third person, or used publicly or otherwise, any recording or document obtained in a manner contrary to

---

19 See, e.g., the Australian *Security Intelligence Organisation Act 1979*, s.26f.

20 See the *Customs Act 1901*, s.219B(1).

21 See s.3(3) of the New South Wales *Listening Devices Act 1969*; and s.42(2) of the Queensland *Invasion of Privacy Act 1971*.

22 Section 4.

23 Section 7(1).

24 The relevant part of Article 368 reads:

> "Sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2 000 à 60 000F, ou de l'une de ces deux peines seulement, quiconque aura volontairement porté atteinte à l'intimité de la vie privée d'autrui:
>
> 1^0 En écoutant, en registrant ou transmettant au moyen d'un appareil quelconque des paroles prononcées dans un lieu privé par une personne, sans le consentement de celle-ci."

Article 368.[25] Moreover, in case of conviction, a court could order the confiscation of any recording or document obtained by or as a result of the surveillance.[26]

11.16 The elements of the offences were the same as in the case of visual surveillance except for the means by which the other person's intimate private life was invaded.[27] Among these elements were the requirements that the other person be located in a private place and that the listening, recording or communicating constitute an attack on that person's intimate private life. As regards the former, a telephone available in the reception area of a hotel to both clients and staff was held by a court not to be situated in a private place, but a telephone booth was held to be a private place.[28] As regards the latter, the recording of a conversation in the context of negotiations about the publication of an article was held not to infringe intimate, private life.[29] In contrast, the general manager of a business and his son-in-law were held to have infringed the intimate private lives of employees when they listened in during lunch-time to the latter's conversations by means of an interphone installed in the canteen. The employees' conversations at the time concerned not only their working lives but also intimate personal matters.[30] An offence under Article 368 was committed by recording the words of a person in a private place even if what was recorded was indecipherable.[31]

11.17 Article 368 has been replaced by Article 226-1 of the New Penal Code which entered into force on 1 March 1994. Article 226-1 provides that it is an offence, by means of any conduct, deliberately to infringe the intimate, private life of another person, *inter alia*, by overhearing, recording or communicating words spoken privately or confidentially, without the consent of the other person. The offence of "listening" (*écoutant*) has been replaced with that of "overhearing" (*captant*); and, as in the case of visual surveillance, the offences need no longer be committed by means of a "device" (*appareil*) but simply by the "conduct" (*procédé*) of a person. Nor is it necessary that the words be spoken in a private place (*lieu privé*). It is sufficient if they are spoken privately or confidentially (*à titre privé ou confidentiel*). Also, as in the case of visual surveillance, presumed consent is no longer linked to the existence of a meeting. Consent will be presumed when the overhearing, recording or communicating occurs with the knowledge of all the persons concerned and without them objecting thereto when

25 Article 369. See also Arts.285 (proceedings against members of the press), 370 (montage) and 372 (attempt).
26 Article 372.
27 See above paras. 10.19-10.20.
28 Besançon, 5 January 1978, D.1978.357.
29 Paris, 26 March 1987, D.1987.IR.104.
30 Tribunal de grande instance, Saint-Étienne, 19 April 1977, D.1978.123.
31 Decision of the criminal division of the Court of Cassation, 19 May 1981, *Bulletin des arrêts de la Cour de cassation en matière criminelle* No. 161, D. 1981.544.

they were in a position to do so.[32] The penalties have been increased and apply also to the keeping, bringing or letting be brought to the knowledge of the public or of a third person, or using in any way whatsoever, of every recording and document obtained in a manner contrary to Article 226-1.[33] Attempt is subject to the same penalties.[34] The earlier case law on the interpretation of Articles 368 and 369 remain relevant in so far as the wording of these Articles has been carried over into the New Code.

(c) Germany

11.18 Paragraph 1 of Article 201 of the German Criminal Code provides:

> "Whoever, without authority,
>
> 1. records the non-publicly spoken word of another on a sound-recorder or
>
> 2. makes use of a recording which was so produced or makes it available to a third person
>
> is guilty of a criminal offence ..."

Also guilty of a criminal offence under paragraph 2 of the same Article is:

> "Whoever, without authority,
>
> 1. listens in with an eavesdropping device to the non-publicly spoken word of another which was not intended for his knowledge or
>
> 2. publicly communicates, whether verbatim or in its essential content, the non-publicly spoken word of another which was recorded

---

32 The relevant part of Article 226-1 reads:

> "Est puni d'un an d'emprisonnement et de 300 000F d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui:
>
> ...
>
> 2^{0} En captant enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel;
>
> Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils y soient opposés alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé."

33 Article 226-2, which reads:

> "Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.
>
> Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables."

34 Article 226-5.

according to paragraph 1(1) or listened to according to paragraph 2(1)."

Public communication is only an offence when it is "of a kind liable to infringe the legal interests of another. It is not illegal when it is made for the protection of overriding public interests."[35] Attempt is penalised under paragraph 4 of Article 201. Intention to do the prohibited acts is required. The offences are punishable with a term of penal servitude or a fine, the maximum term of imprisonment being higher where the convicted person is an office holder or someone engaged in the public service.[36] In case of conviction, any sound-recorder or eavesdropping device used in connection with the offence may be confiscated.[37]

11.19 These provisions aim to protect whatever is said other than in public in the interests of the free flow of oral communications between human beings. What is protected are spoken words which are not directed at the general public or not beyond a limited circle of persons. What is decisive is not the number of listeners but the limited nature of the audience and the possibility of control over the range of expression. Not merely the will of the speaker, but also the purpose and type of the dialogue is relevant. While intentional eavesdropping by others without the knowledge of the speaker will not take the words spoken outside the non-public sphere, a factual publication may result where persons unnoticed by the speaker overhear what is said. Any audible expression of thought is protected, irrespective of content. It may be spoken face-to-face, by telephone, by private radio or even be recorded on a sound-recorder.[38] An eavesdropping device is a technical device which makes the word audible beyond its natural field of sound. It includes built-in microphones, micro listening devices and telephone tapping equipment, but excludes amplifiers and headphones or earpieces.[39]

11.20 The offence under paragraph 2(2) is limited to cases where a legal interest of the speaker is infringed. This would exclude, e.g., the passing on of comments about the weather. A legal interest will be infringed not only where secrets are disclosed but also where the speaker is unwillingly placed in a public light. However, even when a legal interest of the speaker is infringed by a publication, no offence will be committed where there is an overriding public interest in publication. Of relevance in this regard may be the value of the information for the education of the public and the formation of public opinion.[40]

11.21 To commit an offence, a person must have acted without authority, that is, without legal permission or the consent of the speaker. Consent may be implied in certain circumstances, as where it is routine commercial practice to

---

35 Para. 2.
36 Para. 3.
37 Para. 5.
38 See, e.g., Karlsruhe, *Neue Juristische Wochenschrift* 1979, 1513.
39 See, e.g., decision of the Federal Supreme Court, *Neue Juristische Wochenschrift* 1982, 1398.
40 See, e.g., BGHZ 73, 124, affirmed by the Federal Constitutional Court, BVerfGE 66, 116.

record business calls.[41] Consent to a recording does not however necessarily constitute consent to disclosure of what is recorded to a third party or parties, and further consent may be required if such communication is to be lawful. Nor does consent to someone listening to a conversation necessarily constitute consent to that person recording the conversation. The monitoring of a conversation may therefore constitute an offence unless consent is expressly or impliedly given in the circumstances.

11.22 General grounds of legal justification apply to all offences, and these allow a weighing of the private interest of the speaker against other interests. The private recording of obscene or nuisance telephone conversations has been held to be justified as has recording a conversation to prevent the commission of a criminal offence.[42]

(d) United Kingdom

11.23 It is an offence under s.1(1) of the *Interception of Communications Act 1985* for a person intentionally to intercept a communication in the course of its transmission by means of a public telecommunication system. There are a number of exceptions to this offence, one being where a person "has reasonable grounds for believing that the person to whom, or the person by whom, the communication is sent has consented to the interception."[43] Participant monitoring by a third party is therefore permitted in the United Kingdom in the context of telecommunications. Otherwise aural surveillance is not specifically prohibited in the United Kingdom though, as in Ireland, there are extensive regulations governing wireless telegraphy.[44]

11.24 We noted above that the Younger Committee on Privacy recommended the creation of an offence of surreptitious surveillance which would apply to the use of both listening and optical devices.[45] Also, the later Committee on Privacy and Related Matters, being concerned about the threat to privacy posed by the use of surveillance devices, recommended the creation of new criminal offences to deal specifically with this problem.[46] In view of this comparable legislative vacuum in an adjoining common law jurisdiction, it may be worth recalling here what these recommendations were. As modified by Calcutt II, the proposed offences were:

(i) placing a surveillance device on private property without the consent of a lawful occupant, with intent to obtain personal information with a view to its publication;

---

41 For an example of this in Ireland see above para. 2.4.

42 See, e.g., BVerfGE 34, 247; BGHZ 27, 284; BGH 14, 385; Frankfurt Court of Appeal, *Neue Juristische Wochenschrift* 1979, 1172.

43 Section 1(2)(b).

44 See, for example, the *Wireless Telegraphy Acts 1949* and *1967*.

45 See above para. 10.37.

46 See above paras. 8.17-8.21, 8.24-8.25 and 10.38.

(ii) using a surveillance device (whether on private property or elsewhere) in relation to an individual who is on private property, without the consent of the individual to such use, with intent to obtain personal information about that individual with a view to its publication;

(iii) recording the voice of an individual who is on private property, without the individual's consent to the recording, with a view to its publication and with intent that the individual shall be identifiable.

These offences were furthermore to be reinforced by a new offence of trespass. The creation of an offence of publishing a recording or information obtained by means of a surveillance device was considered and rejected by both Calcutt I and Calcutt II.[47]

11.25 It was also recommended that it should be a defence to any of the new offences that the act was done:

(i) for the purpose of preventing, detecting or exposing the commission of any crime or other seriously anti-social conduct; or

(ii) for the purpose of preventing the public from being misled by some public statement or action of that individual; or

(iii) for the purpose of informing the public about matters directly affecting the discharge of any public function of the individual concerned; or

(iv) for the protection of public health or safety; or

(v) under any lawful authority.[48]

(ii) The Commission's view

11.26 We believe it desirable that some specific offence be created in Ireland to register society's disapproval of invasive snooping, to deter such conduct and to protect individuals' interest in privacy. The offence should not depend upon the means by which sound is communicated. It should apply whether words are spoken face to face or are carried over a distance by means of wireless telegraphy or a telecommunications system. Moreover, in our view, it should apply even to situations where the words are not directly communicated to another person. A person's voice may be recorded, e.g. on a telephone answering machine, and the recording may be illegitimately accessed by a person

47 See above para. 8.22.

48 See above paras. 8.21 and 8.25.

other than the intended recipient.

11.27 We do not however believe that all eavesdropping should be penalised. As in the case of visual surveillance, we think that the offence should catch only those cases in which eavesdropping has been rendered possible by sense-enhancing technology. It is technological developments which pose the greatest threat to privacy, and it is the use of devices to enable something to be heard which could not otherwise be overheard which should be targeted by the criminal law. In our view, if persons wish to keep what they are saying private, it is reasonable that they should take some precautions to place themselves beyond the earshot of others, and the law of several countries employs a criterion of a reasonable expectation of privacy in the circumstances.[49] It should also be borne in mind that, under our recommendations, an eavesdropper who e.g. listens at a closed door to what is being said inside a room will be civilly liable for such conduct.[50] *We* therefore *recommend that it should be an offence to infringe the privacy of another person by listening to or recording the voice of that person by means of an aural device, without the consent of the person or of some other person legally entitled to give consent on behalf of the person. Consent may be express or implied.*[51] We favour a phrasing of the offence by reference to a person's voice rather than a person's spoken words. Thus, as phrased by us, the offence would catch the use of a bugging device to listen to a nationalist humming a loyalist tune in the bath (or vice versa), this being information the disclosure of which could be highly embarrassing to the person concerned.[52]

11.28 For the purpose of this offence, *privacy should be defined to mean private life*. Interference with oral correspondence which does not constitute an infringement of a person's private life would still be protected in the telecommunications context by the offences of interception of telecommunications messages.[53] The merit of our recommendation is that it focuses on the interest to be protected, that of privacy, and makes it clear that this is the purpose of the proposed statutory offences. It would be for the courts to tease out the parameters of private life on a case-by-case basis, and, for the same reasons as we give above in relation to visual surveillance, we do not think that there should be any reference to location in the formulation of the offences.[54] In this connection we note that, under the New Penal Code of France, the offences relating to aural surveillance, in contrast to those dealing with visual surveillance, no longer make any reference to a private place but merely require that the words be spoken privately or confidentially. Nor do we think that what is overheard or recorded should be specifically limited to private or personal matters. The offence we recommend penalises particular methods of invasion of private life. Whether or not what has been infringed constitutes the private life

---

49 See, e.g., the provision of the Canadian Criminal Code quoted above at n.18.

50 See above para. 9.21ff.

51 See further below paras. 11.37-11.44 on participant monitoring.

52 It would also catch the unauthorised accessing of a telephone answering machine by means of an electronic device: see above para. 11.25.

53 See above para. 5.53.

54 See above para. 10.46.

of another person may depend upon such considerations as the location of the other person and/or the content of what was heard or recorded. The recording of a nationalist humming a loyalist tune in the bath would be an infringement of the nationalist's private life by virtue of the location of the humming. In contrast, such humming in a public place such as a street would not normally be regarded as pertaining to private life. Were however a number of persons to meet in a secluded part of a public park to discuss personal matters, eavesdropping on their conversation by means of an aural device might constitute an infringement of their private life.

11.29 It would also be necessary, for the purposes of this legislation, to define the meaning of aural device. Clearly it is desirable to exclude from any definition such devices as hearing aids which are designed to improve a person's hearing. On the other hand, we want to include all devices which enable a person to overhear something which they could not overhear by use of the normal human senses. *We* therefore *propose that aural device be defined as an electronic device which enables sound which would not otherwise be within the range of human hearing to be heard or recorded.*

11.30 As in the case of the offence we recommend in relation to visual surveillance,[55] we consider that some advertence to the infringement of the private life of another person should be required; and, for the same reasons we give in relation to visual surveillance, *we recommend that the offence of aural surveillance cover both the intentional and the reckless infringement of the private life of another person.*

11.31 *It should also be an offence to communicate the purport or substance of what was heard or recorded by means of an aural device in contravention of the privacy of a person to another person or persons or to the public without the consent of the person whose voice was heard or recorded or the consent of some other person legally entitled to give consent on behalf of that person.* Again, *consent may be express or implied*; but *it should be a defence that the person communicating the substance or purport of what was heard or recorded did not know and had no reason to believe that the voice had been heard or recorded in contravention of the privacy of a person. This offence should cover only the intentional communication of the purport or substance of what was heard or recorded but should apply where the hearing or recording constituted either an intentional or a reckless infringement of the privacy of the other person.*

11.32 In the vast majority of cases, the surveillance to which these offences will apply will be surreptitious or covert. We do not believe however that they should be limited to such surveillance. Although it will be rare that the offending surveillance is overt, there may be some cases in which overt aural surveillance would impact adversely on an individual's privacy and, if so, it should be penalised. An example would be where a long-range listening device is used

---

55 See above para. 10.45.

without any concealment, but the person overheard is either unaware of the device or of the capacity of the device to pick up what she or he says. We think it reasonable that persons should be expected to take precautions against being overheard by other persons who are within earshot if they want what they say to remain private. In our view, however, persons should not be expected to keep abreast of developments in technology so that they can realistically appraise the likelihood of being overheard by means of an aural device. The criterion of earshot, that is, the normal range of human hearing, by reference to which the offences we recommend have been phrased, seems to us to afford a workable and more certain yardstick for the courts to apply than one relating to developments in technology. Moreover, it is easily understood and gives a clear indication to persons generally as to when what they say will be protected by the criminal law and when not.

11.33 There are circumstances in which it is legitimate to infringe the privacy of another person by using a device to overhear or record what the person says, and provision will therefore have to be made in the legislation for exceptions. The clearest examples are perhaps privacy-invasive surveillance by the Gardaí and the Defence Forces in the interests of the prevention and investigation of crime and for the protection of national security. As in the case of the use of optical devices, we think that the law should explicitly recognise the competence of the Gardaí and the Defence Forces to engage in aural surveillance of a particular person or persons or premises for these purposes, and that any such surveillance should be authorised and regulated in the same way as the interception of telecommunications messages are at present. *We* therefore *recommend that the régime applying to the interception of communications under the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 be extended, mutatis mutandis, to the use of aural devices, as defined above, by the Gardaí and the Defence Forces.* For the reasons we give above in relation to video surveillance, we think that in general only the Gardaí and the Defence Forces should be empowered to resort to such surveillance for these purposes.[56] If some other public body, such as the Office of the Revenue Commissioners, wishes to procure evidence of e.g. tax evasion by recording a person's conversations, it should enlist the services of the Gardaí in this regard, in which case the conditions, procedures and safeguards we propose will apply. There should be no special exemption e.g. for a local authority which wishes to gain evidence of a fraudulent civil claim.[57] Should the authority wish to investigate the matter itself or employ the services of another, such as a private detective, for this purpose, both the authority and anyone acting on their instructions should be expected to respect the privacy of the person being investigated.

