

THE LAW REFORM COMMISSION
AN COIMISIÚN UM ATHCHÓIRIÚ AN DLÍ
(LRC 57-1998)

REPORT ON
PRIVACY:
Surveillance and
the Interception of Communications

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

© Copyright
First Published

The Law Reform Commission 1998
June 1998

ISSN 1393-3132

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;
Ms Hilary A Delany, B.L., Lecturer in Law, Trinity College, Dublin;
The Right Honourable Dr Turlough O'Donnell, Q.C.;
Mr Arthur F Plunkett, Barrister-at-Law;
Ms Patricia T Rickard-Clarke, Solicitor, Partner, McCann Fitzgerald Solicitors.

John Quirke is the 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 six Reports containing proposals for the reform of the law. It has also published eleven Working Papers, twelve Consultation Papers, a number of specialised Papers for limited circulation and eighteen Reports in accordance with Section 6 of the 1975 Act. Details may be found on pp.265-270.

Dr Gerard Quinn, B.A., LL.B., LL.M. (Harv.), S.J.D. (Harv.), Barrister-at-Law, is the Director of Research.

Mr Geoff Moore, B.C.L., Ms Lia O'Hegarty, B.C.L., LL.M. (Mich.), LL.M. (Harv.), Barrister-at-Law, and Ms Róisín Pillay, LL.B., LL.M (Cantab.), Barrister-at-Law, are Researchers.

Ms Mary Teresa Faherty, Ms Dympna Forde and Ms Deborah Parkes are the Administrative Staff.

Further information from:

The Secretary,
The Law Reform Commission,
Ardilaun Centre,
111 St. Stephen's Green,
Dublin 2.
Telephone: 475 1310.
Fax No: 475 1265.
Email: ircsecretary@tinet.ie.

The Law Reform Commission

AN COIMISIÚN UM ATHCHÓIRIÚ AN DLÍ

ARDILAUN CENTRE
111 ST. STEPHEN'S GREEN
DUBLIN 2
IRELAND
TELEPHONE (01) 475 1310
FAX (01) 475 1265

30th June 1998

An Taoiseach Bertie Ahern, T.D.,
Office of the Taoiseach,
Government Buildings,
Dublin 2.

Dear Taoiseach,

Pursuant to the provisions of the *Law Reform Commission Act, 1975*, I have the honour to transmit to you herewith the Commission's Report on **Privacy: Surveillance and the Interception of Communications** (LRC 57-1998).

The Commission proposes to publish this Report in the near future.

Yours sincerely,


ANTHONY J. HEDERMAN
PRESIDENT

Encl.

TABLE OF CONTENTS	PAGE
CHAPTER 1: OVERVIEW	1-23
<i>A. The Background to this Report</i>	1
Introduction	1
1. Why Privacy is Worthy of Legal Protection in a Democratic Society	2
2. The Dangers Posed by New Technology	5
3. The Inadequacy of Existing Irish Law	7
4. The Need for Law Reform	10
<i>B. Overview of Report</i>	12
5. Objective - Protecting Reasonable Expectations of Privacy against Surveillance	12
6. Privacy and the Public Interest, Including Freedom of Expression	13
7. The Conformity of Our Recommendations with the European Convention on Human Rights	15
8. Privacy in the Global Village - The International Dimension	15
9. Overview of Recommendations	18
(a): Civil Law Reform	19
(b): The Enactment of New Criminal Offences	20
(c): The Provision of New Regulatory Safeguards	20
(d): Miscellaneous Technical Recommendations	22
10. Outline of Report	22

Part I - General

CHAPTER 2: WHAT WE MEAN BY PRIVACY AND WHAT WE MEAN BY THE PUBLIC INTEREST	24-39
<i>A. What We Mean By Privacy</i>	24
1. General	24
2. Factors Relevant to a "Reasonable Expectation" of Privacy	26
3. The Non-Exhaustive Nature of the Indicators	31
<i>B. What We Mean By The Public Interest</i>	32
1. The Emergence and Authority of the "Public Interest" Concept	32

	TABLE OF CONTENTS	PAGE
2.	Our View as to the Public Interest in Disclosure of Information Obtained by Surveillance	35
	(a) Elements of the Public Interest	35
	(b) Qualifications to the Public Interest Defence	37
 CHAPTER 3: THE PRIVACY PROBLEM AND THE INADEQUACY OF EXISTING LAW IN IRELAND		40-62
1.	The Existence of a Privacy Problem	40
2.	The Constitutional Template	43
	<i>The Constitutional Right of Privacy</i>	43
	<i>Surveillance in Constitutional Litigation</i>	47
	<i>Conclusion</i>	48
3.	The Inadequacy of Domestic Law	49
	(a) Existing Civil Law Protections	49
	(b) Existing Criminal Law Protections	51
	(c) Data Protection Legislation	53
	(d) Freedom of Information Legislation	57
	(e) Broadcasting Regulation	58
	(f) Non-Statutory Codes of Practice	59
4.	Summary	62
 CHAPTER 4: IS LEGISLATION CALLED FOR ?		63-72
1.	General	63
2.	The Arguments Against a Legislative Solution	63
	i. <i>Should the Market - Not the Law - Determine Boundaries ?</i>	63
	ii. <i>Is Self-Regulation Sufficient ?</i>	64
	iii. <i>Is the Concept of Privacy Amenable to Legislative Expression ?</i>	66
	iv. <i>Can the Law Provide an Adequate Balance between Privacy and other Competing Rights and Interests ?</i>	68
	v. <i>Is Privacy Legislation Futile ?</i>	69
	vi. <i>Will Privacy Legislation be Exploited by Powerful Parties?</i>	69
3.	The Report of the Commission on the Newspaper Industry (the Finlay Report) Considered	70
4.	Conclusions	71

TABLE OF CONTENTS**PAGE****Part II - International Benchmarks for Reform**

CHAPTER 5: THE PROPOSED PRIVACY LEGISLATION AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS	73-81
1. Article 8 - Right to Respect for "Private Life"	73
2. Article 10 - Freedom of Expression and its Implications for Privacy Legislation	76
3. Conclusions	80
CHAPTER 6: THE PROTECTION OF PRIVACY IN COMPARATIVE LAW	82-100
1. Civil Liability for Surveillance	82
Germany	83
France	83
United States	83
Canada	84
New Zealand	84
2. Civil Liability for "Intrusion" on Privacy through Publication	85
Germany	85
France	86
Canada	87
United States	88
3. Criminal Liability for Invasions of Privacy	88
Germany	88
France	89
Denmark	90
Australia	90
Norway	91
4. Regulatory Safeguards	92
Denmark	92
Sweden	93
Norway	94
France	95
5. Due Process Protections of Covert Police Surveillance	96
Norway	96
Sweden	96
Australia	97
United Kingdom	98
6. Conclusions	99

TABLE OF CONTENTS

PAGE

Part III - Recommendations

CHAPTER 7: CORE RECOMMENDATION - THE CREATION OF CIVIL LIABILITY FOR PRIVACY-INVASIVE SURVEILLANCE AND HARASSMENT	101-106
A: Core Recommendation - The Enactment of a Tort of Privacy-Invasive Surveillance	101
B: Subsidiary Recommendation - The Enactment of a Tort of Harassment	103
C: Defences	103
D: Remedies	104
E: Technical Aspects of the New Torts	105
CHAPTER 8: MAIN ANCILLARY RECOMMENDATIONS - THE CREATION OF CIVIL LIABILITY FOR THE DISCLOSURE, DISSEMINATION OR PUBLICATION OF INFORMATION OR MATERIAL OBTAINED AS A RESULT OF PRIVACY-INVASIVE SURVEILLANCE OR HARASSMENT	107-109
A: Proposed New Torts of Disclosure of Material Obtained by Surveillance or Harassment	107
B: Defences	107
C: Remedies	108
CHAPTER 9: PROPOSED CRIMINAL, REGULATORY AND SUPPLEMENTARY PROVISIONS	110-118
Introduction	110
A: Proposed New Offences	110
B: Defences	113
C: Regulatory Provisions Directed at Particular Forms of Surveillance by State Authorities and Others	114
D: The Power of the Courts to Hold Proceedings <i>In Camera</i> or to Restrain Publication Relating to Proceedings	117
E: Technical Amendments of the Postal and Telecommunications Legislation	117
F: Miscellaneous	118

TABLE OF CONTENTS	PAGE
CHAPTER 10: PROPOSED HEADS OF A BILL TO PROTECT THE INDIVIDUAL FROM PRIVACY-INVASIVE SURVEILLANCE	119-164

Annexes

ANNEX I: PRIVACY AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS	165-222
ANNEX II: EVOLUTION OF THE PRIVACY DEBATE IN THE UNITED KINGDOM	223-245
ANNEX III: DATA PROTECTION LAW AND THE USE OF CCTV	246-251
ANNEX IV: THE POWER OF THE COURTS TO HOLD PROCEEDINGS <i>IN CAMERA</i> OR TO RESTRAIN PUBLICATION RELATING TO PROCEEDINGS	252-257
ANNEX V: RESOLUTION ON PRIVACY OF THE PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE	258-261
ANNEX VI: LIST OF PERSONS FROM WHOM WRITTEN SUBMISSIONS HAVE BEEN RECEIVED	262
ANNEX VII: LIST OF PERSONS WHO PARTICIPATED AT OUR LISTENING EXERCISE	263
LIST OF LAW REFORM COMMISSION PUBLICATIONS	265-270

CHAPTER 1: OVERVIEW

"Watching people against their will... forces them to see themselves and their plans through the eyes of another, as object rather than subject, undermining their self-respect and evincing a lack of respect for their freedom to make choices without pressure from the outside." ¹

A. THE BACKGROUND TO THIS REPORT

Introduction

1.1 *This Report contains the Law Reform Commission's final recommendations with respect to privacy in the specific context of surveillance and the interception of communications. This Report does not cover the entire sweep of privacy but focuses on one discrete aspect, namely the invasion of privacy through surveillance and interception. While this Report covers in a general way the privacy problem posed by surveillance in all contexts it does not address the peculiarities that may arise in highly specific contexts such as employment, healthcare and the prison system. These areas pose additional and discrete problems best addressed /separately and later.*

1.2 *This Report should be read against the backdrop of the extensive comparative research and provisional recommendations contained in our Consultation Paper on the subject which was issued in September 1996². What that research revealed above all else was the growing nature of the problem of surveillance in contemporary society, the inadequacy of existing law and a trend toward the adoption of legislative solutions³.*

1.3 *Privacy is listed as one of the Commission's main areas of review in its Programme of Work⁴ and this Report should therefore be seen as one element of work under that Programme on the general privacy issue.*

1 David Feldman, *Privacy as a Civil Liberty*, 47 *Current Legal Problems* (1994) 41 at p. 62 (paraphrasing S.I. Benn).

2 Law Reform Commission, *Consultation Paper on Privacy: Surveillance and the Interception of Communication* (1996) ISSN 1383-3140, hereinafter 'our Consultation Paper'.