11.34 Also, as in relation to visual surveillance, *a warrant should be addressed, as appropriate, to a named police officer or officer of the Defence Forces not below*

---

56 See above para. 10.58.

57 See above paras. 3.21-3.22 for an example of the use by a local authority of the services of a private detective to get evidence of a suspected fraudulent personal injuries claim.

a certain rank who should be responsible for the due execution of the warrant;[58] and *we think it desirable that internal guidelines be drawn up by each force in respect of the implementation of a warrant and the handling, disclosure, etc. of material and information obtained thereunder.*

11.35 In addition to these exceptions for the Gardaí and the Defence Forces, we need to examine whether there are other situations in which aural surveillance that is invasive of a person's privacy should be permitted. The surveillance device installed in a bank for security purposes may not only take pictures but also record sound, and whereas the taking of the picture will not usually infringe the integrity of the person, the sound-recording of what a person said may well relate to the person's private life. Under our recommendations, the taking of the picture will not normally constitute an offence, but the sound recording may well do so unless it is specifically exempted from the criminal liability we propose above. We think that there should be a limited exception for such recordings since they may aid in the protection of persons and property and it is generally not possible to select in advance those comments which will fall into this category and those outside it. However there is a need to ensure that where personal information of no security value is recorded it is not retained or disclosed to others. *We* therefore *recommend that it should be a defence to the offences we propose for the defendant to show that she or he acted to protect her or his person or property or another person or persons and that the material or information obtained by the surveillance was used only for this purpose and that the material or information and any copy thereof was destroyed as soon as the reason for its retention ceased to exist. The burden of proving this defence would fall on the defendant, and should be discharged on the balance of probabilities.*

11.36 We have also considered whether it should be a defence that the person who engaged in the surveillance or communicated to another what was heard or recorded acted in order to prevent or to expose the commission of a crime. Such a defence would be wider than the exception we propose above for the Gardaí since, under the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*, authorisation to intercept may only be granted where the crime constitutes a statutorily-defined serious offence. To introduce a defence covering the commission of crime in general would, we believe, not afford sufficient protection to privacy. There may however be merit in allowing a general defence in relation to the prevention and detection of serious crime, while requiring that when the surveillance is conducted by the Gardaí, it be subject to specific authorisation, conditions and safeguards similar to those applying to the interception of communications. As in the case of surveillance by the Gardaí, there would need to be a statutory definition of serious crime so that it would be clear when it was legitimate to use an aural device in such a way as to infringe the privacy of another person and when not. Persons likely to engage in aural surveillance, such as members of the media and private detectives, could reasonably be expected to acquaint themselves with the types

58 See above para. 10.61.

of offence in respect of which the defence would be available. It should also be borne in mind that what we are addressing here is justification for the invasion of privacy. Under our recommendations, surveillance which does not constitute an infringement of the private life of another person would not be penalised. *The Commission is undecided at this stage on whether a general defence relating to the prevention or exposure of crime should apply to the proposed offences.*

(iii) Participant monitoring

11.37 We furthermore need to consider whether either of the two forms of participant monitoring, that is, the recording of a conversation by a party to it and listening to or recording a conversation by a third party with the consent of a party to the conversation, should be excluded from the offences we are proposing. Since the offence of unlawful aural surveillance which we are proposing requires lack of consent to the surveillance on the part of the person whose privacy is infringed thereby, what we are addressing here is whether there should be specific exceptions (i) for the recording of a conversation by a party to it without the consent of the other party or parties, and (ii) for the listening to or recording of a conversation by a third party with the consent of a party to the conversation but without the consent of the other party or parties.

11.38 Our brief review of the law and proposals in other countries shows that it is not unusual for specific provision to be made for participant monitoring but that the countries surveyed differ in respect of what is permitted. In general, the Australian legislation permits the use of a listening device by a party to a conversation and the recording or listening to a conversation by a third party if one or more of the participants consent thereto. Participant monitoring is only regulated in the United Kingdom in the context of the interception of telecommunications and only where a third party is concerned. Explicit consent is not required. The existence of reasonable grounds for belief in consent is sufficient. In contrast, the New French Penal Code seems to require consent if a party to a conversation wishes to record the conversation and only presumes consent when the monitoring, whether carried out directly by a participant or by a third party, occurs with the knowledge of all the participants and without them objecting thereto when they are in a position to do so. Consent is also required in Germany, but may be implied in the circumstances. Consent to someone listening to a conversation does not however necessarily imply consent to the recording of the conversation.

11.39 The Australian Law Reform Commission was divided on the issue of the regulation of participant monitoring, at first adopting the view that monitoring should not be permitted but the majority ultimately recommending that participant monitoring be allowed, that is, that a person be entitled to record a conversation to which the person is party without the knowledge or consent of any other party and that a third party be entitled to listen to and record a conversation if at least one of the parties to the conversation agrees to this. This appears to be the present position under Irish law with respect to telecommunications messages.

11.40 The arguments for and against a prohibition on monitoring were detailed as follows by the Australian Commission:

> "*Arguments for Regulating Participant Monitoring*
> Participant monitoring allows what could have been relayed to outsiders selectively, after the fact and supported only by the word of one party, to be disseminated in its entirety, accurately, often simultaneously and supported by independent evidence. It is said that, unless it is regulated, it could lead to honesty and frankness in discussion being compromised, and discussion itself becoming cautious and bland, losing its intimate, personal and informal character. Freedom and frankness of speech are much prized in our community. It would clearly be undesirable if these qualities were to be lost. Another argument in favour of regulating participant monitoring asserts that it represents a distinctive kind of threat to privacy. The party to the conversation who secretly makes a recording can present matters in a way that is entirely favourable to his position because he controls the situation. He knows that he is recording it. The opportunity for other parties to dispute what was actually said or add to it, qualify it or attempt to put it into context is lessened.
>
> *Arguments against Regulating Participant Monitoring*
> *Current Practice*. Participant monitoring is an accepted practice in many parts of the private sector. It is used by many people to protect their interests, particularly in commercial, business and domestic contexts. Many of the submissions that the Commission received in the course of its inquiry indicated that a requirement to give explicit warnings that conversations were being recorded would have a deleterious effect on many standard arrangements and common usages. In fact, many would see a prohibition on the use of listening and recording devices for participant monitoring as a failure to recognise and reflect contemporary practices and standards. Just as a party is free to construct a permanent record from notes or recollection, albeit imperfect, he should not be legally prevented from recording them as accurately as technology will allow.
>
> *State Legislative Approaches*. In all States in which legislation exists to regulate the use of listening devices, participant monitoring, in one form or another, is allowed. There is no regulation, by Territorial or Tasmanian law, of the use of listening devices. Participant monitoring is therefore permitted. It is expressly permitted under the New South Wales and Queensland law, and permitted, although not expressly, under Western Australia and Victoria law. Only in South Australia is there any restriction on participant monitoring. Even there, the restriction is expressed vaguely and is in terms quite wide enough to permit a party to most conversations to record them without the knowledge of other parties. No evidence that any of the harmful social effects that critics of participant monitoring suggest have occurred was presented to the

Commission throughout the six years of its inquiry. Indeed, so far as these things can be assessed, personal conversations still seem as full of 'exaggeration, obscenity, agreeable falsehoods and ... expressions of anti-social desires [and] views not intended to be taken seriously' as ever they were. Lack of regulation has not produced the chilling effects that some fear.

Damages of Regulating Participant Monitoring. There are a number of dangers with proposals that participant monitoring, generally, be prohibited. Tape recording of sounds and conversations is now a common practice in purely domestic and friendly circumstances. Tape recordings can be taken of family events, without some there being aware that it is happening. It can be done at parties for fun. This conduct should not bear the full weight of the criminal law. Accidental recording without the consent of some parties might also occur. The innocent recorder of social events might be placed at a risk completely disproportionate to the undesirability of what he may have done.

Fundamental Problem Unresolved. A person speaking to another does so at his own risk. Whatever he says can be recalled, correctly or incorrectly, by the other parties to the conversation and can be reported, correctly or incorrectly, as they see fit. A person speaking to another must take the risk, ordinarily inherent in so doing, that his hearer will make public what he has heard. There are many ways of recording conversations. Notes written immediately the conversation has finished is one way. Shorthand notes, or longhand notes, taken during the conversation are others. A listening device simply replaces other techniques of recording that the party to the conversation might use. The fundamental difficulty - the fact that the conversation can be recorded or recalled in circumstances and for purposes outside one party's control - still remains. To regulate the use of some forms of recording does not remove that difficulty."[59]

11.41 We appreciate that there may be legitimate reasons for participant monitoring, and believe that the formulation of the offences we propose will in fact allow participant monitoring in many of the situations given by the Australian Law Reform Commission as examples of when it should be permitted. Under our proposals, consent to recording whether by a party to a conversation or a third party and to third party listening may be implied, and this will often be the case on family occasions and at parties and other social events. Moreover, our proposed definition of an aural device would exclude, e.g., the use of a tape-recorder which was only capable of recording sounds within earshot. Any routine practice of recording business calls would also be excluded from the offences we propose both because consent would be implied if such recording was normal and because there would be no infringement of another person's

---

59 *Report No. 22 on Privacy*, paras. 1128-1132 (paragraph numbers and footnotes omitted).

private life. Furthermore, the defence we propose in relation to the protection of person and property would also allow for recording without consent within limits where these interests were threatened, as would a defence relating to the prevention or detection of serious crime. The question for us therefore is whether, given the particular formulation of the offences we propose, there should be a specific exception to allow for a greater degree of participant monitoring or, on the contrary, to prohibit it where it would not fall within the offences proposed.

11.42 We are concerned about the possibility of abuse of monitoring and think it desirable that there exist legal safeguards in respect of any such abuse. *We welcome submissions on whether the recording of a conversation by a party to the conversation should be permitted even without the knowledge or consent of the other party or parties. Furthermore, we welcome submissions on whether disclosure of the substance or purport of the recorded conversation should not be an offence anymore than it would be if the disclosure was based on memory or notes rather than a recording.* If information is passed in confidence during a conversation by one person to another person or persons, then, if an obligation of confidence attaches in the circumstances, the law on breach of confidence will afford some protection against unauthorised disclosure.[60]

11.43 However, we think that the situation is different where monitoring occurs by a third party on behalf of the State. State surveillance in the context of the interception of communications is already subject to extensive legal regulation. Yet by using the services of a private individual such as an informer who is party to a telephone conversation with a suspect, the police may avoid the system of warrants and attendant safeguards under the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.* In our view, this is undesirable. Participant monitoring on behalf of or in co-operation with State authority, whether it be of telecommunications or oral communications generally, should be legally regulated. The principle of legal regulation of state surveillance, including restriction of the competence to engage in surveillance to certain branches of the administration and safeguards for individuals subjected to surveillance, has already been accepted by the Government and the Oireachtas, and indeed is required by the State's international obligations. *We* therefore *recommend that where surveillance involving the use of an aural device*[61] *is carried out on behalf of or in co-operation with the Gardaí or the Defence Forces, the warrant procedure and safeguards described above should apply in respect of such surveillance.*[62] This means, for example, that the use by the

---

60 See above paras. 4.33.-4.62.

61 As defined above at para. 11.29. The same requirement should apply to surveillance involving the use of an optical device as defined above at para. 10.44.

62 We mention only the police and the Defence Forces here since there are the only public authorities which we recommend should have special powers of aural or visual surveillance. Should other authorities be given such powers, surveillance carried out on behalf of or in co-operation with them should likewise be subject to the warrant procedure and safeguards. It should be noted that the European Court of Human Rights held in a recent case involving the clandestine recording of a telephone conversation by a private individual with the assistance of a high-ranking police officer that (i) the state was responsible for the recording, and (ii) in any event, the person unwittingly recorded was entitled to the protection of domestic law in respect of such recording: see above para. 7.24.

Gardaí of the services of an informer to record a conversation with a suspect would only be permitted in the circumstances presently laid down in the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act* and, if authorised, would be subject to the same conditions and restrictions as apply under this Act to the interception of communications. Where an individual threatened with, e.g., blackmail surreptitiously records a conversation with the blackmailer, this would not constitute an offence since it would fall within our proposed exceptions in respect of participant monitoring. However, if that individual took the recording to the Gardaí in order to get the Gardaí to take action against the blackmailer, any further recording by the individual of such conversations if done in co-operation with the Gardaí would require authorisation by warrant.

11.44 We have found it more difficult to decide whether there should be a blanket exception for third party monitoring where the third party is a private individual acting either on his or her own behalf or on behalf of another private individual who is party to the conversation, or whether the exception we propose above should apply only to direct monitoring by the party to the conversation. Such monitoring will be carried out on behalf of or in co-operation with a party to the conversation. *We welcome submissions on whether, in the case of participant monitoring, it should be an additional defence to the offence of communication that the communication was made to a person or persons on whose behalf or in co-operation with whom the listening or recording was carried out.*[63] This would mean that communication to other persons without the consent of all parties to the conversation would be an offence unless any of the general exceptions to liability applied.

Regulation Of The Trade In Aural Devices[64]

11.45 One of the methods adopted by some states to control surveillance is to control the devices used for surveillance. A variety of strategies are used. One is to control inter-state trade in the devices by restricting or even prohibiting the importation of certain devices. Another is to control the outlets within the state from which devices may be obtained, e.g., by requiring a licence for their sale. Yet another is to control the manufacture of devices within the state, e.g. by making their manufacture subject to a permit or licence.

11.46 There is limited Irish legislation in the field of wireless telegraphy which seeks to employ all these strategies but with the aim of controlling interference with wireless telegraphy rather than the use of wireless telegraphy apparatus for the purpose of surveillance.[65] Section 7 of the *Wireless Telegraphy Act, 1972* empowers the Minister for Transport, Energy and Communications by order to specify apparatus of any class or description which may not be sold, let on hire,

---

63 See above para. 11.31 on this offence.

64 What we say below in relation to regulation of the trade in aural devices also applies *mutatis mutandis* to regulation of the trade in visual devices.

65 See above para. 5.35.

manufactured or imported without a licence when it appears expedient to the Minister for the purpose of preventing or reducing the risk of interference with wireless telegraphy or for such other purpose as the Minister shall specify. An order was made in 1981 applying to personal radio equipment and was simply stated to be made for the purpose of preventing or reducing the risk of interference with wireless telegraphy.

11.47 Comparable powers exist in the United Kingdom under s.7 of the *Wireless Telegraphy Act, 1967* in that jurisdiction. There are however interesting differences between the British and the Irish legislation. Under the British Act, orders apply only to the manufacture and importation of apparatus and no order shall be made or terms or conditions attached to the granting of authority for manufacture or importation "unless the Board of Trade are satisfied that the order, authority, term or condition in question is compatible with the international obligations of the United Kingdom."[66]

11.48 More extensive provision exists in French law for the control of trade in surveillance devices, backed up by criminal sanctions. Under Article 371 of the former Penal Code, provision was made for a list of devices to be drawn up in accordance with conditions laid down by decree after consultation with the Conseil d'État. These devices were those intended to pick up conversations at a distance and which would allow the commission of an offence contrary, *inter alia*, to Article 368 of the Code.[67] The manufacture, importation, possession, display, offering, rental or sale of devices on the list was subject to ministerial authorisation, the granting of which was also to be subject to conditions laid down in the same decree. Manufacture etc. without such authorisation or not in compliance with any conditions attaching to authorisation was an offence punishable with a term of imprisonment and/or a fine. In case of conviction for an offence involving lack of authorisation, the court was to order the confiscation of the devices concerned.[68]

---

66 Section 7(4).

67 Article 371 reads:

> "Une liste des appareils conçus pour réaliser les operations pouvant constituer l'infraction prévue à l'article 186-1 et des appareils qui, conçus pour la détection à distance des conversations, permettant la réalisation de l'infraction prévue à l'article 368, sera établie dans les conditions fixées par décret en Conseil d'État.
>
> Les appareils figurant sur la liste ne pourront être fabriqués, importés, détenus, exposés, offerts, loués ou vendus qu' en vertu d'une autorisation ministerielle dont les conditions d'octroi seront fixées par le même décret.
>
> Est interdite toute publicité en faveur d'un appareil susceptible de permettre la réalisation des infractions prévues, selon le cas, aux articles 186-1 ou 368, lorsqu'elle constitue une incitation à commettre ces infractions.
>
> Sera puni des peines prévues, selon le cas, aux articles 186-1 ou 368 quiconque aura contrevenu aux dispositions des alinéas précédents."

See above para. 11.15 concerning Article 368. Article 186-1 deals with the unlawful interception, diversion, use or disclosure of telecommunications by a public official or an employee of a supplier of telecommunications services.