3 See generally chapters 8, 10, and 11 of the Consultation Paper and for a summary see chapter 6 of this Report.

4 First Programme for Examination of Certain branches of the Law with a view to their Reform, Ptl. 5984, 1977 at para 13.

1.4 In brief, our **core recommendation** is for the enactment of a civil tort directed against acts of privacy-invasive surveillance in circumstances where a "reasonable expectation" of privacy exists. We also make **another recommendation** for the enactment of a new but related civil tort of harassment. These torts would be directed to infringements of the privacy of natural (i.e. human) persons, not of bodies corporate, though (as pointed out by the European Court of Human Rights) this does not mean that infringements of the privacy of natural persons cannot occur in a corporate setting.

1.5 Our **main ancillary recommendation** is for the enactment of a related civil tort directed against the unjustified disclosure through publication or otherwise of information, images, etc., obtained as a result of the tort of unlawful surveillance or harassment. This does not amount to a full privacy law as conventionally understood - a prohibition on the publication of all manner of private material. Rather, the ambit of our ancillary recommendation builds on our main recommendation which is aimed at surveillance and interception. We make provision for a public interest defence to the tort of disclosure of information obtained as a result of unlawful surveillance.

1.6 With respect to **criminal law** we recommend that sanctions should be limited and confined to the most outrageous forms of intrusion in circumstances where the expectation of privacy is at its highest (in a dwelling) or where the activity in question is inherently private (e.g. private conversations), with supplementary prohibition of disclosure of information obtained by means of infringements of these provisions. Consistent with these recommendations we also propose an offence of trespass on private property effected for the purpose of obtaining personal information.

1.7 Lastly we make several specific recommendations with respect to **regulatory safeguards** in the context of certain types of surveillance of both public and private places conducted by the Gardaí and certain types of self-protective surveillance by owners or occupiers of premises, and other miscellaneous technical matters including the amendment of existing legislation.

1.8 To facilitate understanding of our recommendations we provide in Chapter 10 a detailed draft **Heads of Bill** setting out the new statutory torts and criminal sanctions we envisage together with explanatory notes for the Heads.

1. **Why Privacy is Worthy of Legal Protection in a Democratic Society**

1.9 Why is privacy so important? The distinctive feature of this Report is that it is animated throughout by a human rights approach to privacy. Privacy is not merely instrumental⁵ to the achievement of other goals but is a basic human right that applies to all persons in virtue of their status as human beings.

5 See generally Charles Fried, *Privacy*, 77 Yale L.J. 475 (1968).

It is not possible to overstate just how fundamental privacy is in a developed and civilised legal system. A sense of its importance can be gleaned by rehearsing briefly some of the many important overlapping values that are served by it⁶.

1.10 **First**, privacy is closely connected to notions of inherent human dignity. The intimacies of private life go to the very core of what it means to be human. Privacy is therefore worthwhile in itself in protecting human personality or the inherent dignity of the person⁷. This is reflected in what the European Court of Human Rights refers to as the "physical and moral integrity"⁸ of the person.

1.11 **Secondly**, privacy is closely related to human freedom, autonomy and self-determination. Privacy provides vital space for personal growth and development and for the exercise of freedom. Human beings are not means to the ends of others but are ends in themselves and are free to choose their own goals in life. Self-determination means, in part, the freedom to select which aspects of one's personality should be shared with others and on what terms. Central to autonomy and the selection of personal life-choices is freedom from coercion and manipulation and the preservation of space for emotional release, self-evaluation and growth. This explains why privacy is so closely connected to the protection of human personality found in many constitutions including that of Germany. As the European Commission on Human Rights expressed this point:

"[private life] is of such a scope as to secure to the individual a sphere within which he can freely pursue the development and fulfilment of his personality."⁹

1.12 The pursuit of private goals will often involve the formation of voluntary relations with others of varying degrees of intimacy. As the European Commission pointed out, privacy therefore entails the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality¹⁰. Another way of looking at this is that privacy is necessary to give efficacy to the exercise of many different liberty interests including freedom of association.

6 For a compendium of the most significant works in the field see the International Library of Essays in Law & Legal Theory, Vols. I & II, Raymond Wacks (Ed.), *Privacy* (Dartmouth, 1993). See also Ferdinand Schoeman (Ed.), *Philosophical Dimensions of Privacy: an Anthology* (Cambridge University Press, 1984); and Julie C. Innes *Privacy, Intimacy and Isolation* (Oxford University Press, 1992). For an evaluation of the relative merits of the theories of privacy see Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*, (Cornell U. Press, 1997).

7 See generally Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. Law Rev. 34 (1967).

8 See, e.g., judgment of the European Court of Human Rights in *X & Y v. The Netherlands*, (1985) 8 E.H.R.R. 235 at para 22 (private life is a concept which covers the physical and moral integrity of the person, including his or her sexual life).

9 *Bruggeman & Scheuten v Germany*, Report of the European Commission on Human Rights, 5 DR, 100 at para 55.

10 *X v. Iceland*, Decision of the European Commission on admissibility, 5 DR, 86 at p. 87.

1.13 **Thirdly**, privacy is much more than a tool for protecting the seclusion of the individual. It is an organising principle of civil society¹¹. Although man is a social animal and not a hermit, an orderly civil society is itself impossible without some sanctuaries away from everyday life. Privacy is at the heart of the implicit social contract in every society by which the terms of peaceful co-existence are set¹². In short, privacy entails much more than the protection of the person in seclusion; it is a way or organising society.

1.14 **Fourthly**, privacy is closely connected to the democratic life of the polity. This is so in at least two senses. First, democratic theory itself points strongly to the need for personal space. This is so because democracy rests on - and is bounded by - the dignity and equal inherent self-worth of all human beings. Democracy is not merely a process but also a value system. Secondly, an assurance of some secluded space away from public gaze is necessary to provide reassurance to those who have a contribution to make and who wish to enter public life.

1.15 Privacy is important for all these reasons and is therefore indispensable to the full flourishing of the human personality in a free society. We stress that while personal space is at its most visible in "private places" or on private property, it is not premised on, nor is it limited to, conceptions of property. Indeed, the chief deficiency of much existing law is that it tends to protect privacy - if at all - through property and through legal tools that protect property interests. Considering the values honoured by privacy, as set out above, one may have a "reasonable expectation" of privacy in many different contexts. It follows, in our view, that there may well be a residuum of privacy or a "reasonable expectation" of privacy even in a public place. This view accords with the overall approach being adopted by the European Commission and Court of Human Rights in interpreting Article 8 of the European Convention on Human Rights¹³.

1.16 Since privacy is so deeply connected to the inner sanctum of the person its violation can inflict deep and raw wounds and leave lasting damage. Intrusion into personal space can often be fairly characterised as a violation of the person. Furthermore - and due to the value and role of privacy in an orderly civil and democratic society - one person's loss of privacy is almost always of some broader social significance. In an important sense, one person's loss is every person's loss since it tears away at the terms of peaceful co-existence in society. Cumulatively such losses jeopardise every person's privacy and cannot be long ignored in democratic society.

11 See generally, Jack Hirshleifer, *Privacy: its Origin, Function and Future*, 9 J. of Legal Studies, 649 (1980); and Ferdinand Schoeman, *Privacy and Social Freedom* (Cambridge University Press, 1992).

12 See, e.g., Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Calif. L. Rev. (1989) 957.

13 See e.g., *Halford v. United Kingdom*, Judgment of the Court, 24 E.H.H.R. (1997) 523 at para. 45 (conclusion that there had been a 'reasonable expectation of privacy' with respect to the use of an office telephone on the facts of the case).

2. The Dangers Posed by New Technology

1.17 Does surveillance pose a threat to privacy and, if so, how grave is the threat today? We believe that there is a privacy problem arising out of surveillance and that it is grave enough to warrant a legislative response. Two factors explain why there is a privacy problem in this regard today in Ireland:

(1) the technological revolution of the past few decades and the widespread availability of such technology,

(2) the move toward an information-based culture where many actors have a growing interest in gathering information about others through, *inter alia*, various techniques of surveillance.

1.18 Such an information-gathering interest may range from the perfectly legitimate (e.g., prevention and detection of crime by the Gardaí) to the utterly depraved (e.g., voyeurism) with many shades of grey in between.

1.19 The technological breakthroughs have been spectacular. It is surprising if not shocking to learn of the ease with which this technology can pry open personal space which may previously have been considered safe. Specific examples of listening and optical surveillance devices which are generally available were listed by the Australian Law Commission as long ago as 1983. The gravity of surveillance as a threat to personal privacy in today's world can be understood from considering the following list:

- parabolic microphones with ranges extending to more than 250 metres,
- miniature tape-recorders which can be concealed inside, for example, cigarette packets,
- binoculars having built-in cartridges,
- listening devices laminated onto business cards,
- brief-case cameras, activated by pressing a button on the briefcase,
- residual light image intensifiers with ranges of up to 10 kilometres for long range 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 use¹⁴.

1.20 Indeed, the range and sophistication of technological devices which can be used for surveillance purposes have increased substantially since the Australian Law Reform Commission studied the topic of privacy, and technological innovation continues at an amazing rate. We pointed this out in our Consultation Paper and gave the following examples of recently developed surveillance devices:

- small video cameras which can be held in the palm of one's hand, and
- an artificial "eye" which, by a combination of optical computing and neural networking, can "learn" to recognise objects in a way which mimics human sight.¹⁵

1.21 More recently, surveillance technology is reportedly being developed using systems that can operate outside the visible light spectrum, such as:

- Forward-Looking Infra-Red systems which are able to detect human activity behind walls¹⁶ and
- Computerised Face Recognition technology which will enable the matching of an image on the street and a file on a database.

1.22 The next development in the technology will reportedly involve the development of an interactive link between surveillance technology and computerised data banks (CCTV surveillance networks). This will potentially allow for automatic tracking of the movements of individuals.¹⁷ Technology is

14 Australian Law Commission, *Report on Privacy*, 1983, No. 22, at para 94.

15 *op. cit.*, pp. 10-11.

16 See, e.g., S J Smith, *Thermal Surveillance and the Extraordinary Device Exception: Re-Defining the Scope of the Katz Analysis*, 30 *Valparaiso U. L. Rev.* 1071 (1996); M A Lanning, *Thermal Surveillance: Do Infrared Eyes in the Sky Violate the Fourth Amendment?*, 52 *Wash. & Lee L. Rev.* 1772 (1995).