68 Article 372.

11.49 On 25 March 1993, a decree was issued pertaining to the list of devices.[69] It provides that the list should be drawn up by order of the minister in charge of telecommunications after consultation with a special commission.[70] An application for authorisation for manufacture etc. of these devices must be made to this minister and the decree specifies information which must be given in the application.[71] The maximum duration of any authorisation in six years and conditions may be attached to an authorisation.[72] Moreover, the acquisition or possession of a device featuring on a list also requires ministerial authorisation.[73] The maximum duration of such authorisation is three years and use of the devices may be subject to conditions designed to avoid abuse of their use.[74] Authorisation may be withdrawn on specified grounds.[75]

11.50 Provisions similar to Article 371 on the regulation of trade in aural devices have been retained in the New Penal Code.[76] However, as of 1 January 1995, no list of devices has been drawn up. It is also an offence to advertise a device (*réaliser une publicité en faveur d'un appareil*) capable of enabling the commission of an offence of unlawful surveillance, when the advertising constitutes incitement to commit the offence.[77]

11.51 Control of trade by means of a list of devices can be problematic. One problem is that unless the devices are described in broad terms, the list will always lag behind developments in technology. Another is that many devices may be used for lawful purposes and reference, as in the French legislation, to devices intended to carry out operations which may constitute an offence or permit the commission of an offence may lead to uncertainty as to whether or not a device can validly be included on the list. Moreover, a device may be put together from several component parts each of which has some perfectly legitimate use, which use would not, on its own, call for regulation. Assembly may occur post-manufacture, post- importation and even post-sale. The parts may even be sold separately, it being understood that a purchaser will most likely subsequently assemble them for use as a surveillance device. The French provisions would seem to try to catch post purchase assembly in that they cover possession (*détention*) as well as manufacture etc. However, avoidance of such control would not appear to be all that difficult, and the effectiveness of such a strategy seems to us to be doubtful. We therefore do not recommend the introduction of any such system in respect of aural devices in general in Ireland. Nor do we think that control by means of licensing for manufacture etc. should be extended beyond the present régime pertaining to certain types of apparatus for wireless telegraphy. For the same reasons as given above, the efficacy of a general licence requirement for the manufacture etc. of aural devices would be open to doubt.

---

69 This decree is reproduced at Appendix F.
70 Article 2 of the decree.
71 Articles 3 and 4.
72 Article 5.
73 Articles 7 and 8.
74 Article 9.
75 Article 11.
76 Articles 226-3.
77 *Ibid.* See also Articles 186-1 of the earlier Penal Code.

It would also place an additional administrative burden on the State which is unlikely to be justified in terms of restricting the unlawful use of surveillance devices.[78]

11.52 With specific regard to controlling the importation of aural devices, it should be recalled that restrictions on the importation of goods from other European Union states have to be justified under EU law. The free movement of goods between member states is a fundamental principle of the Union and, in particular, any restriction on the importation of goods which are freely available in another member state or states is subject to stringent conditions not only as to the reason for the restriction but also as to the proportionality of the measure and any possible discrimination.[79] Moreover, Articles 30 to 34 of the EC Treaty have been interpreted by the European Court of Justice as prohibiting the imposition of a requirement for an import licence for intra-community trade.[80] These are further reasons why we do not favour control on the importation of aural devices.

---

78 See the *Report of the Committee on Privacy*, 1972, paras. 532-535 and Appendix P, for further examples of the control of trade in surveillance devices. This Committee thought that a system of control by licensing would be unworkable in Britain (see paras. 567-570 of the *Report*) and concluded that:

> "licensing can be a useful control for some limited purposes, but the difficulty of defining the devices to be controlled, the variety of legitimate uses and their large numbers have convinced us that in this area licensing would be unduly cumbersome and probably ineffective" (para. 570).

79 See case 120/78, *Rewe-Zentral AG v. Bundesmonopolverwaltung für Branntwein* [1979] E.C.R. 649; and, in general, D. Wyatt and A. Dashwood, *European Community Law*, 3rd ed., ch. 8, and S. Weatherill and P. Beaumont, *EC Law*, chs. 15-17.

80 See Cases 51-54/71, *International Fruit Company NV and Others v. Produktschap voor Groenten en Fruit* [1971] E.C.R. 1107; Case 41/76, *Criel, née Donckerwolcke and Shou v. Procureur de la République au Tribunal de Grande Instance, Lille and Director General of Customs* [1976] E.C.R. 1921; Case 68/76, *Commission v. French Republic* [1977] E.C.R. 515; and Case 124/81, *Commission v. United Kingdom* [1983] E.C.R. 203.

CHAPTER 12: THE INTERCEPTION OF COMMUNICATIONS

Introduction

12.1 With limited exceptions, the interception of postal packets or telecommunications messages is an offence, as is the disclosure or other use of information obtained by means of or as a result of interception.[1] We accept that such conduct should in principle be penalised. Persons are entitled to expect that their post and their telecommunications enjoy a high degree of security, and that in general what is sent by either route will only be seen or heard by the intended recipient. If persons could not rely on the secrecy of these services, communication would be hedged by caution and frankness and personal relationships would suffer. Protection by the civil law alone would probably not be sufficient to secure the desired degree of secrecy. The deterrent effect and moral condemnation of the criminal law are needed in this area.

12.2 The exceptions to criminal liability are essentially the same in relation to each form of communication, with one additional exception applying to the interception and disclosure of telecommunications messages. The additional exception relates to an investigation by the police of complaints of harassing or obscene telephone calls.[2] At first glance, it might seem anomalous that the interception of a person's telecommunications by or on behalf of the police is otherwise subject to specific authorisation by ministerial warrant and to legal safeguards whereas all that is needed under this exception is suspicion of one of the specified offences grounded in a complaint from a person claiming to have received such a call. However interception in such cases will usually occur with the agreement of the recipient of the call, and can be regarded as protective of privacy rather than invasive of it. It should nevertheless be borne in mind that the same telephone line often serves more than one person, e.g. members of a

---

1 See ss.84(1) & 98(1) of the *Postal and Telecommunications Services Act, 1983.*

2 See above paras. 5.55 & 5.56.

family living in the same building, and there is no specific legal check against malicious or ill-based complaints. While it may be assumed that the Gardaí do not automatically proceed to interception on every complaint, we think it desirable that this exception be tightened somewhat. Accordingly, *we recommend that section 98(2) of the Postal and Telecommunications Services Act, 1983 should be amended to require that the interception be authorised by a member of the Garda Síochána not below the rank of superintendent.*[3] The conditions and procedures to be complied with before interception may be initiated are a matter for internal garda management.

12.3 The other exceptions apply to the interception both of postal packets and telecommunications messages and to the disclosure of their contents. First, there are exceptions relating to the provision of the relevant service.[4] For example, An Post may open a postal packet which is undeliverable or which has not been collected[5]; and a telecommunications message may be intercepted in connection with the installation and maintenance of a telephone line or handset.[6] These exceptions seem to us to be reasonable especially as the latter is further qualified by the condition that the interception or disclosure must occur in the course of and only to the extent required by the person's operating duties. Secondly, in both cases, interception or disclosure is permitted when a person is acting under lawful authority.[7] Again, provided such authority is clearly laid down by statute or case law, we see no objection to these exceptions. Lastly, interception is permitted in both cases where a person is acting in pursuance of a direction issued by the Minister for Justice under section 110 of the *Postal and Telecommunications Services Act, 1983*. Such directions may be issued to An Post to intercept postal packets and to Bord Telecom Éireann to intercept telecommunications messages in connection with the investigation of serious crime and in the interests of the security of the State. Since 1993, these interceptions have been subject, under the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act*, to specific ministerial authorisation and stringent conditions.[8]

12.4 It would not be appropriate for us thoroughly to examine in this Paper the régime established by the 1993 Act. It would be particularly inappropriate for us to reopen fundamental issues of policy which have only recently been decided and to give our own preferred decisions thereon. For example, it is not uncommon in both civil and common law countries for the interception of communications by the police in the investigation of crime to be subject to court authorisation and control, whereas national security interceptions are subject to extrajudicial forms of control. In contrast, a common scheme is applied under the Irish legislation to interceptions for both purposes and control over both types of interception has been entrusted to persons and bodies other than the

---

3 Cf. s.8(a) of the *Data Protection Act, 1988*.
4 See paras. 5.39 & 5.55 above.
5 See above para. 5.40.
6 See above para. 5.59.
7 See above paras. 5.42 & 5.58.
8 See ch. 6.

courts. A judicial element has been incorporated into the forms of review of compliance with the scheme laid down in the Act by the appointment of a designated judge to monitor the operation of the Act in general and of a Complaints Referee to consider allegations of interception. These forms of review have only been in operation for a very short time, and an assessment of their effectiveness would be premature. It is for these persons in the first instance, particularly the designated judge, to evaluate the legislative scheme and to make proposals for its reform, if and as necessary.

12.5 We do however think it appropriate that we give our views on some matters pertaining to both the scope and the content of this legislation in the general context of our study of the threat posed to privacy by surveillance. We have already recommended that the scheme be extended so as to cover not only the interception of postal packets and telecommunications messages but also the use of aural and optical devices for the purpose of surveillance.[9] With specific regard to participant monitoring, we have also recommended in considering aural devices that there should be some further limitation on the disclosure of information obtained by third party monitoring.[10] We are of the view that the same principles should apply to the participant monitoring of telecommunications as to such monitoring of aural communications in general. Accordingly, *we recommend that the Postal and Telecommunications Services Act, 1983 be amended to prohibit disclosure of the substance or purport of information obtained by third party monitoring, by the third party, to a person or persons other than the party or parties on whose behalf or in co-operation with whom the monitoring was carried out, without the consent of that party or those parties.* We have also noted that, whereas the provisions of the 1983 Act apply only to telecommunications messages in the course of transmission, there is no such explicit limitation with regard to postal packets. We should therefore consider this limitation on the protection of telecommunications messages in comparison to the breadth of that afforded postal packets. We have further noted that the protection relates only to telecommunications messages transmitted by Bord Telecom Éireann and to postal packets conveyed by An Post. In this era of the deregulation of both services, we should look at whether these limitations are outdated and whether the scope of the protection should be increased to take account of market developments. In addition, what is protected under the 1983 Act are postal packets and telecommunications messages, and we have seen that there is some lack of clarity as to the precise meaning of each of these expressions. We shall therefore also say something about the definition of these terms.

12.6 Technological as well as economic developments have had a significant impact in recent years on the field of communications. A product of both developments has been an explosion in the use of electronic mail. Such mail is increasingly used for a variety of purposes, including marketing and business purposes as well as the communication of all types of information. We shall try to assess the adequacy of existing legal safeguards for the protection of such mail

---

9 See above paras. 10.49 & 11.32.
10 See above para. 11.41.

from interception and to determine whether additional safeguards are desirable in respect of the communication of information by this means, bearing in mind that our concern in this Paper is primarily to protect privacy and not other interests.

12.7 Lastly, technological developments also mean that various forms of encryption are now available as a means of protecting the secrecy of electronic communications, and we shall briefly consider whether a legal obligation should be placed on a communications carrier either to offer an encryption service to its customers or itself to use such a method of protecting the secrecy of communications carried by it.

Deregulation Of Postal And Telecommunications Services

12.8 We have seen that the offence of unlawful interception of postal packets and related postal offences under section 84 of the *Postal and Telecommunications Services Act, 1983* are of a general kind and do not depend upon conveyance of the postal packet by An Post.[11] Given the increasing deregulation of the postal services and the proliferation of private carriers, it is most important that these offences continue to be of a general kind and are not limited to transmission by any particular carrier or carriers. In contrast, the offence of unlawful interception of telecommunications messages and related offences under section 98 of the same Act apply only to messages transmitted by Bord Telecom Éireann.[12] Clearly this limitation to a particular carrier is outdated in view of the worldwide deregulation of telecommunications services. *We* therefore *recommend that section 98 should be amended to cover transmission by means of any public telecommunications system.*[13]

12.9 We note that statutory provision already exists under the 1983 Act for directions under section 110 to be issued, and hence the scheme applicable to police and national security interceptions under the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* to be extended, to carriers other than An Post and Bord Telecom Éireann. The Minister for Transport, Energy and Communications may, subject to certain conditions and with the consent of the Minister for Finance, by order provide for the grant of a licence to any person to provide a postal service or a telecommunications service of a class or description specified in the order to which an exclusive privilege granted to either An Post or Bord Telecom Éireann under the Act relates.[14] Terms and conditions may be attached to a licence[15]; and where such a licence is granted to perform any function:

> "... every provision of [the] Act and or any other enactment relating to [An Post or Bord Telecom Éireann, as appropriate] which is specified

---

11 See above para. 5.43.
12 See above para. 5.53.
13 For our recommended definition of this term see below para. 12.19.
14 Section 111(1)(a).
15 *Ibid.*

in regulations made by the Minister under this section shall in respect of that function and subject to such conditions, limitations or modifications as may be prescribed in such regulations, apply to the licensee as it applies to [An Post or Bord Telecom Éireann]."[16]

While consideration of licensing as such is outside the scope of this Paper, we think it important that the scheme under the 1993 Act apply to the interception of post and telecommunications conveyed by all carriers offering a postal or telecommunications service to the public, and we note that many postal carriers seem at present to be operating without a licence, in breach of the exclusive privilege conferred by the 1983 Act on An Post. In view of market developments, the days of monopolies and exclusive privileges are by and large over, and new legislation relating to the provision of postal and telecommunications services will be required to reflect these developments. Meanwhile, *we recommend that existing licensing powers be used by the Minister for Transport, Energy and Communications to ensure that all postal and telecommunications carriers who offer their services to the public and for which services a licence is required are brought within the scheme of the 1993 Act; and that regulations be made under section 111(5) of the Postal and Telecommunications Services Act, 1983 for this purpose. Legislative provision should also be made for the extension of the scheme to postal carriers offering a service to the public for which a licence is not presently required.*[17]

Definitions

(i) The meaning of postal packet

12.10 Because of the ongoing deregulation of the postal services, it is important that any definition of the expression "postal packet" not be phrased by reference solely to An Post. We have seen that the present definition is not so restricted but that there is some uncertainty as to the physical objects falling within the scope of the expression.[18] It is desirable that any definition take account of developments in modern technology, such as the transmission of postal electronic mail.[19] The objective is to protect against illegitimate interception all communications by post, and it is undesirable that this protection hinge on whether or not a particular item is a "post card", "book packet" or other sub-category of "postal packet". Some awareness of the difficulties inherent in an itemised definition seems already to have existed in 1908 since the Post Office Act of that year provided that, if there was any question as to whether an item fell into a particular sub-category or not, the Postmaster-General was to decide the question.[20] In this regard we also note the evidential provisions introduced by the *Postal and Telecommunications Services Act, 1983*, which state that evidence that an article is in the course of transmission by post or has been

---

16 Section 111(5).
17 See above para. 2.28.
18 See above paras. 5.45-5.52.
19 See above para. 2.19 on this form of mail.
20 Section 19. See above para. 5.47.

accepted for transmission by post shall be sufficient evidence that the article is a postal packet.[21]

12.11 We are concerned here only with the definition of the expression "postal packet" in relation to the protection of such packets from unauthorised interception, and we believe that the simpler and more embracing a term for this purpose the better. One solution which would meet these criteria would be to replace the expression "postal packet" with that of "postal communication". The latter term would divorce protection from the existence of a physical object, such as is suggested by the word "packet", and would include new forms of communication, such as the transmission of computerised data by a postal service. It would also be less restrictive than a term such as "postal message" which indicates that what is protected is limited by content and/or the purpose for which it is being sent. "Postal communication" might be defined as any communication in the course of transmission by post.

(ii) The meaning of telecommunications message

12.12 We have seen that the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* defines the expression "telecommunications message" by reference to its meaning in the *Postal and Telecommunications Services Act, 1983*, but that no specific definition of the expression is in fact given in the latter statute. Rather the 1983 Act refers to earlier statutes for the particular meaning of words and expressions, but no definition of the specific expression "telecommunications message" is to be found in these earlier statutes either.[22] We think it desirable that the expression be clearly defined in relation to the interception of communications, and are inclined to favour a definition by reference to "communications" rather than "messages" to describe what is protected since we are of the opinion that anything communicated by means of a telecommunications system should be protected not merely "messages". Moreover, both the legislation of other countries, relevant international texts to which Ireland subscribes and EU law employ variants of the word "communication".

12.13 In the 1980s it became apparent in the U.S.A. that federal legislation on the interception of communications had not kept pace with technological developments,[23] and in 1986 this legislation was amended to keep abreast of these developments. Under the *Electronic Communications Privacy Act*,[24] "electronic communications" were added to the types of protected communications and were defined to mean "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part

---

21 Section 8(1) and Part I of the Fourth Schedule: see above para. 5.52.

22 See above paras. 5.61-5.69.

23 See, e.g., *U.S. v. Gregg*, 629 F.Supp. 958 (W.D.Mo.1986), in which it was held that the legislation in question did not apply to telex communications because telexes did not constitute oral communications. *Aff'd* 829 F.2d 1430 (8th Cir. 1987), *cert. denied* 486 U.S. 1022 (1988).

24 Pub.L.No.99-508, 100 Stat. 1848.

by a wire, radio, electromagnetic, photoelectronic, or photo-optical system."[25]

12.14 A variety of terms are used in the Constitution, the Convention and the Administrative Regulations of the International Telecommunication Union.[26] Among the terms used are radiocommunication, telecommunication, telegram, telegraphy and telephony, all of which are defined in an Annex to the ITU Constitution. "Radiocommunication" is defined as "telecommunication by means of radio waves"; "telecommunication" as "any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electro-magnetic means"; "telegram" as "written matter intended to be transmitted by telegraphy for delivery to the addressee"[27]; "telegraphy" as "a form of telecommunication in which the transmitted information is intended to be recorded on arrival as a graphic document"[28]; and "telephony" as "a form of telecommunication primarily intended for the exchange of information in the form of speech". The most useful term for our purpose as a possible substitute for the expression "telecommunications message" is "telecommunication". Indeed many of the other words are defined by reference to this term.