17 See the extensive treatment of advances in surveillance technology in the consultation paper of the STOA (Scientific and Technological Options Assessment) programme of the Directorate General for Research (Directorate B) of the European Parliament: *An Appraisal of Technologies of Political Control*, (6/1/1988, PE 168 499). The paper does not necessarily represent the views of the European Parliament.

already available to broadcast the footage generated by CCTV systems over the internet.¹⁸

1.23 An enormous range of devices with extraordinary potential for intrusiveness (including for example a video camera in the form of a shower head) is now available cheaply by mail order over the internet,¹⁹ and there is a corresponding market in anti-surveillance devices similarly available. We allude in this Report²⁰ to copious accounts in the newspapers that sophisticated surveillance technology is being used in Ireland.

1.24 At the same time that this technological revolution is taking place, Ireland is, in common with most other countries, making the transition to the Information Society. In such societies information is the key to wealth and power. Surveillance is nearly always (though not invariably) done for a purpose and that purpose is usually connected to the collection of information, images and other material. It is not relevant here whether the information, etc., is subject to automatic processing within the meaning of data protection legislation. What is at issue is the growing demand for information which in turn generates a demand for further and better methods of acquiring such information through, *inter alia*, surveillance. The subsequent use of the information (whether legitimate or otherwise) is separate from the phenomenon of a seemingly growing demand to pierce the veil of privacy to obtain that information in the first place.

3. The Inadequacy of Existing Irish Law

1.25 The issue of the inadequacy of existing Irish law is explored in detail in Chapter 3.

1.26 A growing public concern in most countries, including Ireland, at the lack of comprehensive or effective legal protection in this area was noted by us in our First Programme for law reform. Many countries, including Ireland, have a web of laws that protect isolated aspects of privacy. A few countries, mainly European, have tailor-made privacy laws that adequately protect privacy in the round and directly. The subject has already been looked at by a variety of law reform bodies throughout the world and continues to attract much attention.

1.27 Due to its very nature, surveillance is as unobtrusive as it is intrusive. Even where the victim happens to detect the use of surveillance there is often nothing he/she can do in law. Existing law provides little opportunity for full or effective redress. It is highly unlikely that most individuals would be able to

18 See, e.g. <<http://www.spy.org.uk/camerasf.htm>>. "Webcams" (stand-alone cameras not part of a CCTV system) may be directly attached to a computer and the coverage relayed over the Internet: see, e.g. <<http://www.perceptualrobotics.com/live/hgen.asp>>.

19 See, e.g., <<http://www.londonspyshop.com>>; <<http://www.spyzone.com>>; <<http://www.spycatcher.uk.com>>; <<http://novexcanada.com>>; <<http://www.ourworld.compuserve.com>>; <<http://www.viewscape.co.uk>>.

20 para. 3.14, *infra*. and footnote thereto.

detect the occurrence of surveillance unless the fruit of the surveillance is used openly against them. Even where private information that has been obtained as a result of, or by means of, surveillance, is published the individual in question has little incentive to come forward and complain since to do so might compound his/her embarrassment at the revelation of true (but private) information.

1.28 Moreover, even where the purposes for using surveillance are perfectly legitimate (surveillance cameras mounted by the police in semi-public or public thoroughfares for the purposes of prevention and detection of crime) there exists no specific legislative or regulatory regime providing safeguards against abuse and assurances to the public at large.

1.29 Can existing Irish law cope adequately with the privacy problems associated with the threat to personal space posed by surveillance? We believe that it cannot.

1.30 To grasp the inadequacy of existing law it is necessary to keep in mind the high human values honoured by privacy. It is also necessary to realise that there are different - but intimately related - aspects of privacy which are the subject of protective measures in the legal system. This is quite apart from the authority of the protective norm in question, e.g., treaty law, Constitutional law, common law, statutory law. No overall or integrated doctrine has yet emerged to unify these three aspects. The human rights vision helps us identify the deficiencies of these fields both in isolation and as they relate to one another.

1.31 Although, as we indicate in Chapter 3 below, the Constitution as interpreted by the Supreme Court recognises a right of privacy, the content and boundaries of that right remain unclear and in the absence of legislation are dependent for their future development on the fortunes of case law. Among other things, case law depends to a considerable extent on the involvement of persons who can afford to bring (or defend) cases. This cannot meet the immediate need for a clear statement of the rights and obligations of citizens as a whole in circumstances where, in our view, the right of privacy is under an actual and present threat.

1.32 The amalgam of common law doctrines that constitute the privacy shield/s (e.g., trespass, nuisance) was historically constructed to protect privacy in the context of property and in the enjoyment of property. This was usefully labelled "territorial privacy" by a Canadian Task Force in the 1970s²¹. There are several problems connected with "territorial privacy" - problems or deficiencies that give rise to the need for comprehensive legislation. These along with other aspects of the law of tort which incidentally bear on the right of privacy are listed in Chapter 3 below. It is clear that they do not meet the present-day need for protection of privacy from surveillance and disclosure or publication of private information obtained thereby.

21 *Privacy and Computers*, Department of Communications and Department of Justice, Canada (1972).

1.33 Current Irish law does offer some piecemeal protection for personal information. This chiefly occurs in the areas of data protection law²²; rights of anonymity in certain criminal proceedings²³, in family matters²⁴ and in matters connected with personal taxation²⁵; the legal or equitable doctrine of confidence²⁶; and freedom of information legislation²⁷. There is, however, no overall protection of private information under Irish law at present. There is, in short, no tailor-made privacy tort with which to prevent the publication of private information.

1.34 Information privacy is not, however, the core focus of this Report. Most acts of surveillance will be targeted at information. Sometimes that information will be of a private nature and sometimes not. Either way, surveillance carried out with a view to the accessing of that information *prima facie* entails a breach of the privacy shield and this is our core focus in this Report. Only to the extent that the information so extracted is private in its nature is there an overlap between information privacy and the focus of this Report.

1.35 The privacy shield which we propose to protect in this Report is essentially information-insensitive. What is important in the concept of a privacy "shield" is that a person has a right to be protected against intrusion into his/her private space whenever he/she has a reasonable expectation of privacy irrespective of whether such intrusion actually results in the obtaining of private information (or indeed any information) about the person intruded upon.

1.36 As the Law Reform Commission of New South Wales states in its Issues Paper on *Surveillance*:

"...there is no necessary connection between surveillance and the collection of information. As surveillance is considered intrusive in itself, regardless of any information-collecting purpose, mere regulation of the use of information obtained by surveillance is likely to be considered insufficient protection of privacy."²⁸

Intrusion upon one's house is a prime example, but the unjustified and systematic surveillance or surreptitious watching of a person even in public would be another.

22 *Data Protection Act, 1988.*

23 See S.7 of the *Criminal Law (Rape) Act, 1981* and Ss. 3, 4 of the *Criminal Law (Incest Proceedings) Act, 1995.*

24 For a review of the situation obtaining with respect to access to and publicity involving family proceedings see Law reform Commission Consultation Paper *Family Courts* (1994), chapter 5 'The Privacy of Family Proceedings'.

25 See, e.g. *Income Tax Act, 1967* and *Offences Against the State Act, 1963.*

26 See our Consultation Paper on Privacy, *loc. cit.* pp. 68-82.

27 *Freedom of Information Act, 1997.*

28 *op. cit.* at para 2.17.

4. The Need for Law Reform

1.37 The issue of the need for law reform is explored in detail in Chapter 4.

1.38 After much comparative research and after the benefit of submissions²⁹ on our Consultation Paper on this subject as well as an extremely useful "listening exercise"³⁰ involving all those who made submissions and many other interested parties, we now recommend the introduction of legislative protections for privacy in Ireland in the specific context of surveillance and the interception of communications. The real question, in our view, is not whether privacy as a human right is deserving of protection through the legal system but how other competing rights and interests can be appropriately accommodated. We are confident that our specific recommendations will, if enacted, adequately respect the competing interests and rights at stake.

1.39 Our main concern is to craft recommendations aimed at perfecting the privacy shield and making it play a more visibly direct and effective role in protecting privacy in the context of the threats posed by surveillance.

1.40 We believe that we demonstrate in this Report that there are three general reasons why this is an area appropriate for law reform.

1.41 **First**, and not least, as already stated, privacy is under a constant and growing threat especially from new technology. The threat did not originate in technology but the introduction of high technology makes its resolution all the more urgent.

1.42 **Second**, established legal doctrine, which only indirectly protects privacy, can no longer cope or keep up with these developments. The legal regulation of telecommunications and the absence of comparable legal regulation governing other forms of surveillance creates an unjustifiable imbalance in the protective coverage of the law. Nor is it safe to simply assume that time-honoured boundaries will be respected and that this technology will not be used in a privacy-invasive manner or with privacy-invasive effects.

1.43 **Third**, the theoretical possibility of a constitutional action is no substitute, we feel, for adequate legislative provision. As stated in paragraph 3.25 of our Consultation Paper and further emphasised both above and in Chapter 3 below, although it is now established by case law that the personal rights of the citizen guaranteed by Article 40.3.1^o of the Constitution include a right to privacy, the scope and content of this right are as yet ill-defined and require further and much more specific development if there is to be an effective and clear privacy law available to citizens.

29 See Annex V for list of written submissions.

30 See Annex VI for list of participants.

1.44 Similarly, though the genius of the common law lies in its capacity for organic growth and renewal, reliance on the courts to reform the existing patchwork quilt constituted by the relevant common law is not, in our view, a satisfactory way to proceed.

1.45 It must also be remembered that privacy is qualitatively different from many other legitimate goals of State policy. It is not merely a desirable objective in any civilised society but is also a basic human right. It is protected in principle not merely under the Constitution but also under various international human rights treaties to which Ireland is a party including Article 8 of the European Convention on Human Rights. Ireland's primary obligation under that Convention is to "secure" the rights protected under that Convention for everyone (Article 1 ECHR). Taking rights seriously entails a comprehensive evaluation of the capacity of the legal system to provide practical protections and remedies. Such analysis reveals that privacy is inadequately protected in Ireland at the moment against the growing threat posed by surveillance and interception activities. Our view, which is outlined in chapter 5, is that the legislation we propose would be well within Ireland's margin of appreciation under that Convention.