12.15 The word "telecommunications" is also widely used in EU law. Although the word itself is not usually defined in the relevant texts, related terms are defined and it is possible to abstract from these definitions the meaning of the word "telecommunications". For example, the term "public telecommunications network" is typically defined to mean "the public telecommunications infrastructure which enables signals to be conveyed between defined network termination points by wire, by microwave, by optical means or by other electromagnetic means."[29] From this it may be understood that telecommunications are signals conveyed by wire, microwave, optical or other electromagnetic means. "Telecommunications services" are typically defined to mean "services the provision of which consists wholly or partly in the transmission and routing of signals on the public telecommunications network by means of telecommunications processes, with the exception of radio-broadcasting and television."[30]

12.16 It would seem from the above definitions that the word "telecommunication" is a possible substitute for the expression "telecommunications message". It can also be seen that these definitions contain two elements. They are definitions by reference to (i) what is communicated *and* (ii) the means of communication. As to the former, the word

---

25 18 U.S.C. §.2510(4).

26 See above paras. 7.63-7.68.

27 The term also includes radiotelegrams unless otherwise specified.

28 A graphic document records information in a permanent form and is capable of being filed and consulted; it make take the form of written or printed matter or of a fixed image.

29 Council Directive 93/38/EEC of 14 June 1993, Art. 1(14). See also, e.g., Council Directive 91/263/EEC of 29 April 1991, Art. 1(2); Council Directive 90/531/EEC of 17 September 1990, Art. 1(13); Commission Directive 90/388/EEC of 28 June 1990 Art. 1; and Council Directive 90/387/EEC of 28 June 1990, Art. 1(3).

30 Council Directive 93/38/EEC, Art. 1(15). See also, e.g., Council Directive 90/531/EEC, Art. 1(14); Commission Directive 90/388/EEC, Art. 1; and Council Directive 90/387/EEC, Art. 1(4).

"telecommunications" in the EU law cited refers only to signals, whereas the ITU texts and the U.S. legislation include also signs, writing, images, sounds, intelligence of any nature and, in the case of the U.S. legislation, also data. In a digitalised system, signs, writing, images, etc. will be converted into signals for the purpose of transmission, but in an analogue system it may be e.g. sound which is transmitted rather than signals. There may therefore be some merit in the adoption of a broader definition for the purpose of the Irish law regulating the interception of communications. Moreover, a broad definition would be capable of bringing within the scope of protection the stage in a digitalised system at which signals are converted into such forms as writing, images and intelligible sound and *vice versa*. As to the means of communication, the U.S. legislation refers to a wire, radio, electromagnetic, photoelectronic or photo-optical system; the ITU texts to wire, radio, optical or other electromagnetic means; and the EU directives to wire, microwave, optical or other electromagnetic means. In our view, the inclusive phrasing of the latter two definitions by reference to "other electromagnetic means" is to be preferred to the U.S. wording, which moreover covers electronic means of communication in general not merely forms of telecommunication. We think that of these two, the EU phrasing would be the more appropriate in the context of Irish telecommunications legislation.

(iii) A common definition?

12.17 An even simpler solution to the replacement of the expressions "postal packet" and "telecommunications message" is afforded by the British *Interception of Communications Act* of *1985*. It simply uses the word "communication" and prohibits the interception of a communication "in the course of its transmission by post or by means of a public telecommunication system".[31] No definition of "communication" is given in the Act. Nor is there any definition of "post". But "public telecommunication system" has the same meaning in the 1985 Act as in the *Telecommunications Act 1984*,[32] that is, a telecommunication system designated as such by the Secretary of State and the running of which is authorised by a licence under that Act.[33] "Telecommunication system" is defined in the 1984 Act to mean:

> " ...a system for the conveyance, through the agency of electric, magnetic, electro-magnetic, electro-chemical or other electro-mechanical energy, of -
>
> (a) speech, music and other sounds;
> (b) visual images;
> (c) signals serving for the impartation (whether as between persons and persons, things and things or persons and things) of any matter otherwise than in the form of sounds or visual images;

---

31 Section 1(1).
32 See s.10(1) of the 1985 Act.
33 See s.7 of the 1984 Act.

or

(d) signals serving for the actuation or control of machinery or apparatus."[34]

12.18 We are attracted by the simplicity of this approach and by its inclusive nature. Thus not only are such items as letters, postcards, telegrams and facsimiles covered, so are voice telephony and computerised data transmitted along telegraph wires or sent through the post.[35] What is protected against interception is defined essentially by reference to the system of transmission, that is, the post or telecommunications, and the same term, "communication", is used for what is protected when transmitted by either system. The elasticity of such a general term allows for the development of new forms of communication but is not so vague as to lack the degree of specificity required in the criminal law. *We* therefore *recommend that the expressions "postal packet" and "telecommunications message" be replaced in sections 84 and 98 of the Postal and Telecommunications Services Act, 1983 and generally in the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993 with the word "communication".*[36] *Where there is a need to distinguish between whether the communication is being transmitted by post or by telecommunications, the qualifying phrase "in the course of transmission by post" and/or "in the course of transmission by means of a public telecommunications system" should be added, as appropriate.*[37] *Similarly, these qualifying phrases would need to be added in relation to the offences under sections 84 and 98 of the 1983 Act* in order to exclude, e.g., a face to face conversation.

12.19 We do not favour a legislative definition of the word "communication". Rather, should a question arise as to whether or not a particular transmission constitutes a "communication", in the event of legal proceedings being taken, it should be left to the courts to determine the question in the particular case. We do however favour legislative guidance on the meaning of the phrases "in the course of transmission by post" and "in the course of transmission by means of a public telecommunications system". *A communication should be regarded as in the course of transmission by post from the time of its being delivered to a postal carrier to the time of its being delivered to the addressee.*[38] It is of course desirable that interference with communications both pre- and post-transmission, whether by the post or telecommunications, also be addressed by the law. Since

---

34 Section 4(1).

35 See Hansard, H.C., Vol. 76, col. 1135.

36 We note that in fact the word "communication" is already used in the 1993 Act to mean a postal packet or telecommunications message: see s.1. Implementation of our recommendation would mean that it would be more widely used in this Act. It is beyond our present remit to consider whether the expressions "postal packet" and "telecommunications message" should be replaced more generally in legislation, but it is interesting that, although the phrase "communication in the course of transmission by post or by means of a public telecommunication system" is used in connection with the offence of unlawful interception of communications under s. 1 of the British *Interception of Communications Act*, the expression "postal packet" and the word "message" in relation to telecommunications have been retained in that jurisdiction for other offences: see, e.g., s.58 of the *Post Office Act 1953* and ss.43(1) & 44(1) of the *Telecommunications Act 1984*.

37 See, e.g., s. 2(4)(b)(i) of the 1993 Act.

38 Cf. sections 74 and 90 of the *Post Office Act, 1908*, as amended by s.8(1) and Part I of the Fourth Schedule of the *Postal and Telecommunications Services Act, 1983*: see above para. 5.52.

such interference usually occurs in an institutional context,[39] we shall consider it in future reports when we come to study the protection of privacy and surveillance in specific contexts.[40] However, with reference to transmission by means of a telecommunications system, we think it desirable that any transition stage on entry to or exit from the system as when, for example, sound is converted into signals and *vice versa* should be included. *We* therefore *recommend that transmission by means of a telecommunications system should be understood to include emission and receipt. "A public telecommunications system" should be defined as "a public telecommunications infrastructure which enables signs, signals, writing, images, sound, data or intelligence of any nature to be conveyed between defined network termination points by wire, microwave, optical or other electromagnetic means."*[41] This definition is modelled on that of the "public telecommunications network" given in the EU directives cited above, with an extended list of forms of communication as suggested by the U.S. legislation.[42]

12.20 A consequence of the implementation of these recommendations may be the narrowing of the present protection afforded postal packets since, under the present law, it seems that these packets are protected against interception generally, not only while in the course of transmission by post. We shall be considering interference with the post more generally when we look at the protection of privacy in particular contexts, and consequently the recommendations we make here should not be read in isolation from any recommendation we make in this regard in our later study.

12.21 There is one further point which we should address here. Since we are concerned specifically with the protection of privacy, we should ask whether the communications to be protected should be restricted to those with a personal content. Canadian legislation, for example, employs the concept of a "private communication".[43] If we were drafting a comprehensive régime solely for the protection of privacy, it might be appropriate to include some such qualification. However, the Irish legislation we are considering deals generally with the interception of postal and tele-communications, and it is in this context that we are deciding what should be protected, albeit with the protection of privacy as our primary concern. Moreover, most states regulate the interception of such communications without reference to the content or nature of the communication. We therefore think that no such qualification should be included in the 1983 and 1993 Acts.

---

39 For example, prisoners' letters may be censored before being put in the post, and a letter to a manager at a business address may be opened and read by a secretary.

40 See above para. 1.8.

41 The interception of communications on a non-public or private telecommunications system will be considered in our study of privacy and surveillance in particular contexts.

42 See above paras. 12.14 & 12.16-12.17.

43 See above n. 18, p.315.

Interception Of Electronic Mail

12.22 There is no specific offence of interception of electronic mail. In so far as such mail constitutes a telecommunications message under existing legislation or would constitute a communication in the course of transmission by means of a public telecommunications system under our earlier recommendation,[44] unauthorised interception of such mail will be an offence under section 98(1) of the *Postal and Telecommunications Services Act, 1983*. Also, unauthorised access to such mail may constitute the offence of operating a computer with intent to gain such access under section 5 of the *Criminal Damage Act, 1991*; but it should be noted that the section requires that the mail (data) be "kept" somewhere. Where the computer is operated within the State, the data which it is intended to access may be kept either within or outside the State. Where the computer is operated outside the State, it is only an offence under section 5 if the intention was to access data kept within the State. It has been queried whether all interceptions of data would fall within the scope of section 5 in that the data may not in some circumstances be regarded as "kept" in the relevant place.[45] Certainly it may be argued that anything in the course of transmission should not be regarded as "kept" anywhere; and, on this interpretation of the section, it affords little, if any, protection against the interception of electronic mail.

12.23 It seems then that the secrecy of electronic mail is protected by s.98(1) of the *Postal and Telecommunications Services Act, 1983* during transmission and, under our recommendation, protection would extend to the stages of entry into a public telecommunications system and exit from a system. Protection pre-entry and post-exit depends upon the interpretation of section 5 of the *Criminal Damage Act, 1991*. If the data is not actually stored ("kept") anywhere at the time of interception or attempted interception, it may not be protected. Moreover, developments in technology may one day enable access to unstored data at these stages by means of a device other than one which falls within the technical or legal definition of a computer.[46] We therefore recommend the creation of a new offence which will clearly cover such situations. *It should be an offence for any person, other than the person entitled to consent to or to authorise accessing of the data concerned, intentionally to access any data without lawful excuse.*[47] *Data should be defined for the purpose of this offence as information which is automatically processed*[48]; and *a person should be regarded as having a lawful excuse if she or he believed that the person or persons whom she or he believed to be entitled to consent to or authorise accessing of the data had consented or would have consented to or authorised the accessing had the person or persons known of it.*[49]

---

44 See above para. 12.18.

45 See R. Clark, "Computer Related Crime in Ireland", (1994) 3 *European Journal of Crime, Criminal Law and Criminal Justice* 252 at 269-270.

46 For a legal definition of this term see our *Report on the Law Relating to Dishonesty*, LRC 43-1992, para. 29.25.

47 Cf. our recommendation that an offence of dishonest use of a computer should be created in our *Report on the Law Relating to Dishonesty*, para. 29.29.

48 Cf. s.1(1) of the *Data Protection Act, 1988*.

49 Cf. s.6(2)(a) & (b) of the *Criminal Damage Act, 1991*.

Encryption

12.24 One line of defence in seeking to preserve the secrecy of communications is to encrypt them. It places an additional obstacle in the way of the prying onlooker or eavesdropper. Where encryption is used, unauthorised interception or disclosure is not sufficient in itself to reveal the content of the communication. A further step of decoding is necessary in order to render the communication intelligible, and the more sophisticated the encryption, the more difficult the task of decoding. Encryption may therefore provide a counter to the inherent vulnerability of certain electronic data and communications and is potentially of great use where it is thought particularly important to protect the secrecy and/or privacy of communications.

12.25 Initiatives have already been taken at the national level in the United States of America with a view to introducing an encryption service to secure the secrecy of telecommunications while allowing the encryption to be overridden by law enforcement agencies in order e.g. to combat organised crime. On 16 April 1993, the U.S. Administration announced a proposal for a "Key-Escrow chip" or "Clipper Chip". The scheme has been described as follows:

> "Telephone users are to hold trusted "Clipper Chips" which they can use to encrypt their conversations. Each such device will have two unique keys, numbers that will be needed by authorised government agencies to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" data bases that will be established by the Attorney General. Access to these keys will be limited to government officials with legal authorisation to conduct a wire tap."[50]

Not surprisingly, reaction to this proposal in the U.S.A. has been mixed. It has been welcomed by some as a guarantor of secrecy, criticised by others as deficient for this purpose and mistrusted by yet others as a form of state control in the guise of Orwell's "Big Brother".

12.26 Steps have however already been taken to make the Clipper Chip technology available not only in the U.S.A. but also overseas.[51] In February 1994, licensing procedures were modified to facilitate the export of encryption products and thereby make it easier for U.S. companies to sell these products abroad. Also, an Interagency Working Group on Encryption and Telecommunications has been established by the U.S. Administration to work with industry and public interest groups to develop new encryption technologies and to review and refine the Administration's policies with respect to encryption.

12.27 U.S. dominance in this field of technology has not gone unnoticed by the institutions of the European Union. There has been concern that European countries may become dependent upon non-European states such as the U.S.A.

---

50 European Commission, *Green Paper on the Security of Information Systems*, 1994.

51 See, e.g., the European Commission Report, *INFOSEC '94 - The Security of Information Systems*, 1994, p.14.

for the security of electronic information systems, and a number of research projects have been undertaken at European level in recent years in this area. While recognising the importance for the single market of the security of communications-based services, the EU institutions are also aware of the importance for this market of the free movement of information between member states and are anxious not to create unnecessary technical barriers to the transborder flow of personal data in the name of protecting secrecy and/or privacy.

12.28 On 31 March 1992, the Council adopted a Decision which establishes a framework for consideration by the EU of the security of information systems.[52] The aim is to provide users and producers of electronically stored, processed or transmitted information with appropriate security of information systems against accidental or deliberate threats, and a Senior Officials Group on the Security of Information Systems was set up to advise the Commission on these matters. The Decision describes six action lines appropriate to the development of strategies to enable the free movement of information within the single market, while ensuring the security of the use of information systems throughout the Union.[53] As part of the implementation of the Decision, a number of INFOSEC projects were funded from 1992 to 1994. The most recent of these, INFOSEC '94, dealt with electronic signatures and trusted third party services.[54]

12.29 We noted above that measures are being taken within the EU in the context of public digital telecommunications networks to ensure the protection of personal data and privacy; and that it has been proposed that an obligation should be placed on telecommunications organizations to provide adequate, state-of-the-art protection of personal data against unauthorised access and use and that, where there is a particular risk of a breach of the security of a network, as in the case of mobile radio telephony, a telecommunications organization should inform subscribers of this risk and offer them an end-to-end encryption service.[55]

12.30 Whether or not such obligations are enacted by way of EU law, *we think it desirable that the Government investigate further the feasibility and the*

---

52 Council Decision 92/242/EEC.

53 The six action lines were:

Action Line 1 - Development of a strategic framework for the security of information systems;

Action Line 2 - Identification of user and service provider requirements for the security of information systems;

Action Line 3 - Solutions for immediate and interim needs of users, suppliers and service providers;

Action Line 4 - Development of specifications, standardisation, evaluation and certification in respect of the security of information systems;

Action Line 5 - Technological and operational developments in the security of information systems;

Action Line 6 - Provision of security of information systems.

54 See Commission Report, *INFOSEC '94 - The Security of Information Systems*, 1994.

55 See above para. 7.13.

appropriateness of requiring telecommunications operators to provide an encryption service to subscribers. We do not possess the technical expertise which would be required to undertake such a study ourselves, but developments in other countries as well as in the EU lead us to believe such a study is necessary if Ireland is to keep abreast of the revolution in communications technology. As has been pointed out:

> "In the emerging information society traditional techniques of securing information, such as signatures, envelopes, registration, sealing, depositing and special delivery need to be matched by electronic equivalents."[56]

12.31 Clearly many of the concerns over the security of electronic data have nothing to do with privacy. They are fostered by commercial and other considerations. The rapid growth in telematics has huge implications for the way people will conduct their lives in the twenty-first century. As a wide range of information and services becomes available on a universal basis over a telecommunications link, the prospect of a truly "global village" comes closer to realisation. In this context, information privacy[57] becomes merely one of a large number of issues which need to be addressed, most of which will call for legal regulation not only at the national but also at the international level. Indeed, by virtue of the nature of such technology, individual national measures can only be of limited effect. In this area international co-operation and regulation are essential if privacy along with other interests are to be effectively protected.

---

56 *INFOSEC '94*, p.30.

57 See above para. 1.6 for this category of claims to privacy.

CHAPTER 13: SUMMARY OF PROVISIONAL RECOMMENDATIONS

We provisionally recommend that:

1. The following torts should be created by statute (paras. 9.18-9.62):

   (i) invasion of the privacy of another person by means of surveillance;
   (ii) disclosure or publication of the purport or substance of information or material obtained by means of privacy-invasive surveillance.