1.46 We are not opposed in principle to effective schemes of self-regulation. Quite the reverse. We, of course, warmly welcome the introduction of voluntary codes of practice and the evolution of self-regulation in broadcasting and the mass media. The Broadcasting Complaints Commission was set up pursuant to the *Broadcasting Authority (Amendment) Act, 1976* and RTÉ has its own Code of Practice adopted pursuant to the *Broadcasting Acts*. The latest example of this laudatory trend is the *Code of Practice on Privacy* adopted by the National News Papers of Ireland in 1997. Indeed, we strongly encourage more self-regulation particularly in the private investigators' industry where nationwide self-regulation has been lacking until now. Our view is that the enactment of appropriate legislation does not mean that private actors cannot or should not regulate their own activities. We do not view appropriate mechanisms of self-regulation and the enactment of legislation as mutually exclusive. Rather, we see self-regulation and legislation of the type we recommend as mutually reinforcing. Self-regulation could be made work best, in our view, if developed under and directed towards fulfilling the requirements of legislation that reassures the public by the provision of judicially enforceable protections.

1.47 In the last analysis, self-regulation - no matter how commendable and necessary - cannot be a substitute for legally enforceable rights which can only be provided for by legislation. The ultimate arbiters of issues concerning the infringement of the citizen's right of privacy must be, and can only be, the courts.

1.48 In our view the provision of civil remedies must be supplemented by the enactment of appropriate criminal sanctions. The criminal law provides the vital element of deterrence and ensures that the Gardaí have a role in clearly defined circumstances. Naturally, different considerations of a qualitative kind arise in the context of the criminal law where a much sharper focus on particularly

egregious acts of intrusion is required. We have taken great care in this regard to confine criminal sanctions to the minimum and to define the constituent elements of the proposed new offences with added particularity and clarity.

1.49 Different considerations again arise in the context of regulatory safeguards where it is safe to assume the legitimacy of some surveillance activities but necessary to consider the introduction of protections against abuse.

B. OVERVIEW OF REPORT

5. Objective - Protecting Reasonable Expectations of Privacy against Surveillance

1.50 Our understanding of a "reasonable expectation of privacy" is set out in detail in Chapter 2 below.

1.51 There are many different variables to be taken into account in determining whether an invasion of privacy has occurred through surveillance and what form the appropriate legal or regulatory response should take. The surveillance may be overt or covert. The place under surveillance may be private or public. The technique of surveillance may be aural or visual. The category of user varies greatly as does the degree of legitimacy of the interest in engaging in surveillance.

1.52 The law must acknowledge all these variables and allow in particular as much space for the pursuit of legitimate interests as is compatible with respect for the right of privacy. This requires flexibility of the law as well as adequate procedural safeguards. Apart from aural interception, privacy interests do not presently figure prominently in regulating the use and manner of use of the full range of surveillance techniques in Ireland. In introducing privacy into the overall equation we emphasise that what we seek to advance and protect is what the ordinary man on the street would consider to be a "reasonable expectation of privacy". Naturally, everyday living exposes all of us to varying and generally acceptable levels of being observed. Such ordinary and natural incidences of everyday living including, for example, tourist or recreational photography, are not materially affected by our recommendations. We explain below and particularly in chapter 2 what we mean by a "reasonable expectation" of privacy and the kinds of indicators that we consider to be relevant in determining whether such expectation arises on the facts of any given case.

1.53 Our approach in protecting reasonable expectations of privacy navigates between more extreme approaches exemplified in the laws of other countries. On the one hand there is the stringent protection of privacy in a civil law country

such as Germany, and on the other hand there is the more relaxed approach seen in U.S. law.³¹

6. Privacy and the Public Interest, Including Freedom of Expression

1.54 Our understanding of the public interest and the public interest defence is set out in detail in Chapter 2 below.

1.55 Bringing privacy to the fore of legal consciousness does not, of course, mean ignoring other human rights that may come into play. Privacy is a way of organising human co-existence; it does not deny such co-existence. It is a relational right whose boundaries depend in part on perceptions and judgments about the right relations between people.

1.56 The boundary to privacy is particularly problematic when it comes to the competing right of freedom of expression. In providing for the possibility of balancing privacy with other rights we are particularly aware that many of these rights can have a value both for the individual and for more generalisable social interests. Freedom of expression is obviously one such competing right.³² It enables the press to perform a vital watchdog role in democratic society. It honours what is commonly referred to nowadays as "the people's right to know" certain information. The public interest involved here is obviously and powerfully present in Article 10 of the European Convention on Human Rights which sets very demanding standards in the area of media liability. These standards are generally much higher than those set under Irish law.

1.57 A pattern is, however emerging whereby Irish statutory law and constitutional interpretation is moving towards an acknowledgement that the public has a right to information in some cases. For example, the *Freedom of Information Act, 1997* protects against the disclosure of personal or private information. That protection can, however, be overridden if the public interest in disclosure outweighs the public interest in secrecy (Section 28(5)). It is of interest that the Irish law of confidence has been interpreted by the Supreme Court in the sensitive sphere of banking to yield where there is a clear public interest in the disclosure by the media of allegations of serious misconduct to the public at large.³³ Furthermore, the "people's right" to know certain information is evident in a recent decision of the Supreme Court which upheld media

31 See, further, Chapter 2 at par. 2.10 (*E: Status*) and see, generally, Chapter 6.

32 For a succinct review of the range of individual and social justifications for freedom of expression (self-realisation; liberty; the pursuit of truth; interest accommodations and social stability; exposure and the deterrence of the abuse of power; the facilitation of accountability in democratic society) see generally Kent Greenawalt, *Free Speech Justifications*, (1989) 89 Col. L. Rev. 119.

33 *National Irish Bank Ltd. and National Irish Bank Financial Services Ltd. v. Radio Telefis Éireann*, unreported judgment of the Supreme Court, 20 March 1998, per Lynch J (O'Flaherty & Barrington JJ concurring), Keane J (joined by Hamilton C.J.) dissenting.

publicity connected with an ongoing criminal trial and with the discretion of trial judges in controlling the same in the interests of the administration of justice.³⁴

1.58 The main question is not whether the public interest should be allowed as a reckonable factor in our Report but how. We believe that the tasks of protecting privacy and maintaining an open and vibrant marketplace of ideas are in fact mutually reinforcing although a clash between them is possible in some circumstances. We provide for this possibility by recommending a new "public interest" defence to disclosure through publication and otherwise when such results from privacy-invasive surveillance. We envisage a public interest arising in circumstances involving the detection or prevention of serious crime, the exposure of serious illegality or wrongdoing, the need to inform the public on a matter of public importance, and the need to prevent the public from being misled by public conduct (including statements) of a person having or seeking public office where the matter disclosed is relevant to the performance or capacity to perform the functions of that office. The sort of protection for privacy we envisage is not a haven for those who may seek to keep information from the public on matters where there is a clear public interest.

1.59 We insist, however, that the public interest secured by the people's right to know a particular piece of information is not synonymous with whatever happens to interest the public. Mere newsworthiness is not a reliable proxy for the public interest. As stated succinctly by the Royal Commission on the Press in its Report of 1977 (the "McGregor Report")³⁵:

"It is sometimes argued that the only opposition to publication of details about people's private lives comes from those with something to hide. We do not agree. We believe that everyone has a right to privacy, and that newspapers should only breach it where there is a clear connection with a demonstrable and important public interest."³⁶

1.60 The exposure of true facts does not, in our view, have any absolute value.³⁷ We emphasise that respect for privacy and for the rule of law is as much in the public interest as is the "people's right to know".

1.66 It must be remembered that, in so far as our recommendations go to publication, they go to the publication of truthful information (whether private

34 *The Irish Times Ltd., Examiner Publications (Cork) Ltd., Independent Newspapers Ireland Ltd. and News Group Newspapers Ltd. and Radio Telefís Éireann v. Ireland and the Attorney General and His Honour Judge Murphy*, Circuit Court Judge of the Cork Circuit, unreported Judgment of the Supreme Court, 2 April 1998. See also the judgment of Geoghegan J. in *Charles J. Haughey & Ors. v. Mr. Justice Michael Moriarty & Ors., Ireland and the Attorney General* (Unreported Judgment of the High Court, 28 April, 1998). In his judgment Geoghegan J. explicitly used the concept of a "legitimate public interest" to delimit the right to privacy (at p. 24-5). In the instant case the legitimate public interest at stake was one of ensuring the efficient conduct of the relevant tribunal. [This case is currently under appeal to the Supreme Court.]

35 Cmnd. 6810 (July 1977)

36 *loc. cit.*, para. 10.136.

37 For general reflections on the inherent and instrumental role and limits of truth see Frederick Schauer, *Reflections on the Value of Truth*, 41 Case Western L. Rev. 669.

in its nature or otherwise) obtained by illegal means (i.e., contrary to the new statutory torts we propose) and not to the publication of truthful (but private) information *simpliciter*.

7. The Conformity of Our Recommendations with the European Convention on Human Rights

1.67 In our reflections and in our final Report we have taken great care to test our recommendations with Ireland's existing international obligations and especially those arising under the European Convention on Human Rights. Put simply, our view is that Article 8 of the European Convention which protects the right to respect for private life is at the very least permissive toward the kind of protective legislation we propose. Indeed it is plausible to read the case law under Article 8 as *requiring* Ireland to take positive measures to ensure that privacy is protected as between private parties. Furthermore we are confident that the legislation we propose, bearing in mind particularly the "public interest" defence we recommend *with respect to wrongful publication*, is quite compatible with Ireland's margin of appreciation under Article 10. This margin is expansive enough to allow contracting States to apprehend a pressing social problem with respect to privacy and to opt for legislation as an appropriate solution with the proviso that adequate space be left for a "public interest" defence. In short, we consider that our recommendations, suitably qualified by the "public interest" defence, would, if enacted, amount to an appropriate and proportionate response to the privacy problem thus apprehended and be fully compatible with the obligations of the State under the Convention.

8. Privacy in the Global Village - The International Dimension

1.68 In making our final recommendations we are painfully aware that Ireland is now firmly integrated within the Global Village. Our growing interdependence with the world - especially within the European Union but also beyond - is a complicating factor in the context of this Report.

1.69 For one thing, this interdependence is reflected in the fact that a worldwide market now exists for surveillance technology. Furthermore, the ongoing process of economic deregulation has dispersed this technology widely into private hands with the result that traditional legal protections that focus almost exclusively on the State as the sole potential abuser miss a large part of their target. Non-State actors pose just as much a threat as the State itself. The demand for such technology by private actors seems set to grow and not diminish. Restricting this market using traditional tools like import controls, a licensing regime for vendors, a licensing regime for users, etc., is unwieldy and likely to be piecemeal and ineffective.

1.70 Our interdependence is also reflected in the fact that a secondary worldwide market also exists for private information which is being treated more

and more as a commodity. The demand for such information, whether obtained through surveillance or otherwise, is quite varied and is only likely to grow as Ireland becomes, in common with other countries, a knowledge-based Information Society and economy.

1.71 The Irish market is not therefore an isolated one. Solutions to the problems of privacy, especially since the market for surveillance devices and indeed the market for private information is global, should ideally take a multilateral form. Indeed the Parliamentary Assembly of the Council of Europe has itself recently called for the drafting of a detailed convention on privacy³⁸. The Motion for a Resolution calling for the drafting of a privacy convention was referred to the Parliamentary Assembly's Committee on Legal Affairs and Human Rights for a report. The *rapporteur* to that committee (Mr Schwimmer) convened an open hearing on the topic in December 1997 and issued his report in June 1998³⁹. The *rapporteur* rejected the argument for a new convention on the basis that Article 8 of the European Convention on Human Rights is satisfactory and on the assumption that national law either already is, or ought to become, sufficient in itself to handle the matter. He proposed instead that a draft resolution should be presented to the Parliamentary Assembly calling on those governments that have not yet done so to pass legislation guaranteeing the right to privacy.

172. The Schwimmer report was debated in the Parliamentary Assembly on 26 June 1998 and a resolution on the Right to Privacy was duly adopted⁴⁰. The final resolution mirrors and indeed strengthens the draft put forward by Mr Schwimmers. It rejects the call for a privacy convention for the same reasons outlined by Mr Schwimmer (i.e., adequacy of Article 8 and the existence of effective national legislation)⁴¹. With respect to those Member States that do not yet have privacy-specific legislation the resolution calls the introduction by those states of such legislation along certain guidelines provided (see para. 1.74 below)⁴². This would include Ireland.

173. Among the more notable features of the resolution are the following. First, the resolution acknowledges that personal privacy is often invaded even in countries with specific legislation to protect it since "people's private lives have

38 *Motion for a Resolution for a European Convention on Privacy*, presented by Mr David Atkinson and others in the Parliamentary Assembly of the Council of Europe, 5 September 1997 (DOC. 7897). For debate see Report of the Proceedings of the Parliamentary Assembly of the Council of Europe, 1997 Ordinary Session, 23 September 1997 (AS (1997) CR 27). The motion was carried and is now before the Committee for Legal Affairs of the Council.

39 Report of the Committee on Legal Affairs and Human Rights (*rapporteur*: Mr. Schwimmer), *Rights to Privacy*, Parl. Assembly Doc. 8130, 3/6/1998.

40 Resolution 1165 (1998), provisional text adopted on 26 June 1998 (24th Sitting). The Schwimmer report was considered alongside two formal opinions on the same; see Doc. 8147, opinion of the Committee on Culture and Education (*rapporteur*: Mr Staes) and Doc. 8146, opinion of the Social, Health and Family Affairs Committee (*rapporteur*: Mr Mitterand).

41 Para 14.

42 Para 14.

become a highly lucrative commodity for certain sectors of the media"⁴³. Secondly, the resolution notes that public figures must recognise that the role they play in public life automatically entails "increased pressure on their privacy"⁴⁴. This is not, however, the same as stating that the private lives of public figures are an open book. Thirdly, the resolution defines public figures generally to include "those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or any other domain"⁴⁵. Fourthly, the resolution asserts that "[i]t is in the name of a one-sided interpretation of the right of freedom of expression...[under Article 10]...that the media invade people's privacy, claiming that their readers are entitled to know everything about public figures"⁴⁶. Fifthly, the resolution concedes that the public has a right to know certain things about the private lives of public figures which therefore calls for a careful balancing of privacy and freedom of expression⁴⁷. Sixthly, the resolution asserts that the two rights in question (privacy and freedom of expression) "are neither absolute nor in any hierarchical order, since they are of equal value"⁴⁸.

174. The resolution calls for privacy-specific legislation where none exists (or the supplementation of existing legislation) along the following lines (para. 14);

"i. an action in civil law should be guaranteed to be able to claim possible damages for invasion of privacy;

ii. editors and journalists should be rendered liable for invasions of privacy by their publications, as they are for libel;

...

iv. economic penalties should be envisaged for publishing groups which systematically invade people's privacy;

v. following or chasing persons to photograph, film or record them, in such a manner that they are prevented from enjoying the normal peace and quiet they expect in their private lives or even such that they are caused actual physical harm, should be prohibited;

vi. a civil action...by the victim should be allowed against a photographer or a person directly involved, where "paparazzi" have trespassed or used "visual or auditory enhancement devices" to capture

43 Para 6.

44 Para 6.

45 Para 7.

46 Para 8.

47 Paras 9 and 10.

48 Para 11.

recordings that they otherwise could not have captured without trespassing;

vii. provision should be made for anyone who knows that information or images relating to his or her private life are about to be disseminated to initiate emergency judicial proceedings such as summary applications for an interim order or an injunction postponing the dissemination of the information, subject to an assessment by the court as to the merits of the claim of an invasion of privacy;

viii. the media should be encouraged to create their own guidelines for publication and to set up an institute with which an individual can lodge complaints of invasion of privacy and demand that a rectification be published".

1.75 Furthermore, the resolution calls on the Governments of the Member States to encourage professional bodies to draw up standards for entry into the profession as well as standards for self-regulation and a code of journalistic conduct, to foster the development of media education, and to facilitate access to the courts and simplify the legal procedures relating to press offences in order to ensure that the rights of victims are better protected (para 16).

1.76 While this resolution is not legally binding it does have significant moral authority since it was adopted under the authority of the Parliamentary Assembly of the Council of Europe which represents some 40 European countries. The approach taken in the resolution strongly reinforces our own analysis of the need for legislation and for the kind of legislation required. The full text of the resolution is reproduced in annex V.

1.77 We are strongly of the view that we cannot and should not wait for multilateral action to take place before taking steps in the right direction under domestic law. In recognition of the cross-border nature of the market for private information we do make a specific recommendation dealing with civil liability for disclosure through publication or otherwise in Ireland of private material obtained overseas by methods which, if employed in Ireland, would be contrary to our recommended tort of privacy-invasive surveillance.

9. Overview of Recommendations

1.78 Concerning terminology in this Report, we use the generic term "surveillance" to include aural and visual surveillance, irrespective of the means employed, and the interception of communication. The concept of surveillance implies in its ordinary usage some form of watching, spying, eavesdropping, besetting or following a person about for the purpose of invading that person's privacy, whether by means of technical devices or not, including listening to or recording a conversation or message to or from a person, otherwise than as a lawful party thereto.

1.79 In addition to this, we propose that two particular forms of privacy-intrusive behaviour which may not strictly speaking fall within the everyday meaning of surveillance should be included within the meaning of that term for the purposes of our recommendations on the civil side in this Report. These are the act known as "participant monitoring" in which one party to a message or conversation records the message or conversation in whole or in part without the knowledge of another party thereto; and "third party monitoring" in which a person not a party to a message or conversation records that message or conversation in whole or in part with the agreement of one party thereto but without the knowledge of another. Both of these acts are to be regarded in our view as involving privacy-invasive surveillance of the unknowing party.

1.80 Our main recommendations can be summarised as follows:

(a) Civil Law Reform

- **Core Recommendation - tort of privacy-invasive surveillance:**
the enactment of a new statutory tort to protect against the invasion of privacy by means of surveillance subject to certain conditions and defences. We itemise the many factors which a Court is empowered to take into account in determining whether a "reasonable expectation" of privacy arises on the facts of a given case. We use the term surveillance generically to include aural surveillance, visual surveillance, interception of communication, participant monitoring and third party monitoring. The defences include consent (express or implied) and the exercise of a legal power, duty or right.

[see Heads 1(3)(i) and 2 (i) of the Draft heads of Bill].

- **Subsidiary Recommendation - tort of harassment:**
the enactment of supplementary civil provisions in the sphere of harassment.

[see Head 2 (ii) of the Draft Heads of Bill].

- **Ancillary Recommendation - tort of disclosure through publication and otherwise of information obtained as a result of privacy-invasive surveillance or harassment:**
the enactment of an associated statutory tort directed against the disclosure through publication or otherwise of information that results from such surveillance or harassment, subject to the defence of consent (express or implied) and the defence that the publisher did not believe and had no reasonable grounds to believe that the information had been obtained by tortious means, and subject also, where the information had been obtained through surveillance but not through harassment, to a "public interest" defence.

[see Head 2 (iii) of the Draft Heads of Bill].

Ancillary Recommendation - tort of publication in Ireland as a result of an act which, if it occurred in Ireland, would amount to privacy-invasive surveillance or harassment:

- *the enactment of a tort directed against the publication within the State of information, etc., obtained outside the State by means or as a result of acts which, if committed within the State, would have amounted to civil wrongs under the proposals (see above). [see Head 2 (iv) of the Draft Heads of Bill].*

Remedies

- *the possibility of a range of remedies for these torts including privacy orders (preventive injunctions), damages or an account of profits. [see Heads 4 & 5 of the Draft Heads of Bill].*

(b) The Enactment of New Criminal Offences

Targeting the egregious abuse of surveillance technology:

- *the enactment of new statutory offences directed against the most egregious abuse of privacy-invasive surveillance technology involving (1) surveillance of private dwellings and (2) surveillance of private conversations no matter where they occur;*
- *the enactment of a new offence (3) of trespass on private property with a view to obtaining personal information; and*
- *the enactment of supplementary offences of disclosure of information obtained in contravention of these provisions. [Heads 9 and 10]*

(c) The Provision of New Regulatory Safeguards

Provision of a basis in positive law for police surveillance of private places:

- *recommendation that, notwithstanding the provisions mentioned at B above, there should be a procedure for authorisation by warrant, by a Chief Superintendent for an initial short period and by a District Judge thereafter, for police surveillance (involving optical or hearing devices) of private places where this is justified for the prevention or detection of any crime in respect of which a search warrant may be issued under any statute or for the purposes for which a search warrant may be obtained under the Criminal Assets Bureau Act, 1996. Criteria should be laid down concerning the necessity for the surveillance and the justification for it including the likely impact of the surveillance on the rights of any person. Supplementary provisions should be enacted regarding the use which may be made of information gained. [Head 11(2)]*

Provision for police surveillance of public places:

- *recommendation that, subject to a recommended provision of limited surveillance by private persons (see below), fixed optical or hearing devices may not be used for the purposes of surveillance of public places except by a member of An Garda Síochána acting under and in accordance with an authorisation granted by a member of the Garda Síochána not below the rank of Chief Superintendent;*
[Head 11(3)]
- *recommendation that a comprehensive CCTV Code of Practice with respect to police surveillance of public places should be developed and placed on a statutory basis;*
[See Chapter 9]
- *provision for overall judicial review of surveillance by the Garda Síochána along the lines laid down by the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.*
[Head 11(7)]