   This statute should be drafted along the following lines:

   An Act To Protect The Privacy Of The Individual From Intrusive Surveillance

   Definitions
   1. *In this Act -*

   "the Court" means the Circuit Court or the District Court;

   "privacy order" has the meaning assigned to it by section 5 of this Act;

   "surveillance" includes aural and visual surveillance, irrespective of the means employed, and the interception of communications.

Causes of action

2. *It is a tort, actionable without proof of damage, for a person intentionally -*

   (i) to invade the privacy of another person by means of surveillance; or

   (ii) to disclose or publish the purport or substance of information or material obtained by means of privacy-invasive surveillance.

Defences

3. *(1) It is a defence to an action under subsections (i) and (ii) of section 2 of this Act to show that -*

   (i) the plaintiff, or some other person legally entitled to give consent on behalf of the plaintiff, consented, either expressly or impliedly, to the invasion, disclosure or publication, as the case may be; or

   (ii) the defendant was fulfilling a legal duty or exercising a legal power or right and the impact of the surveillance, disclosure or publication on the privacy of the plaintiff was not disproportionate to the legal interest pursued, having regard to the values of a sovereign, independent, democratic state.

   (2) It is also a defence to an action under subsection (ii) of section 2 of this Act to show that the defendant did not believe and had no reasonable grounds to believe that the information had been obtained by means of privacy-invasive surveillance.

   (3) The defences under subsections (1) and (2) of this section are without prejudice to any constitutional rights of the defendant.

Remedies

4. *In an action under section 2 of this Act, the Court may grant such relief as it considers appropriate in the circumstances, including any or all of the following:*

   (a) damages;

   (b) an account of profits;

   (c) a privacy order;

   (d) delivery up to the plaintiff of all material that

has come into the defendant's possession by reason or in consequence of the tort.

Privacy order

5. *(1) The Court may, if it is of opinion that there are reasonable grounds for believing that a tort is being or is about to be committed contrary to section 2 of this Act, by order (in this Act called a "privacy order"), prohibit the defendant from invading the privacy of the other person or disclosing or publishing the information or material, as the case may be, until further order by the Court or until such other time as the Court shall specify.*

(2) A privacy order may be varied by the Court on the application of either the plaintiff or the defendant.

(3) A privacy order may be discharged by the Court on the application of either the plaintiff or the defendant if the Court is satisfied that the privacy of the individual on whose behalf the order was made does not require that the order shall continue in force.

(4) A privacy order made by a court on appeal from another court shall be treated as if it had been made by that other court.

(5) A privacy order shall take effect on notification of its making being given to the defendant.

(6) Oral communication to the defendant by or on behalf of the plaintiff of the fact that a privacy order has been made, together with production of a copy of the order, shall, without prejudice to the sufficiency of any other form of notification, be taken to be sufficient notification to the defendant of the making of the order.

(7) If the defendant is present at the sitting of the Court at which the privacy order is made, that person shall be taken for the purposes of subsection (5) of this section, to have been notified of its making.

(8) An order varying or discharging a privacy order shall take effect on notification of its making being given to the plaintiff or defendant, being the person other than the person who applied for the variation, and for this purpose subsections (6) and (7) of this section shall apply with the necessary modifications.

(9) *The Court, on making, varying or discharging a privacy order, shall cause a copy of the order in question to be given or sent as soon as practicable to the plaintiff and the defendant.*

(10) *Non-compliance with subsection (9) of this section shall not affect the validity of the order.*

(11) *An appeal from a privacy order shall, if the court that made the order or the court to which the appeal is brought so determines (but not otherwise), stay the operation of the order on such terms (if any) as may be imposed by the court making the determination.*

Right of action

6. (1) *A right of action under section 2 of this Act accrues to the person whose privacy is alleged to have been or to be about to be invaded and to any other person who is legally entitled to act on behalf of that person.*

(2) *An action or right of action under section 2 of this Act, in so far as concerns the remedy of damages, is extinguished by the death of the person whose privacy is alleged to have been invaded. An action or right of action under section 2 of this Act, in so far as concerns the remedy of a privacy order, survives the death of the person whose privacy is alleged to have been invaded.*

Limitation period

7. *An action under section 2 of this Act shall be commenced within three years from the date on which the person who claims his or her privacy has been invaded became aware or ought reasonably to have become aware of the surveillance, disclosure or publication, as the case may be.*

Right of action and other remedies

8. (1) *The rights of action and the remedies under this Act are in addition to, and not in derogation of, any other right of action or remedy available otherwise than under this Act.*

(2) *This section shall not be construed as requiring any damages awarded in an action under section 2 of this Act to be disregarded in assessing damages in any other proceedings arising out of the same act as gave rise to a*

cause of action under section 2.

Title

9. *This Act may be cited as the Surveillance Privacy Act.*

2. The Scheme of Civil Legal Aid and Advice should be extended to actions under Recommendation 1. (para. 9.60)

3. As an alternative and less preferred option to Recommendation 1, the conduct which, in the following Recommendations (4-19), we propose should be criminalised should also be tortious. (para. 9.22)

4. It should be an offence to infringe the integrity of another person by observing the person by means of an optical device or by taking the person's picture by means of an optical device, without the consent of that person or of some other person legally entitled to give consent on behalf of that person. Consent may be express or implied. Taking a picture should be understood to include both the taking of still pictures and the recording of a picture on video tape. An optical device should be defined as a video camera or other similar electronic device. Both the intentional and the reckless infringement of the integrity of another person should be penalised. (paras. 10.41-10.45)

5. It should be an offence to communicate a picture taken by means of an optical device in contravention of the integrity of a person to another person or persons or to the public without the consent of the subject(s) of the picture or the consent of another person legally entitled to give consent on behalf of the subject(s). Consent may be express or implied. It should be a defence to this offence that the person communicating the picture did not know and had no reason to believe that the picture had been taken in contravention of the integrity of a person. This offence should cover only the intentional communication of a picture, but should apply where the taking of the picture constituted either an intentional or a reckless infringement of the integrity of the other person. (para. 10.47)

6. It should be a defence to the offences we propose under Recommendations 4 and 5 that the surveillance was intended to protect the life of a person. (para. 10.51) It should also be a defence that the infringement of the integrity of a person occurred in the exercise of lawful authority. (para. 10.55)

7. Video surveillance by the Gardaí and the Defence Forces of a particular person or persons or premises in the investigation of serious crime or in the interests of the security of the State should be subject to ministerial authorisation and, *mutatis mutandis*, to a régime such as that applicable

to the interception of communications under the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.* Moreover, it is desirable that internal guidelines be drawn up by each force in respect of the implementation of a warrant authorising video surveillance and of the handling, disclosure etc. of information and material obtained thereby. (paras. 10.56-10.66)

8. Where a public place is subject to video surveillance, the person responsible for the surveillance should be under a legal obligation to display an easily legible notice to this effect at all access points. A public place should be defined as "any place to which the public or any section of the public has access, on payment or otherwise, as of right or by virtue of express or implied permission." Where an area comprises a number of distinct units, each unit should be considered a separate public place for the purpose of the notice requirement. The notice requirement should apply to constant or regular surveillance by means of an automatically-functioning optical device, and optical device should be defined as a video camera or other similar electronic device. Failure to comply with the notice obligation should be an offence of strict liability. There should be an exception to the requirement for video surveillance carried out under ministerial authorisation by the Gardaí and the Defence Forces. (paras. 10.67-10.71)

9. It should be an offence to infringe the privacy of another person by listening to or recording the voice of that person by means of an aural device, without the consent of the person or of some other person legally entitled to give consent on behalf of the person. Consent may be express or implied. Privacy should be defined to mean private life; and aural device should be defined as an electronic device which enables sound which would not otherwise be within the range of human hearing to be heard or recorded. The offence should cover both the intentional and the reckless infringement of the private life of another person. (paras. 11.27-11.30)

10. It should be an offence to communicate the purport or substance of what was heard or recorded in contravention of the privacy of a person to another person or persons or to the public without the consent of the person whose voice was heard or recorded or the consent of some other person legally entitled to give consent on behalf of that person. Consent may be express or implied. It should be a defence to this offence that the person communicating the purport or substance of what was heard or recorded did not know and had no reason to believe that the voice had been heard or recorded in contravention of the privacy of a person. This offence should cover only the intentional communication of the purport or substance of what was heard or recorded, but should apply where the hearing or recording constituted either an intentional or a reckless infringement of the privacy of the other person. (para. 11.31).

11. There should be an exemption from the criminal liability we propose under Recommendations 9 and 10 for aural surveillance by the Gardaí and the Defence Forces of a particular person or persons or premises in the investigation of serious crime and in the interests of the security of the State. Such surveillance should be subject to ministerial authorisation and, *mutatis mutandis*, to a régime such as that applicable to the interception of communications under the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*. Moreover, it is desirable that internal guidelines be drawn up by each force in respect of the implementation of a warrant authorising aural surveillance and of the handling, disclosure etc. of information and material obtained thereby. (paras. 11.33-11.34)

12. It should be a defence to the offences we propose under Recommendations 9 and 10 for the defendant to show that she or he acted to protect her or his person or property or another person or persons and that the material or information obtained by the surveillance was used only for this purpose and that the material or information and any copy thereof was destroyed as soon as the reason for its retention ceased to exist. The burden of proving this defence should fall on the defendant, and should be discharged on the balance of probabilities. (para. 11.35) Consideration should also be given to whether or not there should be a defence that the person who engaged in the surveillance or communicated to another what was heard or recorded acted in order to prevent or to expose the commission of a serious offence. (para. 11.36)

13. Where surveillance involving the use of an aural or optical device is carried out on behalf of or in co-operation with the Gardaí or the Defence Forces, the warrant procedure and safeguards applicable to the interception of communications under the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* should apply, *mutatis mutandis*, to such surveillance. (para. 11.43)

14. Section 98(2) of the *Postal and Telecommunications Services Act, 1983* should be amended to require that the investigation be authorised by a member of the Garda Síochána not below the rank of superintendent. (para. 12.2)

15. The *Postal and Telecommunications Services Act, 1983* should be amended to prohibit disclosure of the purport or substance of information obtained by third party monitoring, by the third party, to a person or persons other than the party or parties on whose behalf or in co-operation with whom the monitoring was carried out, without the consent of that party or those parties. (para. 12.5)

16. Section 98 of the *Postal and Telecommunications Services Act, 1983* should be amended to cover transmission by means of any public telecommunications system. "Public telecommunications system" should

be defined as under Recommendation 20 below. (para. 12.8)

17. The Minister for Transport, Energy and Communications should use existing licensing powers to ensure that all postal and telecommunications carriers who offer their services to the public and for which services a licence is required are brought within the scheme of the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*; and regulations should be made under section 111(5) of the *Postal and Telecommunications Services Act, 1983* for this purpose. Legislative provision should also be made for the extension of the scheme to postal carriers offering a service to the public for which a licence is not presently required. (para. 12.9)

18. The expressions "postal packet" and "telecommunications message" in sections 84 and 98 of the *Postal and Telecommunications Services Act, 1983* and in the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* should be replaced with the word "communication". Where there is a need to distinguish between whether the communication is being transmitted by post or by telecommunications, the qualifying phrase "in the course of transmission by post" and/or "in the course of transmission by means of a public telecommunications system" should be added, as appropriate. These qualifying phrases should be used in the rephrasing of the offences under section 84 and 98 of the 1983 Act. A communication should be regarded as in the course of transmission by post from the time of its being delivered to a postal carrier to the time of its being delivered to the addressee. Transmission by means of a telecommunications system should be understood to include emission and receipt. "A public telecommunications system" should be defined as "a public telecommunications infrastructure which enables signs, signals, writing, images, sound, data or intelligence of any nature to be conveyed between defined network termination points by wire, microwave, optical or other electromagnetic means." (paras. 12.18-12.19)

19. It should be an offence for any person, other than the person entitled to consent to or to authorise accessing of the data concerned, intentionally to access any data without lawful excuse. Data should be defined for the purpose of this offence as information which is automatically processed; and a person should be regarded as having a lawful excuse if she or he believed that the person or persons whom they believed to be entitled to consent to or to authorise accessing of the data had consented or would have consented to or authorised the accessing had the person or persons known of it. (para. 12.23)

20. The torts and the offences which we recommend should apply to members of the media as to all other persons. We welcome submissions on this. We reiterate the recommendation in our *Report on Non-Fatal Offences Against the Person* that there be a general offence of

harassment. We also welcome submissions on whether there should be a "group" offence of collective besetting. (para. 8.29)

21. The Government should examine the feasibility and the appropriateness of requiring telecommunications operators to provide an encryption service to subscribers. (para. 12.30)

22. We also think it desirable that:

(a) the Independent Radio and Television Commission, in the exercise of its powers under sections 9(3) and 18(1) of the *Radio and Television Act, 1988*, give thought to including in a code of practice for independent broadcasters guidelines on respect for privacy comparable to those contained in the *Broadcasting Guidelines for RTE Personnel*; (para. 8.30)

(b) The National Union of Journalists consider formulating more detailed provisions on respect for privacy for insertion in its *Code of Conduct* for members; (para. 8.30)

(c) Individual newspapers and other publications consider issuing explicit editorial instructions to staff on respect for privacy. (para. 8.30)

APPENDIX A

Application for a licence under Section 111 of the Postal and Telecommunications Services Act, 1983 (hereinafter called "The Act") to provide Telecommunications Services for the Public.

1. The Telecommunications Services provided for the Public under any Licence granted by the Minister for Transport, Energy and Communications on foot of this application -

   (a) shall be services involving the transmitting, receiving, collecting or delivering of telecommunications messages, other than those to which section 87(3) of the Act relates;

   (b) shall not involve the provision of voice telephony i.e. the commercial provision for the public of the direct transport and switching of speech in real time between public switched network termination points, enabling any user to use equipment connected to such a network termination point in order to communicate with another termination point;

   (c) shall not involve the conveyance of messages by telex, mobile radio telephony, paging or satellite services;

   (d) shall utilise telecommunications links provided by Bord Telecom Éireann under the exclusive privilege conveyed by section 87 of the Act for the conveying of telecommunications messages within the State;

   (e) shall utilise international telecommunications links provided by Bord Telecom Eireann or other network operators licensed by the Minister for Transport, Energy and Communications for any international conveying of telecommunications messages to or from the State;

(f) shall not involve connection to the Public Telecommunications Networks of any equipment which has not been type-approved by the Minister for Transport, Energy and Communications for connection to the public telecommunications networks

This application must be completed in type or block letters.

(i) **In the case of an individual**, the application must be signed by the person in whose name the application is made.

(ii) **In the case of a partnership**, the application must be signed by **each** of the partners.

(iii) **In the case of a company or other body corporate**, the application must be signed by a **director**, company secretary or other authorised officer.

(iv) **In the case of a cooperative or other body**, the application must be signed by the secretary of the cooperative or other body.

2. Name and Address of Applicant:

3. Name under which Applicant proposes to trade if different to above:

Address:

4. If the Applicant is a company, partnership, cooperative or other body please give the name(s) and private address(es) of each of the current directors, company secretary, partners or members of the committee of management:

NAME	ADDRESS
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

5. I hereby declare that the telecommunications services to which this application applies shall, at all times comply in every respect with the service conditions detailed at 1. above, which service conditions I hereby acknowledge to have read and understood.

Signed _____

_____

Full Name of Signatory _____

_____

Position held (where applicant is a company, cooperative or other body corporate)

_____

Date: _____

APPENDIX B

Licence under Section 111(2A) of the Postal and Telecommunications Services Act, 1983, to provide Telecommunications Services to the Public

Licence Number: _____

The Minister for Transport, Energy and Communications (hereinafter referred to as "the Minister") in exercise of the powers conferred on him by Section 111 (as amended by European Communities (Telecommunications Services) Regulations, 1992) of the Postal and Telecommunications Act, 1983 (hereinafter referred to as "the Act"), hereby grants to

_____

(hereinafter referred to as "the Licensee") a licence (No. _____) to provide telecommunications services for the public within, and to and from, the State subject to the following conditions.

Conditions

1. The telecommunications services provided for the public under this licence:-

   (a) shall be services involving the transmitting, receiving, collecting or delivering of telecommunications messages other than those to which Section 87(3) of the Act relates,

(b) shall not involve the commercial provision for the public of the direct switching of speech in real time between public switched network termination points enabling any user to use equipment connected to such a network termination point in order to communicate with another termination point,

(c) shall not involve the conveyance of messages by telex, mobile radio telephony, paging or satellite services,

(d) shall utilise telecommunications links provided by Bord Telecom Éireann under the exclusive privilege conveyed by Section 87 of the Act for the conveying of telecommunications messages within the State,

(e) shall utilise international telecommunications links provided by Bord Telecom Éireann or other network operators licensed by the Minister for any international conveying of telecommunications messages to or from the State,

(f) shall not involve connection to the public telecommunications network of any equipment which has not been type-approved by the Minister for connection to the public telecommunications network.

2. This Licence shall be valid from the date it is granted up to and including the th day of 19 .

3. The application for this Licence was in a form prescribed by the Minister and accompanied by a fee of £

4. This Licence is not transferable.

5. This Licence may be suspended or revoked by the Minister if he is satisfied that:-

(a) the Licensee has breached any of the conditions of this Licence or any provisions of the Act or the European Communities (Telecommunications Services) Regulations, 1992, or

(b) the Licensee has made any false declaration in relation to the application for this Licence, or

(c) it is in the national interest to revoke this Licence, or

(d) the Licensee has ceased to provide public telecommunications services, or

(e) the telecommunications services provided by the Licensee no

longer fulfil the "essential requirements" as defined in Commission Directive No. 90/388/EEC of 28 June, 1990, or

(f) a receiving order for bankruptcy has been made in respect of the estate of the Licensee, or

(g) where the Licensee is a company within the meaning of the Companies Acts 1963 to 1990, an order for its winding up has been made or a resolution for voluntary winding up (within the meaning of those Acts) has been passed by the company otherwise than for the purpose of a merger of reconstruction, or a receiver of the property of the company has been appointed.

6. The conditions of this Licence may be revised from time to time by the Minister.

Signed on behalf of the Minister for Transport, Energy and Communications by:

_____

An officer of the Department of Transport, Energy and Communications, authorised in this behalf by the said Minister

Date: _____

APPENDIX C

The Attorney General's Scheme

The provisions of the Attorney General's Scheme in the High Court and Supreme Court are as follows:

1. The Scheme applies to the following forms of litigation (which are not covered by Civil or Criminal Legal Aid):

   (i) *Habeas corpus* applications.
   (ii) Bail Motions.
   (iii) Such Judicial Reviews as consist of or include Certiorari, Mandamus or Prohibition.
   (iv) Applications under section 50 of the *Extradition Act, 1965*.

2. The purpose of the Scheme is to provide legal representation for persons who need it but cannot afford it. It is not an alternative to costs. Accordingly, a person wishing to obtain from the Court a recommendation to the Attorney General that the Scheme be applied must make his application (personally or through his lawyer) at the *commencement* of the proceedings.

3. The applicant must satisfy the Court that he is not in a position to retain a Solicitor (or, where appropriate, Counsel) unless he receives the benefit of the Scheme. To this end the applicant must provide such information about his means as the Court deems appropriate.

4. The Court must be satisfied that the case warrants the assignment of Counsel and/or Solicitor.

5. If the Court considers that the complexity or importance of the case requires it, the recommendation for Counsel may also include one

Senior Counsel.

6. The costs payable to the Solicitor, and the fees payable to Counsel, under the Scheme are those which would be payable in a case governed by the Criminal Justice (Legal Aid) Regulations current for the time being, applied *mutatis mutandis*.

7. Where there is more than one applicant, but only one matter is at issue before the court, the Solicitor and Counsel assigned shall represent all the applicants.

APPENDIX D

SELECTED CANADIAN LEGISLATION

British Columbia Privacy Act, 1979

Violation of privacy actionable

1. (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of another.

(2) The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, due regard being given to the lawful interests of others.

(3) In determining whether the act or conduct of a person is a violation of another's privacy, regard shall be given to the nature, incidence and occasion of the act or conduct and to any domestic or other relationship between the parties.

(4) Privacy may be violated by eavesdropping or surveillance, whether or not accomplished by trespass; but this subsection shall not be construed as restricting the generality of subsections (1) to (3).

Exceptions

2. (1) An act or conduct is not a violation of privacy where

(a) it is consented to by some person entitled to consent;

(b) the act or conduct was incidental to the exercise of a lawful right or defence of person or property;

(c) the act or conduct was authorized or required by or under a

law in force in the Province, by a court or by any process of a court; or

(d) the act or conduct was that of

(i) a peace officer acting in the course of his duty to prevent, discover or investigate crime or to discover or apprehend the perpetrators of crime; or

(ii) a public officer engaged in an investigation in the course of his duty under a law in force in the Province,

and was neither disproportionate to the gravity of the crime or matter subject to investigation nor committed in the course of a trespass.

(2) A publication of a matter is not a violation of privacy if

(a) the matter published was of public interest or was fair comment on a matter of public interest; or

(b) the publication was, in accordance with the rules of law relating to defamation, privileged;

but this subsection does not extend to any other act or conduct by which the matter published was obtained if that other act or conduct was itself a violation of privacy.

(3) In this section

"court" includes a person authorized by law to administer on oath for taking evidence for the purpose for which he is authorized to take evidence; and

"crime" includes an offence against a law of the Province.

Unauthorized use of name or portrait of another

3. (1) It is a tort, actionable without proof of damage, for a person to use the name or portrait of another for the purpose of advertising or promoting the sale of, or other trading in, property or services, unless that other, or a person entitled to consent on his behalf, consents to the use for that purpose.

(2) A person is not liable to another for the use for the purposes stated in subsection (1) of a name identical with, or so similar as to be capable of being mistaken for, that of the other, unless the court is satisfied that

(a) the defendant specifically intended to refer to the plaintiff or to exploit his name or reputation; or

(b) either on the same occasion or on some other occasion in the course of a program of advertisement or promotion, the name was connected, expressly or impliedly, with other material or details sufficient to distinguish the plaintiff, to the public at large or to the members of the community in which he lives or works, from others of the same name.

(3) A person is not liable to another for the use, for the purposes stated in subsection (1), of his portrait in a picture of a group or gathering, unless the plaintiff is

(a) identified by name or description, or his presence is emphasized, whether by the composition of the picture or otherwise; or

(b) recognizable, and the defendant, by using the picture, intended to exploit the plaintiff's name or reputation.

(4) Without prejudice to the requirements of any other case, in order to render another liable for using his name or portrait for the purposes of advertising or promoting the sale of

(a) a newspaper or other publication, or the services of a broadcasting undertaking, the plaintiff must establish that his name or portrait was used specifically in connection with material relating to the readership, circulation or other qualities of the newspaper or other publication, or to the audience, services or other qualities of the broadcasting undertaking, as the case may be; and

(b) goods or services on account of the use of the name or portrait of the other in a radio or television program relating to current or historical events or affairs, or other matters of public interest, which is sponsored or promoted by or on behalf of the makers, distributors, vendors or suppliers of the goods or services, the plaintiff must establish that his name or portrait was used specifically in connection with material relating to the goods or services, or to their manufacturers, distributors, vendors or suppliers.

(5) In this section "portrait" means a likeness, still or moving, and includes a likeness or another deliberately disguised to resemble the plaintiff, and a caricature.

Jurisdiction

4. Notwithstanding anything contained in another Act, an action pursuant to this Act shall be heard and determined by the Supreme Court.

Action does not survive death
5. An action or right of action for a violation of privacy or for the unauthorized use of the name or portrait of another for the purposes stated in this Act is extinguished by the death of the person whose privacy is alleged to have been violated or whose name or portrait is alleged to have been used without authority.

Manitoba Privacy Act, 1979

Definitions
1. In this Act

"court" means the Court of Queen's Bench except in section 5 where it means any court and includes a person authorized by law to take evidence under oath acting for the purposes for which he is authorized to take evidence; ("tribunal")

"defamation" means libel or slander; ("diffamation")

"family" means the husband, wife, child, step-child, parent, step-parent, brother, sister, half-brother, half-sister, step-brother, step-sister, of a person. ("famille")

Violation of privacy
2. (1) A person who substantially unreasonably, and without claim of right, violates the privacy of another person, commits a tort against that other person.

Action without proof of damage
2. (2) An action for violation of privacy may be brought without proof of damage.

Examples of violation of privacy
3. Without limiting the generality of section 2, privacy of a person may be violated

(a) by surveillance, auditory or visual, whether or not accomplished by trespass, of that person, his home or other place of residence, or of any vehicle, by any means including eavesdropping, watching, spying, besetting or following;

(b) by the listening to or recording of a conversation in which that person participates, or messages to or from that person, passing along, over or through any telephone lines, otherwise than as a lawful party thereto or under lawful authority conferred to that end;

(c) by the unauthorized use of the name or likeness or voice of that person for the purposes of advertising or promoting the sale of, or any other trading in, any property or services, or for any other purposes of gain to the user if, in the course of the use, that person is identified or identifiable and the user intended to exploit the name or likeness or voice of that person; or

(d) by the use of his letters, diaries and other personal documents without his consent or without the consent of any other person who is in possession of them with his consent.

Remedies

4. (1) In any action for violation of privacy the court may

(a) award damages;

(b) grant an injunction if it appears just and reasonable;

(c) order the defendant to account to the plaintiff for any profits that have accrued, or that may subsequently accrue, to the defendant by reason or in consequence of the violation; and

(d) order the defendant to deliver up to the plaintiff all articles or documents that have come into his possession by reason or in consequence of the violation.

Considerations in awarding damages

4. (2) In awarding damages in an action for a violation of privacy of a person, the court shall have regard to all the circumstances of the case including

(a) the nature, incidence and occasion of the act, conduct or publication constituting the violation of privacy of that person;

(b) the effect of the violation of privacy on the health, welfare, social, business or financial position of that person or his family;

(c) any relationship, whether domestic or otherwise, between the parties to the action;

(d) any distress, annoyance or embarrassment suffered by that person or his family arising from the violation of privacy; and

(e) the conduct of that person and the defendant, both before and after the commission of the violation of privacy, including any apology or offer of amends made by the defendant.

Accounting not considered in awarding damages

4. (3) Notwithstanding anything in subsection (2), in awarding damages in an action for violation of privacy of a person, the court shall not have regard to any order made under clause (1)(c) in respect of the violation of privacy.

Defences

5. In an action for violation of privacy of a person, it is a defence for the defendant to show

(a) that the person expressly or by implication consented to the act, conduct or publication constituting the violation; or

(b) that the defendant, having acted reasonably in that regard, neither knew or should reasonably have known that the act, conduct or publication constituting the violation would have violated the privacy of any person; or

(c) that the act, conduct or publication in issue was reasonable, necessary for, and incidental to, the exercise or protection of a lawful right of defence of person, property, or other interest of the defendant or any other person by whom the defendant was instructed or for whose benefit the defendant committed the act, conduct or publication constituting the violation; or

(d) that the defendant acted under authority conferred upon him by a law in force in the province or by a court or any process of a court; or

(e) where the act, conduct or publication constituting the violation was

(i) that of a peace officer acting in the course of his duties; or

(ii) that of a public officer engaged in an investigation in the course of his duty under a law in force in the province;

that it was neither disproportionate to the gravity of the matter subject to investigation nor committed in the course of a trespass; and was within the scope of his duties or within the scope of the investigation, as the case may be, and was reasonably necessary in the public interest;

(f) where the alleged violation was constituted by the publication of any matter

(i) that there were reasonable grounds for the belief that the publication was in the public interest; or

(ii) that the publication was, in accordance with the rules of law in force in the province relating to defamation, privileged; or

(iii) that the matter was fair comment on a matter of public interest.

Right of action in addition to other rights

6. The right of action for violation of privacy under this Act and the remedies under this Act are in addition to, and not in derogation of, any other right of action or other remedy available otherwise than under this Act; but this section shall not be construed as requiring any damages awarded in an action for violation of privacy to be disregarded in assessing damages in any other proceedings arising out of the same act, conduct or publication constituting the violation of privacy.

Effect on law of evidence

7. No evidence obtained by virtue or in consequence of a violation of privacy in respect of which an action may be brought under this Act is admissible in any civil proceedings.

Application of Act

8. (1) Notwithstanding any other Act of the Legislature, whether special or general, this Act applies where there is any violation of the privacy of any person.

Conflict with other Acts

8. (2) Where there is a conflict between a provision of this Act and a provision of any other Act of the Legislature, whether special or general, the provision of this Act prevails.

Newfoundland Privacy Act, 1981

Short title

1. This Act may be cited as *The Privacy Act*.

Definition

2. In this Act "individual" means a natural person.

Violation of privacy

3. (1) It is a tort, actionable without proof of damage, for a person, wilfully and without a claim of right, to violate the privacy of an individual.

(2) The nature and degree of privacy to which an individual is entitled in any situation or in relation to any matter is that which is reasonable in the circumstances, due regard being given to the lawful interests of others; and in determining whether the act or conduct of a person constitutes a violation of the privacy of an individual, regard shall be given to the nature, incidence, and occasion of the act or conduct and to the relationship, whether domestic or other, between the parties.

Examples

4. Without limiting the generality of section 3, proof that there has been

(a) surveillance, auditory or visual, whether or not accomplished by trespass, of an individual, by any means including eavesdropping, watching, spying, besetting or following;

(b) listening to or recording of a conversation in which an individual participates, or listening to or recording of messages to or from that individual passing by means of telecommunications, otherwise than as a lawful party thereto:

(c) use of the name or likeness or voice of an individual for the purposes of advertising or promoting the sale of, or any other trading in, any property or services, or for any other purposes of advantage to the user if, in the course of the use, the individual is identified or identifiable and the user intended to exploit the name or likeness or voice of that individual; or

(d) use of letters, diaries or other personal documents of an individual,

without the consent, expressed or implied, of the individual or some other person who has the lawful authority to give the consent is *prima facie* proof of a violation of the privacy of the individual first mentioned.

Defences

5. (1) An act or conduct is not a violation of privacy where

(a) it is consented to by some person entitled to consent;

(b) the act or conduct was incidental to the exercise of a lawful right of defence of person or property;

(c) the act or conduct was authorized or required by or under a

law in force in the province or by a court or any process of a court; or

(d) the act or conduct was that of

(i) a peace officer acting in the course of his duty for the prevention, discovery or investigation of crime or of the discovery or apprehension of the perpetrators of a crime, or

(ii) a public officer engaged in an investigation in the course of his duty under a law in force in the province,

and was neither disproportionate to the gravity of the crime or matter subject to the investigation nor committed in the course of a trespass.

(2) A publication of any matter is not a violation of privacy if

(a) the matter published was of public interest or was fair comment on a matter of public interest; or

(b) the publication was, in accordance with the rules of law relating to defamation, privileged,

but this subsection does not extend to any other act or conduct whereby the matter published was obtained if such other act or conduct was itself a violation of privacy.

(3) In this section

(a) "court" includes any person authorized by law to administer an oath for the taking of evidence acting for the purposes for which he is authorized to take evidence; and

(b) "crime" includes any offence against a law of the province.

Remedies

6. (1) In an action for violation of privacy, the court may do any or all of the following:

(a) award damages;

(b) grant an injunction;

(c) order the defendant to account to the plaintiff, for any profits that have accrued or that may subsequently accrue to the

defendant by reason or in consequence of the violation;

(d) order the defendant to deliver up to the plaintiff all articles or documents that have come into his possession by reason or in consequence of the violation;

(e) grant any other relief to the plaintiff that appears necessary under the circumstances.

(2) In awarding damages in an action for violation of privacy of an individual, the court may disregard any order made under paragraph (c) of subsection (1) in respect of the violation of privacy.

Additional remedies

7. (1) The right of action for violation of privacy under this Act and the remedies under this Act are in addition to, and not in derogation of, any other right of action or other remedy available otherwise than under this Act.

(2) This section shall not be construed as requiring any damages awarded in an action for violation of privacy to be disregarded in assessing damages in any other proceedings arising out of the same act, conduct or publication constituting the violation of privacy.

Court

8. Notwithstanding anything contained in any other Act, an action for violation of privacy shall be heard and determined by the Trial Division.

Paramountcy

9. (1) Notwithstanding any other Act, whether special or general, this Act applies where there is any violation of the privacy of any individual.

(2) Where there is a conflict between a provision of this Act and a provision of any other act, whether general or special, the provision of this Act prevails.

Limitation

10. No action lies for the violation of the privacy of an individual after the expiration of two years from the time when the violation of privacy first became known or should have become known by that individual nor, in any case, after the expiration of seven years from the date on which the violation of privacy

occurred.

Death

11. A right of action for violation of privacy is extinguished by the death of the individual whose privacy is alleged to have been violated.

Crown bound

12. This Act binds the Crown.

Saskatchewan Privacy Act, 1979

Short title

1. This Act may be cited as *The Privacy Act*.

Violation of privacy

2. It is a tort, actionable without proof of damage, for a person, wilfully and without claim of right, to violate the privacy of another person. 1973-74, c.80, s.2.

Examples of violation of privacy

3. Without limiting the generality of section 2, proof that there has been:

(a) auditory or visual surveillance of a person by any means including eavesdropping, watching, spying, besetting or following and whether or not accomplished by trespass;

(b) listening to or recording of a conversation in which a person participates, or listening to or recording of messages to or from that person passing by means of telecommunications, otherwise than as a lawful party thereto;

(c) use of the name or likeness or voice of a person for the purposes of advertising or promoting the sale of, or any other trading in, any property or services, or for any other purposes of gain to the user if, in the course of the use, the person is identified or identifiable and the user intended to exploit the name or likeness or voice of that person; or

(d) use of letters, diaries or other personal documents of a person;

without the consent, expressed or implied, of the person or some other person who has the lawful authority to give the consent is *prima facie* evidence of a violation of the privacy of the person first mentioned. 1973-74, c.80, s.3; 1979, c.69, s.19.

Defences

4. (1) An act, conduct or publication is not a violation of privacy where:

(a) it is consented to, either expressly or impliedly by some person entitled to consent thereto;

(b) it was incidental to the exercise of a lawful right of defence of person or property;

(c) it was authorized or required by or under a law in force in the province or by a court of any process of a court; or

(d) it was that of:

(i) a peace officer acting in the course and within the scope of his duty; or

(ii) a public officer engaged in an investigation in the course and within the scope of his duty;

and was neither disproportionate to the gravity of the matter subject to investigation nor committed in the course of trespass;

(e) it was that of a person engaged in a news gathering:

(i) for any newspaper or other paper containing public news; or

(ii) for a broadcaster licensed by the Canadian Radio-Television Commission to carry on a broadcasting transmitting undertaking;

and such act, conduct or publication was reasonable in the circumstances and was necessary for or incidental to ordinary news gathering activities.