Surveillance (by means of fixed optical devices) by private persons of public places, or of private places open to the public:

- *recommendation that fixed optical devices may be used for surveillance of a public place by a private person only by means of a device installed and fixed in premises owned or occupied by the user for the bona fide protection and safety of the user's premises including persons therein and provided that appropriate notice to the public of such surveillance is affixed to the premises;*
- *recommendation that surveillance carried out within a private place to which the public have access may only be carried out if notice is given at each entrance to the premises which is available to the public for the purposes of such access;*
- *recommendation that the Minister for Justice may by order lay down additional provisions for giving full effect to these provisions;*
[Head 11(4)]
- *recommendation that codes of practice governing the use of CCTV in various private sectors be elaborated and placed on a statutory basis.*
[see Chapter 9]

Ancillary Recommendations

- *recommendations imposing restrictions on the disclosure or use of information obtained by surveillance governed by the regulatory provisions above, (a) where such surveillance is authorised under those provisions and (b) where it is not.*
[see Head 11]

(d) Miscellaneous Technical Recommendations:

- *the enactment of several amendments to existing legislation to ensure more and better protection of privacy in the context of technological and other changes in surveillance and interception and of the opening-up of the Irish market in postal and telecommunications services to new service providers.*

10. Outline of Report

1.81 The remainder of this Report is divided into three Parts as follows.

- **Part 1 - General** contains an analysis of what we mean by privacy, why privacy is worthy of protection, why there is a privacy problem, why Irish law is presently inadequate to the task, why we consider a legislative solution to be appropriate and practicable, what factors should be relevant in determining when a "reasonable expectation of privacy" occurs and what the "public interest" means in this context.

Part 2 - Benchmarks for Reform outlines the main benchmarks for reform under international human rights law and under selected aspects of comparative law. This Part shows to our satisfaction that change is both permissible in principle under The European Convention on Human Rights and workable in practice given the practical experience of other countries. In particular we highlight the case law under the European Convention on Human Rights in order to demonstrate that what we recommend lies well within Ireland's margin of appreciation under that Convention. Since much of this is new research - especially with respect to the reconciliation of Articles 8 (private life) with 10 (freedom of expression) it is summarised in the body of the Report and the details are contained in an appendix (Annex I). We then summarise the various legislative measures already adopted in selected jurisdictions around the world. For ease of exposition this is summarised in chapter 6. A separate appendix (Annex II) contains a summary of relevant developments in the UK for reference purposes.

- **Part 3 - Recommendations** sets out our recommendations with respect to civil law, criminal law, regulatory law and various technical matters. It contains **Proposed Heads of a Bill** to give effect to our recommendations.

1.82 There are seven annexes to this Report:

- **Annex I** contains new research on the inter-relationship between Articles 8 (private life) and 10 (freedom of expression) under the European Convention on Human Rights.
- **Annex II** contains a brief summary of the evolution of the privacy debate in the UK.
- **Annex III** contains research on the application of data protection law to CCTV systems.
- **Annex IV** contains research on the power of the courts to order proceedings to be held *in camera* and to restrain publication relating to proceedings.
- **Annex V** contains the text of the Resolution on Privacy of the Parliamentary Assembly of the Council of Europe.
- **Annex VI** contains a list of written submissions on our Consultation Paper.
- **Annex VII** contains a list of participants at our "listening exercise" on privacy held on 17 July, 1997.

PART I - GENERAL

CHAPTER 2: WHAT WE MEAN BY PRIVACY AND WHAT WE MEAN BY THE PUBLIC INTEREST

A. WHAT WE MEAN BY PRIVACY

1. General

2.1 As stated in our Consultation Paper, privacy as a concept includes a wide range of personal interests or claims which 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 recognized as a human right, and is to be distinguished from other interests such as secrecy and confidentiality.

2.2 Such definitions of privacy as have been attempted tend not to be all-embracing; yet one such definition which refers to privacy as "the right to be left alone"¹ strikes a common chord with the particular aspects of privacy which we consider in this Report: freedom from privacy-invasive surveillance (including the interception of communication) and harassment, with the concomitant protection against the publication of material obtained by means or as a result of such surveillance or harassment.

2.3 The meaning and scope of privacy as a legal concept has received attention in other jurisdictions. In particular, in the early 1970s a Canadian Task Force identified three categories of claims to privacy:

territorial privacy - a claim to privacy advanced in a territorial or property sense based on the existence of a physical domain within which a claim to be left in solitude and tranquillity is recognized ("a man's home is his castle");

privacy of the person - the notion that each person has a "personal space" bounded not by physical walls and fences but by legal norms and social

¹ Judge Cooley, quoted in L D Brandeis and S D Warren, *The Right to Privacy*, 4 Harvard L.Rev. 193 at 195.

values which protect him from physical harassment and guarantee him freedom of movement and expression, freedom from physical assault and freedom from unwarranted search and seizure of the person); and

privacy in the information context which is a human right based on 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, subject only to exceptions created by overriding social values which may require him to disclose information about himself to the authorities in certain defined circumstances².

2.4 Significantly, the Australian Law Reform Commission in its research on privacy added a fourth category:

"the interest in freedom from surveillance and the interception of one's communications".

2.5 This category of privacy however is not separate from those identified by the Canadian Task Force; it is connected with and is indeed a particular aspect or segment of all three of the latter. Thus, the category of privacy known as surveillance and communications privacy, which is the primary subject matter of this Report, is based on the idea of a legal shield or boundary, the penetration of which by outside persons is prohibited except under specific circumstances laid down by law, which protects the individual from privacy-invasive surveillance (and, as recommended in this report, harassment) in all of the spheres recognised by the Canadian Task Force. Moreover, an unlawful crossing of that boundary (e.g. by placing an electronic device in a person's home, by tapping his telephone or by systematically spying on his movements even in public places) may occur even though no private or intimate information is in fact obtained as a result.³

2.6 The right not to be *harassed* is more specific than the right of privacy and is more easily capable of statutory definition than the latter. Harassment and privacy-invasive surveillance can go hand in hand and accordingly, harassment, though conceptually distinct from surveillance, is covered by the recommendations in this Report. In the remainder of this Chapter, however, which is concerned with the meaning and scope of the concept of *privacy*, especially in the context of *surveillance*, harassment is not expressly mentioned, but references to surveillance may be taken to include harassment where appropriate.

2.7 The particular area of the law of privacy known as the law of confidences, or confidentiality, is not within the scope of this Report. The law of confidentiality applies to information imparted within a *relationship of confidentiality*, expressed or implicit between two or more parties, such that the

2 quoted in our Consultation Paper on *Privacy*, footnote to para. 1.6.

3 *id.*, footnote to para. 1.7.

person in whom trust or confidence is placed will infringe the obligations imposed by that relationship if he or she discloses the information to another without authority.

2.8 The law of confidentiality is already covered to a considerable extent both at common law and in equity though it requires further clarification and development. The English law of confidence is showing signs of considerable development at the hands of the judiciary and there is even English authority to suggest that it may be extended so as to cover at least some cases of disclosure of information obtained by surreptitious surveillance without any prior relationship of confidence (see Chapter 3 below). However, it differs in principle from the law concerning surveillance in that confidentiality assumes a specific relationship of trust between persons leading to an obligation of confidentiality whereas under our proposals, unlawful surveillance assumes no such relationships and may occur without any private or confidential information being obtained or conveyed by or to anyone.

2.9 In this chapter we focus on what we mean by privacy and the circumstances under which a "reasonable expectation" of privacy against surveillance may arise. Later in this Report we outline the various factors that should be taken into account in determining whether surveillance that violates this "reasonable expectation" of privacy can be defended as legitimate.⁴

2. Factors Relevant to a "Reasonable Expectation" of Privacy

2.10 The existence and extent in the particular case of a right of privacy in the sense of freedom from privacy-invasive surveillance (for short, "surveillance privacy") is an issue which is less cut-and-dried than is the case with some other human rights such as the right to private property or the right to vote. "Surveillance privacy" is one of those rights whose existence and extent will inevitably depend to a very high degree upon the circumstances of the case and will vary depending on these circumstances. *A person's right to freedom from privacy-invasive surveillance may for the purposes of this Report be broadly defined as that freedom which a reasonable person in the circumstances of the case is entitled to expect.*

2.11 Since we view privacy as a personal right and one that follows the personal space of the person it follows that a "reasonable expectation" of privacy may even exist in public places. The practical application of this concept is ultimately a matter for the courts in interpreting the legislation having regard to the relevant circumstances and to the accepted customs and mores of society at the relevant time. Nonetheless it is possible to identify a number of factors which in the view of the Law Reform Commission are, *without being exhaustive*, liable to be of particular relevance and assistance to citizens as well as to the courts in

4 *infra*, Chapter 7, Part C.

deciding whether or not in the particular case a particular act is an illicit invasion of a person's right to such privacy.

2.12 The factors which, among such others as the courts may consider appropriate, should in our view be considered by the courts in deciding whether the privacy "shield" has been breached, are as follows:

(a) *Place*

2.13 *The place of surveillance: the home or private premises as against public places*

A person's right to freedom from surveillance is at its highest, and comes closest to being absolute, when he or she is at home. There is logically also a heightened right to such privacy for a person on other kinds of private premises. Yet even at home, a person may so behave (e.g. before the window of a lighted room at night without drawing the curtains or in the garden of a dwellinghouse which is open to public view from the street) that persons in neighbouring premises or casual bystanders (without snooping or resorting to visual or aural surveillance equipment) cannot fail to see or hear what is going on. In some such cases the dweller may even intend to be seen or photographed and clearly there is no invasion of privacy in such a case.

By contrast with the home, a person's reasonable expectation of privacy is greatly reduced when that person is in a *public place*. Persons who are in public places must accept that they are subject to the ordinary and natural incidences of everyday communal living. Thus, the taking of casual photographs in a public place should not normally be held to be an invasion of the privacy of a person who happens to be captured by such a photograph merely because he or she is present in that place at the relevant time.

On the other hand a reduced expectation of privacy is not the same as denying the public any right to adequate safeguards (e.g. adequate notification or limits on the use of footage) against the abuse of overt street surveillance.

Furthermore, the targeting of a particular individual either surreptitiously or against his or her will in a public place, *particularly with a view to publication of that person's photograph*, could well, depending on the circumstances, be held to be an invasion of that person's privacy. The deliberate following (whether surreptitious or otherwise) of a person from place to place with a view to observing his or her movements could, it is suggested, be so categorized.

(b) Object

2.14 *The object or occasion of the surveillance: intimate or private life as against the commonplace or banal*

A person's "reasonable expectation" of privacy may also vary with the object of the surveillance.

Surveillance, even in a public place, which deliberately seeks out or targets the intimate corners of a person's life or personality, such as at a time of death, injury or grieving, where those affected are vulnerable or are otherwise unable at the time to fend off such surveillance may violate a person's "reasonable expectation" of privacy.

Likewise surveillance which intrudes upon relationships between people, at least where they are not flaunted in such a way as to amount to the abandonment of the claim to privacy, may properly lie within the protection of the privacy shield in circumstances where the seeking out of other more mundane material would not be considered objectionable.

(c) Use

2.15 *The use to which material obtained by surveillance is to be put: intended publication or other use which may be objectionable to the subject, as against innocuous use*

A "reasonable expectation" of privacy may arise where the taking of a film or photograph is done with a view to its publication or to its use in some other manner which would be detrimental to the person.

(d) Means

2.16 *The means of surveillance used: the naked eye or natural hearing as against high technology*

There may arise a "reasonable expectation" of privacy against the use of certain types of surveillance devices. The use of privacy-invasive technology may render unacceptable the activity of surveillance which is otherwise acceptable, particularly in public places.

The use, particularly if it were surreptitious, of long-range visual means of surveillance such as high-powered lenses for the purposes of observing people there would be likely depending on the circumstances to involve privacy-invasive surveillance.

Even more egregious would be the use of aural equipment (or indeed video equipment for lipreading purposes) with a view to spying on people's conversations whether in private or in public places.

(e) Status

2.17 *The status or function of the person subjected to surveillance: "public" as compared to "private" persons*

People who are in the public eye (especially where they have placed themselves in the public eye by their own volition, such as politicians running for election, pop stars or other celebrities) cannot have the same "reasonable expectation" of privacy, and a corresponding level of immunity from surveillance, as the ordinary citizen.

Yet even their status in the public eye does not mean that they have no privacy rights. Even public persons enjoy the right to privacy in respect of the intimate details of their private lives - a right they do not abandon upon entering public life.

We navigate between two extreme views as to the effect of the status of the person on the level of reasonable expectation of privacy.

On one view - a view that is loosely characterised as representing the US approach - the fact that a person may have a public persona is sufficient in itself in rendering practically every aspect of that person's life open to scrutiny. Even though only one aspect of that person's persona may protrude into the public side of the public/private line, every aspect of his persona follows. That being so, there is no logical limit to the power to lay bare the secrets of a private life since, by definition, nothing is private any longer.

On another view - a view that is loosely characterised as representing the German approach - certain aspects of a person's private life are always deemed off limits to scrutiny even though the matter in question may, for example, go directly to the functioning or capacity of a public person to hold public office, or may (for example in the case of a secret entry in a person's private diary containing a confession of a crime) be directly relevant to the enforcement of the criminal law against that person.

The first approach suffers from the defect that it is insufficiently sensitive to the extent to which it is possible (indeed desirable) to be both private and public at the same time. On this approach, since a person's life is either completely public or completely private there is little room for discernment between private matters that go to a person's public persona and other private matters that do not. As a matter of human psychology it may well be difficult to divide a person's life into two fixed realms of public and private. But as a matter of ethics and law such a division is imperative. Furthermore - and equally important - attractive though the so-called American approach may seem in some cases, it tends to lead to a situation in which there is a "free for all" right of media intrusion into the private lives of public persons, on the view

that the people are entitled to know everything about their actual or prospective leaders, with the lowest common denominator in terms of media standards becoming the norm, and the law becoming the law of the jungle. We are of the view that this ought to be unacceptable in a civilised society.

The second approach suffers from the opposite defect that some private matters are never acknowledged to go to a person's public persona when in fact they do.

We steer a middle course between these two extremes. We reject the view that once a person can be characterised as "public" that he or she loses all legitimate expectations of privacy. The public/private line may be blurred in such cases but it is still there. We similarly reject an overly rigid view of the public/private line - one that would not allow for the possibility that purely private matter may, on occasion, be of relevance to a person's persona or function. It follows that a person's public status will affect - but not destroy - his/her legitimate expectation of privacy. As will be seen later in Chapter 8 we seek to reflect the fluidity that must *perforce* exist on the borderline between public and private in a public interest defence to wrongful publication. Lying at the heart of the defence is a recognition that some (but certainly not all) private matter may be of some (but not unlimited) relevance in the public sphere.

(f) Consent

2.18 *Any previous conduct by the person subjected to surveillance indicating encouragement of interest by others in his or her private life, or amounting to a partial waiver of his or her right to privacy*

Persons who have deliberately courted publicity in respect of their private lives, for example, by deliberately providing intimate details about themselves and their relationships to the media, cannot expect to be able to "switch off" at will the media or other attention which they have sought. By their own behaviour they have generated a reduced expectation of privacy.

There is a strong element of implied consent in their action. Yet even such people do not by such conduct entirely waive their rights to privacy so as to give others *carte blanche* to intrude at will without permission or restraint on their private lives. Some sense of proportionality continues to apply notwithstanding consent.

(g) *Relationships*

2.19 *The relationship(s) between the parties*

Reasonable expectations of privacy may vary depending on the nature of the relationship, if any, between the parties involved. An act which would undoubtedly be a breach of "surveillance privacy" between strangers might not be so between, say, members of the same family.

A relationship will therefore affect the level of "reasonable expectation" of privacy. However, a residuum of privacy exists even in the most intimate of relationships.

3. The Non-Exhaustive Nature of the Indicators

2.20 Between the opposite ends of the various scales of circumstances and factors, some of which are indicated above, which are relevant to the existence and extent of the right to be free from privacy-invasive surveillance, there are a great number of possible cases and combinations of circumstances which in the last analysis require the assessment of the courts. This should, if our recommendations are enacted into law, result in the building up over time of a body of jurisprudence which, within the framework of the legislation, would define by reference to actual cases the limits and conditions of the right to be free from privacy-invasive surveillance. It would be neither possible nor desirable to attempt to lay down rigid or exhaustive legal rules for this purpose in the legislation itself.

2.21 The impossibility of a specific, fully defined, all-embracing statutory definition of the right of "surveillance privacy" (and of the factors which may override that right which are dealt with later in this Report), which would provide a slide rule for liability in every case, does not however constitute a flaw in our recommendations (it has not been considered a flaw other countries which have advanced and long-standing privacy laws, much of which is judge-made, such as Germany). The absence of a precise delineation of the borderline between what is and is not to be permitted would not in the vast majority of cases prevent the making in advance of reliable judgments by those concerned as to whether a particular act in the circumstances of the case would cross the borderline between lawful action and the tort of privacy-invasive surveillance.

2.22 Where doubts persisted our recommendations would provide a legislative framework for their resolution by the courts. For this purpose we suggest (see para. 2.10 above) the inclusion in the recommended privacy legislation of a series of non-exhaustive factors or considerations which the courts might take into account in assessing the existence and extent of the right to surveillance privacy in particular cases.

2.23 Our reliance on the good judgment of the courts is well-justified. The Constitution of Ireland itself has depended for its full development on what is now a very substantial corpus of judge-made law concerning the full range of fundamental constitutional rights which has been built up in the last 60 years. The legislation we propose would introduce much-needed specificity to the law concerning surveillance privacy while allowing the courts the necessary room to interpret and apply that law so as to deal satisfactorily with the myriad of situations, many of them unforeseeable in advance, which may arise.

B. WHAT WE MEAN BY THE PUBLIC INTEREST

2.24 We set out below the general movement toward the concept of the public interest in freedom of expression doctrine under the Constitution. We then add our own understanding of the kind of shape such a concept would take in the context of providing a defence to wrongful publication of material obtained as a result of privacy-invasive surveillance.

2.25 We consider that a public interest defence to wrongful publication as a result of surveillance is warranted both with respect to the case law under Article 10 of the European Convention on Human Rights (see chapter 5 and the detailed analysis in Annex I) as well as under the Constitution as presently interpreted by the Superior Courts.

2.26 As will be seen under the Heads of Bill, the public interest concept we propose can also operate as an argument to inhibit the issuance of an injunction and as an argument against a motion to hold relevant proceedings *in camera*.

1. The Emergence and Authority of the "Public Interest" Concept

2.27 Freedom of expression is protected under Article 40.6.1^o of the Constitution. It states

"[The State guarantees liberty, subject to public order and morality, for the exercise of]

- i. The right of 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."

2.28 The nature of this guarantee was comprehensively explored in our previous Report on the Civil Law of Defamation⁵. Many interpretative possibilities were explored in that report on the question whether the media enjoyed less, the same or more rights than ordinary members of the public. On the basis of existing case law at that time it did not appear as if the courts were inclined to afford an expansive interpretation to the provision - one that might recognise the special role of the media in Irish democratic life and carve out appropriate or enhanced latitude to publish on matters relating to the public interest. However, since that Report and indeed since the publication of our Consultation Paper on privacy, the Supreme Court has produced a seminal judgment concerning press freedom: *The Irish Times et al. v. Ireland, the Attorney General and His Honour Judge Anthony G Murphy*⁶.

2.29 In that case the Supreme Court stood back from the text of Article 40.6.1^oi and read it in light of democratic theory and the exigencies of accountability in democratic society. Specifically, a plurality of the judgments appear to accept that the press enjoy expansive freedom of expression rights under Article 40.6.1^o and that this freedom (despite previous doubts to the contrary) includes a freedom to report facts as well as opinions and convictions⁷. The case itself involved a clash between the right to a fair trial (Articles 38.1 and 40.3) and the public right of access to (and publicity about) judicial proceedings (Article 34.1). The net issue posed concerned an order made by the trial judge in a drugs prosecution to drastically curtail media reportage of ongoing and contemporaneous court proceedings. Significantly, a plurality of judgments invoked Article 40.6.1^o to further augment the public right of access and publicity under Article 34.1.

2.30 Lying at the heart of the plurality judgments was the view that the public had a right to know how judicial proceedings are being conducted and that the media performs an important function in democratic society in communicating that information. The media is, in essence, the vital bridging link between the demand for (i.e., the democratic right of the people to know the relevant information concerning the trial) and the supply of this information. This right to know and to receive the information and the corollary right to impart that information could be grounded on Article 34 or more generally on Article 40.6.1^o.

5 LRC 38-1991; Annex A: The Constitution and the Law of Defamation, pp. 110-124.

6 Unreported judgment of the Supreme Court, 2 April, 1998.

7 The extension of the freedom contained in Article 40.6.1^oi. to encompass the expression of facts was effectively presaged by necessary implication in a previous Supreme Court decision: *Heaney & McGuinness v. Ireland*, [1997] 1 I.L.R.M. 117.