(2) A publication of any matter is not a violation of privacy where:

(a) there were reasonable grounds for belief that the matter published was of public interest or was fair comment on a matter of public interest; or

(b) the publication was, in accordance with the rules of law relating to defamation, privileged;

but this subsection does not extend to any other act or conduct whereby the matter published was obtained if such other act or conduct was itself a violation

of privacy.

(3) In this section "court" means any person authorised by law to administer an oath for the taking of evidence acting for the purposes for which he is authorised to take evidence. 1973-74, c.80, s.4.

Court

5. Notwithstanding anything in any other Act, an action for violation of privacy shall be commenced, tried and determined in the Court of Queen's Bench. 1973-74, c.80, s.5.

Considerations in determining whether there is a violation of privacy

6. (1) The nature and degree of privacy to which a person is entitled in any situation or in relation to any situation or matter is that which is reasonable in the circumstances, due regard being given to the lawful interests of others.

(2) Without limiting the generality of subsection (1) in determining whether any act, conduct or publication constitutes a violation of the privacy of a person, regard shall be given to:

(a) the nature, incidence and occasion of the act, conduct or publication;

(b) the effect of the act, conduct or publication on the health and welfare, or the social, business or financial position, of the person or his family or relatives;

(c) any relationship whether domestic or otherwise between the parties to the action; and

(d) the conduct of the person and of the defendant both before and after the act, conduct or publication, including any apology or offer or amends made by the defendant. 1973-74, c.80, s.6.

Remedies

7. In an action for violation of privacy, the court may as it considers just:

(a) award damages;

(b) grant an injunction;

(c) order the defendant to account to the plaintiff, for any profits that have accrued or that may subsequently accrue to the defendant by reason or in consequence of the violation;

(d) order the defendant to deliver up to the plaintiff all articles or documents that have come into his possession by reason or in consequence of the violation; or

(e) grant any other relief to the plaintiff that appears necessary under the circumstances. 1973-74, c.80, s.7.

Right of action in addition to other rights

8. (1) The right of action for violation of privacy under this Act and the remedies under this Act are in addition to, and not in derogation of, any other right of action or other remedy available otherwise than under this Act.

(2) This section shall not be construed as requiring any damages awarded in an action for violation of privacy to be disregarded in assessing damages in any other proceedings arising out of the same act, conduct or publication constituting the violation of privacy. 1973-74, c.80, s.8.

Limitation

9. An action for violation of privacy shall be commenced within two years from the discovery of the alleged violation of privacy by the person who claims his privacy has been violated. 1973-74, c.80, s.9.

Death extinguishes right of action

10. A right of action for violation of privacy is extinguished by the death of the person whose privacy is alleged to have been violated. 1973-74, c.80, s.10.

Crown is bound

11. The Crown is bound by this Act. 1973-74, c.80, s.11.

APPENDIX E

PRIVACY COMMISSIONER OF AUSTRALIA

COVERT OPTICAL SURVEILLANCE IN COMMONWEALTH ADMINISTRATION - GUIDELINES

General Guidelines for the Conduct of Covert Optical Surveillance

Limitation to optical surveillance guidelines: The guidelines are limited to optical surveillance activities because whilst there is a fairly comprehensive body of legislation dealing with aural, postal and telecommunications surveillance devices, there is no law dealing with optical surveillance devices.

Adoption: These guidelines are of an advisory nature and are intended to provide a framework for agencies to develop their own guidelines taking into account their role, their priorities and other operational factors, when conducting covert surveillance for statutory investigations.

Not affected: National security organisations and agencies who use covert surveillance for law enforcement purposes.

Agencies in preparing their guidelines for conducting covert surveillance by optical means should consider the following:

1. DECISION TO UNDERTAKE COVERT SURVEILLANCE

IPP[1] 1 requires that information shall not be collected unless the purpose is lawful and directly related to a function or activity of the collector and the collection is necessary or directly related to the purpose. It also states that collection shall not be by unlawful or unfair means.

---

1 IPP = Information Privacy Principle. These Principles, of which there are 11, are listed in s.14 of the Privacy Act 1988.

Purpose of Covert Surveillance

1.1 Covert surveillance may only be undertaken for a lawful purpose which is related to the function and activity of the agency.

1.2 Each agency should identify the circumstances or offences for which covert surveillance may be used and the Acts which may justify the agency undertaking the practice.

Examples include:

- surveillance of healthcare providers suspected of fraud in claiming payments for services provided under the *Health Insurance Act 1973* or the *Veterans' Entitlements Act 1986*
- surveillance of suspected illegal immigrants under the *Migration Act 1958*
- surveillance of staff suspected of theft under the *Crimes Act 1914.*

Decision-maker

1.3 Approval to conduct covert surveillance in any particular case should be made at a senior level, taking into account procedures in place for the conduct of such activities.

Criteria for Decision

1.4 In deciding to conduct covert surveillance agencies should consider the following factors:

(a) That there be reasonable suspicion to believe that an offence or an unlawful activity is about to be committed, is being committed or has been committed

(b) That other forms of investigation have been considered and have been assessed to be unsuitable, or other forms of investigation have been tried and have been found to be inconclusive or unsuitable.

(c) The benefits arising from obtaining relevant information by covert surveillance are considered to outweigh to a substantial degree the intrusion on the privacy of the surveillance subject/s.

Where considered appropriate by agencies the Commonwealth Director of Public Prosecutions or other legal advisers should be consulted concerning the desirability or necessity of obtaining information by covert surveillance.

2. *THE CONDUCT OF THE COVERT SURVEILLANCE OPERATION*

IPP 1 imposes obligations on Commonwealth Agencies relating to the collection of personal information. Collection must be fair and lawful. The information collected must be for a lawful purpose which is directly related to the function or activity of the agency and the collection of information must be necessary for or directly related to that purpose.

In order to comply with these obligations agencies should be mindful of the following:

2.1 The collection of personal information using a covert surveillance operation should be conducted in a lawful manner. Any covert surveillance operation which may involve the commission of a criminal offence or which may give rise to civil action, for example, trespass to lands or goods cannot be sanctioned.

2.2 The collection should not involve entrapment of the surveillance subject. Hence, passive observation is permissible, however, any attempts to actively induce the surveillance subject into a situation in which that person would not ordinarily and voluntarily enter should not be permitted. For example, whilst an investigator could pose as a patient in cases of investigations for overservicing by a doctor to afford an opportunity for the doctor to commit a crime if the doctor is so minded, the investigator should not induce a doctor into a crime the doctor is otherwise unwilling to commit.

2.3 Agencies should avoid any actions which may unreasonably impinge on the privacy and rights of other people, e.g. when using photography, avoid, where practicable, including other individuals such as relatives and friends in the photograph.

2.4 Where practicable only material relevant to the purpose of conducting the covert surveillance should be collected. There should be a clear separation of facts from opinions and only relevant personal information should be included in records resulting from the surveillance.

3. *HANDLING OF RECORDS ARISING FROM COVERT SURVEILLANCE*

Security

IPP 4 requires agencies to protect information with reasonable security safeguards against loss, unauthorised access, use, modification or disclosure; and other misuse. If it is necessary for the record to be given to a person who is providing a service to the agency, then everything which is reasonably within the power of the agency, must be done to prevent unauthorised use or disclosure of information.

Clear instructions on obligations of investigators to safeguard the material collected should be developed by agencies. Agencies should include confidentiality clauses in contracts when employing private investigators.

Access and Correction

IPP 6 concerns access by individuals to their personal information. Individuals are entitled to have access to their files unless a specific provision of a law of the Commonwealth refusing such access applies. In general, the Freedom of Information exemptions will often apply.

IPP 7 concerns an agencies (*sic*) obligations to ensure that the quality of data is maintained by seeing that it remains relevant and is tested for accuracy, is up-to-date, complete and not misleading. This IPP also provides for individuals to attach to records any statement relating to the correction, deletion or addition they consider should be made to the personal information on that record.

Use and Disclosure

IPPs 8 and 9 require agencies to:

. check that information is accurate, up-to-date, complete and relevant prior to using it.

In order to comply with the requirements of IPP 8 agencies will need to consider tests for accuracy of information prior to use. These tests would need to be appropriate to each agencies' (*sic*) specific operations. (For example, how long ago the information was collected, how often it was collected, and the general relevance of historical data - whether the information is up-to-date or not.)

IPP 10 limits the use of personal information. Agencies may not use personal information for purposes other than those for which it is collected unless one of the five exceptions apply.

To comply with this requirement agencies should be aware of the exceptions which authorise use of material collected by covert surveillance for purposes other than the purpose for which the material was collected. In particular agencies should note exception (e) in IPP 10.1, which authorises the use of information where "the purpose for which the information is used is directly related to the purpose for which the information was collected." Agencies should observe IPP 10.2 which requires that agencies keep a note of the uses of particular records where the information has been used for enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of the public revenue. IPP 11 limits disclosure of information outside an agency unless one of the five exceptions apply. IPP 11.2 requires agencies to keep a note of records that are disclosed for the enforcement of the criminal law or a law imposing a pecuniary penalty or for the protection of the public revenue.

Hence material collected by covert surveillance should not be disclosed to any person, body or agency other than in accordance with the IPPs. Agencies should be cognisant of the exceptions which authorise disclosure of information.

It is recommended that safeguards be in place to ensure that, where information is disclosed according to the IPPs, the information is only used or disclosed for the specific purpose for which it was collected. Agencies could consider formal agreements or memoranda of understanding with persons or agencies to whom information is disclosed.

Agencies should also be aware of any relevant secrecy provisions within their enabling legislation.

Retention and Destruction

No IPP directly applies here and the Archives Act is the principal control but the Privacy Commissioner reserves power to give advice on those matters if pertinent to security under IPP 4. It should be noted that information that is unnecessarily kept could be in breach of IPPs 7, 8, or 9.

Monitoring

Agencies should consider incorporating regular monitoring procedures on covert surveillance practices in their reviews of operational procedures/instructions. The Privacy Commissioner has powers under section 27 1(h) of the Privacy Act to conduct audits of agencies. (Further information on this is available in the Privacy Audit Manuals 1 and 2.)

Specific Guidelines for the Conduct of Covert Surveillance by Optical Means When Used for the Surveillance of Claimants for Compensation

These guidelines apply to the use by Commonwealth agencies of covert surveillance by optical means in cases involving compensation claims under the Commonwealth Employees' Rehabilitation and Compensation Act 1988.

1. DETERMINING THE NECESSITY FOR CONDUCTING COVERT SURVEILLANCE

1.1 Prior to undertaking covert surveillance the agency should assess the need to use this technique. Covert surveillance should only be used:

(a) When other less intrusive methods of investigation have been considered and have been assessed to be ineffective and inadequate; or have been tried and the outcome found to be inconclusive.

(b) When the claim is of such a nature as to warrant the use of

covert surveillance and when there is adequate evidence to suggest that the claimant may be:

- misrepresenting his/her disability,
- claiming excessive disabilities,
- malingering, or
- involved in the commission of a fraud.

1.2 Where the benefits arising from obtaining relevant information by covert surveillance are considered to outweigh to a substantial degree the intrusion on the privacy of the surveillance subject.

1.3 Where, if appropriate, the Australian Government Solicitor or other legal advisers have been consulted concerning the desirability or necessity of obtaining information by covert surveillance.

2. *APPLICATION TO CONDUCT COVERT SURVEILLANCE*

IPP 1 imposes obligations on Commonwealth agencies relating to the collection of personal information. Collection must be fair and lawful. The information collected must be for a lawful purpose which is directly related to the function or activity of the agency and the collection of information must be necessary for or directly related to that purpose.

2.1 An application to conduct covert surveillance should be in writing, and include a clear statement on the following:

(a) The purpose for the covert surveillance i.e. document the basis in terms of 1.1(b) above.

(b) The name, address, and other relevant details of the surveillance subject, including:

- the personal characteristics of the surveillance subject to minimise the risk of misidentification
- a description of the surveillance subject's premises e.g. a particular office location or building.

(c) The nature and details of the claim e.g. muscular-skeletal injuries.

(d) The kind of information to be collected by covert surveillance, including:

- the performance of physical activities that may indicate that the individual concerned is making a false claim e.g. ability to lift objects known to be very heavy.

(e) Whether alternative investigative methods have been considered/undertaken to obtain the information required and the results, if any, of these investigations.

Alternative methods may include:

- interviewing claimants
- interviewing witnesses
- reviewing agency records
- reviewing claimant's records.

(f) The relative cost/benefits of undertaking or not undertaking the surveillance, for example:

- an estimate of the financial or other resource costs of the surveillance
- whether the amounts involved in a worker's compensation claim warrant the costs involved in the covert surveillance.

(g) Particulars of the investigator undertaking the surveillance i.e. whether the covert surveillance is to be conducted by:

- departmental investigators
- contract private investigators.

(h) Whether the procedure has been recommended by the Australian Government Solicitor or relevant legal advisers.

(i) The method by which information is to be collected, for example:

- by photography
- by video recordings
- by recording of observations in a log
- by combinations of the above.

(j) The period and scope of the surveillance, including:

- surveillance period e.g. daily
- surveillance dates
- activities to be observed, e.g. gardening, lifting, shopping
- whether the surveillance is to be confined to the domestic environment or extended beyond the claimant's premises.

3. *APPROVAL TO CONDUCT COVERT SURVEILLANCE*

Covert Surveillance should normally be approved in writing on a case-by-case basis, at a senior level in the agency following a written application.

3.1 Approval to conduct covert surveillance in a particular case is only to be given by senior officers at an appropriate management level.

3.2 Approval is to be issued for a limited time only, as follows:

(a) The period of surveillance should be appropriate to the circumstances of each case, but should not extend beyond 30 continuous days. This period may be extended when there is difficulty locating the claimant.

(b) A new application should be made to extend or recommence covert surveillance after the expiry of the initial approval.

4. *THE COLLECTION PROCESS*

4.1 Covert surveillance should be undertaken by trained investigators/surveillance officers. Strict instructions on the conduct of covert surveillance should be issued to the surveillance officers. Points (a) to (d) are of a general nature whilst (e) and (f) are case specific. The instructions should cover:

(a) Avoidance of any actions which may unreasonably impinge on the privacy and rights of other people, e.g. when using photography, avoid, where practicable, including other individuals such as relatives and friends, who may be in contact with the surveillance subject during the surveillance period, in the photograph.

(b) Where practicable only material relevant to the purpose of conducting the covert surveillance should be collected. There should be a clear separation of facts from opinions and only relevant personal information should be included in records resulting from the surveillance.

(c) Instructions on the manner of collection of personal information.

- the collection should not involve the commission of a criminal offence or give rise to a civil action, for example, trespass to land or goods

- the collection should not involve entrapment of the claimant. Hence, passive observation is permissible, however, any attempts to actively induce the claimant into a situation in which that person would not ordinarily and voluntarily enter, thereby creating a false or misleading impression of the person's disabilities, should not be permitted.

(d) Instructions by agencies on obligations of investigators to safeguard the material collected. Agencies should include secrecy provisions in contracts employing private investigators.

(e) The method by which information is to be collected e.g. photography, video recordings or logs with observations recorded. This should be appropriate to the purpose of collection in the particular case.

(f) The period and scope of the surveillance procedure as specified in 2.1(j).

5. *USE AND DISCLOSURE*

5.1 Material collected by covert surveillance is to be used in accordance with the following conditions:

(a) The material is to be used only for the purpose for which the approval described under 3.1 is given, or where exceptions under IPP 10 apply, and

(b) Each agency should ensure that information is accurate, up to date and complete prior to the information being used. Material collected by covert surveillance should not be used in isolation but corroborated by other information to ensure accuracy.

Tests for accuracy may include:

- identity check, i.e. name and address of surveillance subject
- checking timing of the surveillance procedure
- verifying that material collected is consistent with 2.1(c)
- checking that there is no other reasonable explanation for the particular information collected such as:
  - . injured worker able to lift box because he/she was wearing a splint
  - . box lifted by injured worker was empty
  - . activity performed by worker did not involve using injured muscles.

5.2 Material collected by covert surveillance is not to be disclosed to another person, body or agency, other than in accordance with IPP 11.

5.3 When material is disclosed there should be a record of:

(a) The reason/s for disclosure.

(b) The recipient of the information.

(c) The officer authorising disclosure.

5.4 Disclosures for the purpose of enforcement of criminal law or revenue protection must be noted in the surveillance subject's record. (See IPP 11.2).

5.5 Where material is disclosed to another person, body or agency, safeguards should be in place to ensure that the information is only disclosed by the receiving agency or person in accordance with IPP 11. Agencies should consider formal agreements or memoranda of understanding with persons or agencies to whom the information is disclosed to ensure that an audit trail of information can be established for any subsequent use or disclosure.

6. STORAGE AND SECURITY

Agencies should put in place appropriate measures to protect the material against loss; unauthorised access, use, modification or disclosure by:

(a) Restricting access of material to relevant personnel on a "need to know" basis e.g. Comcare case manager.

(b) Storing the material in a secure area e.g. a locked file.

(c) Storing material separately to other routine administrative information about the surveillance subject.

(d) Maintaining a log of all personnel accessing, using or removing the material, in order to establish an audit trail.

7. MONITORING

7.1 Agencies should review their covert surveillance practices periodically. This review may include:

(a) An evaluation of compliance with the guidelines.

(b) A cost/benefit analysis to evaluate the use of covert surveillance as a means of achieving the agency's objectives and taking into account the surveillance subject's right to privacy.

7.2 Agencies should include in their annual reports a summary of the incidence of covert surveillance undertaken. This report should not contain personal information that may lead to identification of particular individuals.

7.3 Agencies should conduct ongoing monitoring of the conduct of covert surveillance and should provide training of staff involved in all aspects of covert surveillance.

APPENDIX F

Décret n°93-513 du 25 mars 1993 pris pour l'application de l'article 24 de la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications

Le Premier ministre, ministre de la défense,

Sur le rapport du garde des sceaux, ministre de la justice, et du ministre des postes et télécommunications;

Vu le code pénal, et notamment ses articles 186-1 et 368;

Vu la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, et notamment son article 24;

Le Conseil d'Etat (section des travaux publics) entendu,

Décrète:

Art. 1er. - La liste des appareils conçus pour intercepter ou détourner des correspondances émises, transmises ou reçues par la voie des télécommunications, ou pour utiliser ou divulguer leur contenu, dans des conditions rendant possible la réalisation de l'infraction prévue à l'article 186-1 du code pénal, est établie par arrêté ministériel.

Est également inscrit sur une liste déterminée par arrêté ministériel tout appareil conçu pour la détection à distance des correspondances, dont les caractéristiques permettent d'écouter, d'enregistrer ou de transmettre des paroles prononcées dans un lieu privé par une personne sans le consentement de celle-ci.

Art. 2. - Ces arrêtés sont pris par le ministre chargé des télécommunications après avis d'une commission consultative placée auprès de lui et comprenant:

1. Un représentant du ministre chargé des télécommunications, président;

2. Un représentant du ministre de l'intérieur;
2. Un représentant du ministre de la défense;
4. Un représentant du ministre chargé des douanes;
5. Un représentant du ministre chargé de l'industrie;
6. Quatre personnalités choisies en raison de leur compétence désignées par le ministre chargé des télécommunications.

La commission peut entendre, à titre d'expert, toute personne compétente.

Elle est saisie pour avis de tout projet de modification des listes visées ci-dessus. Elle peut également formuler des propositions de modification de ces listes.

Art. 3. - Nul ne peut fabriquer, importer, exposer, offrir, louer ou vendre l'un des appareils figurant sur les listes visées à l'article 1er s'il n'y a été préalablement autorisé par le ministre chargé des télécommunications.

Art. 4. - La demande d'autorisation est déposée auprès du ministre chargé des télécommunications. Elle comporte pour chaque type d'appareil:

(a) Le nom et l'adresse du demandeur, s'il est une personne physique, ou sa dénomination, sa raison sociale et son siége social, s'il est une personne morale;

(b) La où les opérations mentionnées à l'article 3 pour lesquelles l'autorisation est demandée et, le cas échéant, la description des marchés visés;

(c) L'objet et les caractéristiques techniques du type de l'appareil, accompagnés d'une documentation technique;

(d) Le lieu prévu pour la fabrication de l'appareil ou pour les autres opérations mentionnées à l'article 3;

(e) L'engagement de se soumettre aux contrôles nécessaires à la vérification du respect des indications fournies dans la demande d'autorisation.

Art. 5. - L'autorisation visée à l'article 3 est délivrée pour une durée maximale de six ans.

Elle peut fixer les conditions de réalisation de l'opération et le nombre des appareils concernés.

Art. 6. - Chaque appareil fabriqué, importé, exposé, offert, loué ou vendu doit porter la référence du type correspondant à la demande d'autorisation et un numéro d'identification individuel.

Art. 7. - L'acquisition ou la détention de tout appareil figurant sur les listes visées

à l'article 1er est soumise à une autorisation délivrée par le ministre chargé des télécommunications.

Art. 8. - La demande d'autorisation est déposée auprès du ministre chargé des télécommunications. Elle comporte pour chaque type d'appareil:

(a) Le nom et l'adresse du demandeur, s'il est une personne physique, ou sa dénomination, sa raison sociale et son siège social, s'il est une personne morale;

(b) Le type d'appareil et le nombre d'appareils pour la détention desquels l'autorisation est demandée;

(c) L'utilisation prévue.

Art. 9. - L'autorisation visée à l'article 7 est délivrée pour une durée maximale de trois ans.

Elle peut subordonner l'utilisation des appareils à des conditions destinées à en éviter tout usage abusif.

Art. 10. - Les titulaires de l'une des autorisations mentionées à l'article 3 ne peuvent proposer, céder, louer ou vendre les appareils figurant dans la liste visée à l'article 1er qu'au titulaire de l'une des autorisations visées à l'article 3 ou à l'article 7.

Ils tiennent un registre retraçant l'ensemble des opérations relatives à ces matériels, conforme au modèle ci-joint.

Art. 11. - Les autorisations prévues à l'article 3 et à l'article 7 peuvent être retirées:

1. En cas de fausse déclaration ou de faux renseignement;
2. En cas de modification des circonstances au vu desquelles l'autorisation a été délivrée;
3. Lorsque le bénéficiaire de l'autorisation n'a pas respecté les dispositions du présent décret ou les obligations particulières prescrites par l'autorisation;
4. Lorsque le bénéficiaire de l'autorisation cesse l'exercice de l'activité pour laquelle a été délivrée l'autorisation.

Le retrait ne peut intervenir, sauf urgence, qu'après que le titulaire de l'autorisation a été mis à même de faire valoir ses observations.

Les autorisations prennent fin de plein droit en cas de condamnation du titulaire au titre des articles 186-1 ou 368 du code pénal.

Art. 12. - Les personnes qui détiennent, fabriquent, importent, exposent, offrent,

louent ou vendent des appareils figurant sur les listes prévues à l'article 1er doivent se mettre en conformité avec les prescriptions du présent décret en sollicitant les autorisations nécessaires dans un délai de trois mois à compter de la publication de l'arrêté prévu à l'article 1er.

Art. 13. - Le garde des sceaux, ministre de la justice, le ministre de l'intérieur et de la sécurité publique, le ministre de l'économie et des finances, le ministre de l'industrie et du commerce extérieur, le ministre du budget, le ministre des postes et télécommunications et le ministre délégué au commerce et à l'artisanat sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 25 mars 1993.

REGISTRE

Renseignements concernant les appareils				Renseignements concernant la cession			
Type de l'appareil, catégorie prévue par l'arrêté	Description sommaire	Référence de l'appareil à l'achat (1)	Date d'entrée en stock	Identité (2) du fournisseur (3) (fabricant, importateur ou vendeur)	Identité de l'acquéreur (2)	Référence et date de délivrance de l'autorisation de l'acquéreur	Date de sortie du stock et signature de l'acquéreur

(1): Référence du type correspondant à la demande d'autorisation, numéro d'identification individuel de l'appareil.
(2): Personne physique: nom et adresse.
Personne morale: dénomination, raison sociale et siège social.
(3): Référence et date de l'autorisation du fournisseur.

THE LAW REFORM COMMISSION
Ardilaun Centre
111 St Stephen's Green
Dublin 2

Telephone: 671 5699
Fax No.: 671 5316

LIST OF LAW REFORM COMMISSION'S PUBLICATIONS

First Programme for Examination of Certain Branches of the Law with a View to their Reform (Dec 1976) (Prl. 5984) **[out of print]** [10p Net]

Working Paper No. 1-1977, The Law Relating to the Liability of Builders, Vendors and Lessors for the Quality and Fitness of Premises (June 1977) [£ 1.50 Net]

Working Paper No. 2-1977, The Law Relating to the Age of Majority, the Age for Marriage and Some Connected Subjects (Nov 1977) [£ 1.00 Net]

Working Paper No. 3-1977, Civil Liability for Animals (Nov 1977) [£ 2.50 Net]

First (Annual) Report (1977) (Prl. 6961) [40p Net]

Working Paper No. 4-1978, The Law Relating to Breach of Promise of Marriage (Nov 1978) [£ 1.00 Net]

Working Paper No. 5-1978, The Law Relating to Criminal Conversation and the Enticement and Harbouring of a Spouse (Dec 1978) [£ 1.00 Net]

Working Paper No. 6-1979, The Law Relating to Seduction and the Enticement and Harbouring of a Child (Feb 1979) [£ 1.50 Net]

Working Paper No. 7-1979, The Law Relating to Loss of Consortium and Loss of Services of a Child (March 1979) [£ 1.00 Net]

Working Paper No. 8-1979, Judicial Review of Administrative Action: the Problem of Remedies (Dec 1979) [£ 1.50 Net]

Second (Annual) Report (1978/79) (Prl. 8855) [75p Net]

Working Paper No. 9-1980, The Rule Against Hearsay (April 1980) [£ 2.00 Net]

Third (Annual) Report (1980) (Prl. 9733) [75p Net]

First Report on Family Law - Criminal Conversation, Enticement and Harbouring of a Spouse or Child, Loss of Consortium, Personal Injury to a Child, Seduction of a Child, Matrimonial Property and Breach of Promise of Marriage (LRC 1-1981) (March 1981) [£ 2.00 Net]

Working Paper No. 10-1981, Domicile and Habitual Residence as Connecting Factors in the Conflict of Laws (Sep 1981) [£ 1.75 Net]

Fourth (Annual) Report (1981) (Pl. 742) [75p Net]

Report on Civil Liability for Animals (LRC 2-1982) (May 1982) [£ 1.00 Net]

Report on Defective Premises (LRC 3-1982) (May 1982) [£ 1.00 Net]

Report on Illegitimacy (LRC 4-1982) (Sep 1982) [£ 3.50 Net]

Fifth (Annual) Report (1982) (Pl. 1795) [75p Net]

Report on the Age of Majority, the Age for Marriage and Some Connected Subjects (LRC 5-1983) (April 1983) [£ 1.50 Net]

Report on Restitution of Conjugal Rights, Jactitation of Marriage and Related Matters (LRC 6-1983) (Nov 1983) [£ 1.00 Net]

Report on Domicile and Habitual Residence as Connecting Factors in the Conflict of Laws (LRC 7-1983) (Dec 1983) [£ 1.50 Net]

Report on Divorce a Mensa et Thoro and Related Matters (LRC 8-1983) (Dec 1983) [£ 3.00 Net]

Sixth (Annual) Report (1983) (Pl. 2622) [£ 1.00 Net]

Report on Nullity of Marriage (LRC 9-1984 (Oct 1984) [£ 3.50 Net]

Working Paper No. 11-1984, Recognition of Foreign Divorces and Legal Separations (Oct 1984) [£ 2.00 Net]

Seventh (Annual) Report (1984) (Pl. 3313) [£ 1.00 Net]

Report on Recognition of Foreign Divorces and Legal Separations (LRC 10-1985) (April 1985) [£ 1.00 Net]

Report on Vagrancy and Related Offences (LRC 11-1985) (June 1985) [£ 3.00 Net]

Report on the Hague Convention on the Civil Aspects of International Child Abduction and Some Related Matters (LRC 12-1985) (June 1985) [£ 2.00 Net]

Report on Competence and Compellability of Spouses as Witnesses (LRC 13-1985) (July 1985) [£ 2.50 Net]

Report on Offences Under the Dublin Police Acts and Related Offences (LRC 14-1985) (July 1985) [£ 2.50 Net]

Report on Minors' Contracts (LRC 15-1985) (August 1985) [£ 3.50 Net]

Report on the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (LRC 16-1985) (August 1985) [£ 2.00 Net]

Report on the Liability in Tort of Minors and the Liability of Parents for Damage Caused by Minors (LRC 17-1985) (Sep 1985) [£ 3.00 Net]

Report on the Liability in Tort of Mentally Disabled Persons (LRC 18-1985) (Sep 1985) [£ 2.00 Net]

Report on Private International Law Aspects of Capacity to Marry and Choice of Law in Proceedings for Nullity of Marriage (LRC 19-1985) (Oct 1985) [£ 3.50 Net]

Report on Jurisdiction in Proceedings for Nullity of Marriage, Recognition of Foreign Nullity Decrees, and the Hague Convention on the Celebration and Recognition of the Validity of Marriages (LRC 20-1985) (Oct 1985) [£ 2.00 Net]

Eighth (Annual) Report (1985) (Pl. 4281) [£ 1.00 Net]

Report on the Statute of Limitations: Claims in Respect of Latent Personal Injuries (LRC 21-1987) (Sep 1987) [£ 4.50 Net]

Consultation Paper on Rape (Dec 1987) [£ 6.00 Net]

Report on the Service of Documents Abroad re Civil Proceedings - the Hague Convention (LRC 22-1987) (Dec 1987) [£ 2.00 Net]

Report on Receiving Stolen Property (LRC 23-1987) (Dec 1987) [£ 7.00 Net]

Ninth (Annual) Report (1986-1987) (Pl 5625) [£ 1.50 Net]

Report on Rape and Allied Offences (LRC 24-1988) (May 1988) [£ 3.00 Net]

Report on the Rule Against Hearsay in Civil Cases (LRC 25-1988) (Sep 1988) [£ 3.00 Net]

Report on Malicious Damage (LRC 26-1988) (Sep 1988) [£ 4.00 Net]

Report on Debt Collection: (1) The Law Relating to Sheriffs (LRC 27-1988) (Oct 1988) [£ 5.00 Net]

Tenth (Annual) Report (1988) (Pl 6542) [£ 1.50 Net]

Report on Debt Collection: (2) Retention of Title (LRC 28-1989) (April 1989) [£ 4.00 Net]

Report on the Recognition of Foreign Adoption Decrees (LRC 29-1989) (June 1989) [£ 5.00 Net]

Report on Land Law and Conveyancing Law: (1) General Proposals (LRC 30-1989) (June 1989) [£ 5.00 Net]

Consultation Paper on Child Sexual Abuse (August 1989) [£10.00 Net]

Report on Land Law and Conveyancing Law: (2) Enduring Powers of Attorney (LRC 31-1989)(Oct 1989) [£ 4.00 Net]

Eleventh (Annual) Report (1989) (Pl 7448) [£ 1.50 Net]

Report on Child Sexual Abuse (September 1990) (LRC 32-1990) **[out of print]** [£ 7.00 Net]

Report on Sexual Offences Against the Mentally Handicapped (September 1990) (LRC 33-1990) [£ 4.00 Net]

Report on Oaths and Affirmations (LRC 34-1990) (December 1990) [£ 5.00 Net]

Report on Confiscation of the Proceeds of Crime (LRC 35-1991) (January 1991) [£ 6.00 Net]

Consultation Paper on the Civil Law of Defamation (March 1991) [£20.00 Net]

Report on the Hague Convention on Succession to the Estates of Deceased Persons (LRC 36-1991) (May 1991) [£ 7.00 Net]

Twelfth (Annual) Report (1990) (PI 8292) [£ 1.50 Net]

Consultation Paper on Contempt of Court (July 1991) [£20.00 Net]

Consultation Paper on the Crime of Libel (August 1991) [£11.00 Net]

Report on The Indexation of Fines (LRC 37-1991) (October 1991) [£ 6.50 Net]

Report on The Civil Law of Defamation (LRC 38-1991) (December 1991) [£ 7.00 Net]

Report on Land Law and Conveyancing Law: (3) The Passing of Risk from Vendor to Purchaser (LRC 39-1991) (December 1991); (4) Service of Completion Notices (LRC 40-1991) (December 1991) [£ 6.00 Net]

Report on The Crime of Libel (LRC 41-1991) (December 1991) [£ 4.00 Net]

Report on United Nations (Vienna) Convention on Contracts for the

International Sale of Goods 1980 (LRC 42-1992) (May 1992) [£ 8.00 Net]

Thirteenth (Annual) Report (1991) (PI 9214) [£ 2.00 Net]

Report on The Law Relating to Dishonesty (LRC 43-1992) (September 1992) [£20.00 Net]

Land Law and Conveyancing Law: (5) Further General Proposals (LRC 44-1992) (October 1992) **[out of print]** [£ 6.00 Net]

Consultation Paper on Sentencing (March 1993) [£20.00 Net]

Consultation Paper on Occupiers' Liability (June 1993) **[out of print]** [£10.00 Net]

Fourteenth (Annual) Report (1992) (PN.0051) [£ 2.00 Net]

Report on Non-Fatal Offences Against The Person (LRC 45-1994) (February 1994) [£20.00 Net]

Consultation Paper on Family Courts (March 1994) [£10.00 Net]

Report on Occupiers' Liability (LRC 46-1994) (April 1994) [£ 6.00 Net]

Report on Contempt of Court (LRC 47-1994) (September 1994) [£10.00 Net]

Fifteenth (Annual) Report (1993) (PN.1122) [£ 2.00 Net]

Report on The Hague Convention Abolishing the Requirement of Legalisation for Foreign Public Documents (LRC 48-1995) (February 1995) [£10.00 Net]

Consultation Paper on Intoxication as a Defence to a Criminal Offence (February 1995) [£10.00 Net]

Report on Interests of Vendor and Purchaser in Land during period between Contract and Completion (LRC 49-1995) (April 1995) [£ 8.00 Net]

Sixteenth (Annual) Report (1994) (PN. 1919) [2.00 Net]

Report on An Examination of The Law of Bail (LRC 50-1995) (August 1995) [£10.00 Net]

Report on Intoxication (LRC 51-1995) (November 1995) [£ 2.00 Net]

Report on Family Courts (LRC 52-1996) (March 1996) [£10.00 Net]

Seventeenth (Annual) Report (1995) (P.N. 2960) [£ 2.50 Net]

Report on Sentencing (LRC 53-1996) (August 1996) [£ 8.00 Net]