2.31 In the instant case all judges were of the view - as had been established in previous precedents - that the right to a fair trial took precedence over the right to know. The relevant test was whether there was a real risk that the right to trial might be jeopardised. On the facts of the case the Supreme Court held that the trial judge could not reasonably have come to that conclusion. Implicit, however, in the ruling is the possibility that had the evidence been more persuasive the trial Judge might properly have imposed appropriate restrictions on publicity.

2.32 What is the significance of this case in the context of this Report? First of all, the acknowledgement by the Supreme Court that the press enjoy an expansive freedom of expression fits with our overall approach which fully acknowledges the value of the media in democratic society. That is precisely why, at the outset, we endeavoured to test our recommendations against the higher standards set under Article 10 of the European Convention on Human Rights. It may well be that the Irish Supreme Court is being progressively influenced by the values and spirit of Article 10 in its overall approach to interpreting Article 40.6.1ⁱ. Indeed, at least one judge (Barrington J.) specifically mentions Article 10. Secondly, the expansive interpretation given to the right to include reportage on factual matters makes sense because the most important democratic function of the media is to impart information on which people can make up their own minds on matters of public concern.

2.33 The *Irish Times* case itself obviously focused on a matter of legitimate public concern. Indeed, it would be hard to find a matter more of public concern than the conduct of ongoing judicial proceedings concerning charges of a serious criminal offence. The Supreme Court did not put forward - because it did not have to - any coherent theory according to which one might determine what was and was not of legitimate public concern or in the public interest. The case does not in any way detract from the validity of the distinction which we make in this Report, and which is vital to the public interest defence we propose, between matters that are of legitimate public concern and matters which are not (such as items which are merely "newsworthy" in the sense that they are liable to arouse curiosity or whet the appetite of some for sensational or scandalous material for its own sake).

2.34 We do not make the unrealistic claim that all private matters are never of public concern or legitimate interest. We acknowledge that there may on occasion be a public right to know, and a corollary right of the media to impart, private information so long as there is sufficient and demonstrable connection between that matter and the public interest. That is exactly why we propound a public interest defence to the new tort of wrongful publication and that is why we empower a trial judge to take explicit account of the public interest in determining whether there is a good case for curtailing publicity connected with ongoing judicial proceedings connected to the kinds of civil and criminal actions we envisage.

2.35 There can, of course, be no doubting that some implicit principle of proportionality should be adhered to in any legislative proposals of the sort we make⁸. The overall obligation on the State under Article 40.3.2° of the Constitution is to protect and vindicate the right of privacy against "unjust attack" and "as best as it may". We do not read into this a preference for self-regulation to the exclusion of statutory regulation. We are of the view that the "public interest" defence we recommend would, by allowing for a calibration of the people's right to know with the right to privacy, ensure ample compliance with any proportionality test in the context of this Report.

2.36 We note in passing the recommendation of the Constitution Review Group (which was mentioned in several submissions made to us) to the effect that Article 40.6.1°i should be replaced with a new provision modelled on Article 10 of the European Convention⁹. The adoption of that proposal would not in any way impinge upon our recommendations, because our recommendations take full account of the European Convention on Human Rights (see below Chapter 5 and Annex I). For the sake of completeness we also note that the Constitution Review Group recommended that a general right of privacy should be specifically mentioned in Article 40.3 of the Constitution.¹⁰

2. Our View as to the Public Interest in the Disclosure of Information Obtained by Surveillance

(a) Elements of the Public Interest

2.37 The issue raised here is what kinds of matter would count as being in the public interest for the purposes of the Heads of Bill notwithstanding that they are private in their nature and obtained as a result of privacy-invasive means? The following, contained in our recommendations, is a non-exhaustive list.

Detection and Prevention of Crime

2.38 First of all, there is a potential "public interest" in the detection and prevention of crime [see Head 3(3)(a)]. There arises a civic responsibility to bring any well-grounded suspicion of criminal activity to the attention of the Gardaí. In our view, the fact that this could have been done but was not done may well be one factor that a court might take into account in determining whether this aspect of the "public interest" properly lies in any given case of publication. On the other hand a court might be swayed in the other direction if, for example, the view is taken that the detection and prevention of crime by the public authorities might benefit by publication or in the event, albeit unlikely, that the conduct of the public authorities themselves is at issue. It is to be noted

8 *Thomas Joseph Cox v. Ireland, the Attorney General, The Minister for Education, and Michael Walsh*, 2 IR (1992) 503.

9 Report of the Constitution Review Group, (Pn 2362, May 1996), at pp. 303-304.

10 *ibid.* at p.262.

that one would not normally expect that, in such a case, the *information* in issue would be about a person's private life, but it may have been obtained by surveillance that intrudes into private space.

Exposure of Serious Illegality or Wrongdoing

2.39 **Secondly**, there is a potential public interest in the exposure of serious illegality or wrongdoing [see Head 3(3)(b)]. Such wrongdoing may involve fraud on the public purse or may point to shortcomings in legislation or in the regulatory system. The illegality or wrongdoing in question must be serious and not trivial. Furthermore, there must be actual "exposure" of illegality or wrongdoing and not merely the publication of a bare and insubstantial belief in the existence of illegality or wrongdoing.

Need to Inform Public on a Matter of Public Importance

2.40 **Thirdly**, there is a potential "public interest" involved in the need to inform the public on a matter of public importance [see Head 3(3)(c)]. This aspect of the "public interest" resonates with the latitude allowed by the European Court of Human Rights for publication of matter that is colourably political or on matters of genuine public interest. There is, in our view, no *necessary or automatic* link between aspects of a person's private life (or indeed their private history) and their fitness for office. Information about a public figure's private life might nonetheless well connect with, and thus have relevance to, his/her fitness for, or function in, public life. However, such a connection would need to be positively established before publication could take place under this defence. We see nothing in the case law under the European Convention on Human Rights that is at variance with this position. While this defence will in practice relate mostly to classic public figures such as politicians it might also potentially apply to others with a similarly high profile including leading corporate executives.

Need to Prevent Public from Being Misled

2.41 **Fourthly**, there is a potential public interest in publishing information concerned with a person's private life in order to prevent the public from being misled by the public utterances or positions taken by them [see Head 3(3)(d)]. In our view this defence should only be available where the public figure (or putative public figure) has by his/her own conduct or statements put an issue into the public domain. It is not the status of the person *simpliciter* that activates the public interest under this strand of the defence. It is some voluntary act or statement that helps to establish or maintain a position or profile that is at odds with the person's true convictions or actual private behaviour. Thus, an *exposé* on the private life of a silent backbencher would not be warranted under this heading. Furthermore, it is only that which shows the contradiction between a public stance and a private reality that is potentially exposable under this defence. The publication of unrelated aspects of a person's private life in order to corroborate a suspicion about a contradiction between a public utterance and private beliefs or behaviour to the contrary ought not normally to count.

(b) *Qualifications to the Public Interest Defence*

2.42 We envisage the following qualifications to the public interest defence as outlined above.

Public Interest Defeated where Harassment Involved

2.43 **First** of all, as already mentioned, it does not apply where the information, etc., has been obtained by way of harassment. The case for publication on the grounds of the public interest is less convincing where the information has been obtained by means of harassment, with its overtones of physical intimidation, than when it has been obtained by surveillance. The public interest in publication is overborne in our view by the immediate and direct public interest in preventing harassment which disturbs the public peace. No encouragement or comfort whatever should be provided whether directly or indirectly by the law to those who engage in harassment or to those who (innocently or otherwise) seek to gain by the results of such harassment.

Requirement of Proportionality

2.44 **Secondly**, the publication of details of a person's private life for the sake of salaciousness should be considered excessive and therefore unlawful [see proviso (b) to Head 3]. It is entirely right that some notion of proportionality should apply since the power to publish in the public interest is an exception to the right of privacy and must be read accordingly.

Defence not Available in Cases of Complicity

2.45 **Thirdly**, the entity engaged in the publication must not have been party to or privy to the act of privacy-invasive surveillance. It would be entirely unconscionable in our view to allow such an entity to gain a direct advantage through its own wrongdoing [see proviso (a) to Head 3].

Defence not Available Where Criminal Acts Occur

2.46 **Fourthly**, the defence should not be available where the acts of privacy-invasive surveillance in question involved, in the opinion of the court, the commission of any of the acts specified in the list contained in the Schedule to these Heads [see proviso (a) to Head 3]. Most of these already - or will be if our recommendations are acted on - constitute criminal offences. The list includes illegal interception, breaches of the *Data Protection Act, 1988* and the *Criminal Damage Act, 1991*, spying on conversations by using aural or visual surveillance devices and unlawfully entering or remaining on private property in order to obtain personal information. We view it as axiomatic that no one should be allowed any benefit arising from the infraction of the criminal law even if they themselves were not party to the infraction.

Defence Only Goes to Publication - Not to Newsgathering Acts that Violate Civil or Criminal law

2.47 **Fifthly**, this defence applies only with respect to publication. We do not recommend that it be made available with respect to acts of privacy-invasive surveillance undertaken for the purpose of information-gathering. We have

considered carefully whether the public interest defence should extend to such news-gathering acts preparatory to publication and we have decided that it should not.

2.48 The argument for so extending the public interest defence builds on the insight that the rationale behind the public interest defence in the context of publication concerns enhancing the quantity and quality of political ideas and information in the democratic marketplace. If so, the argument runs, then the defence should reach further back along the chain of activities that may start with surveillance and end with publication.

2.49 However logical that argument may appear to be,¹¹ sooner or later it clashes with one of the central tenets of the rule of law; namely, that the law should apply equally to all. To allow the defence to reach news-gathering activities would tend to make the individual news-gatherer a judge in his own case. Stories might be chased and information obtained in a privacy-invasive manner on a mere hope or expectation that the public interest defence would apply. Actions might be justified retrospectively if at all. We fear this gives too much scope for self-serving interpretations of the law.

2.50 Furthermore, the public interest defence is itself a creature of peculiar norms that explicitly protect expression. To be sure, the European Court of Human Rights in its recent decisions has begun to recognise that the formal act of expression cannot be completely separated from the environment within which journalists function. This entails an alertness against legal norms that unnecessarily impede those activities. However, that does not mean that every information-gathering act can or should be made immune to suit under a public interest theory.¹² We are reinforced in our view by what the U.S. Supreme Court described as

"the...well-established line of decisions holding that generally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news."¹³

2.51 As the court explained in that case,

"the truthful information sought to be published must have been lawfully acquired. The press may not with impunity break and enter an office or dwelling to gather news... It is, therefore, beyond dispute that '[t]he publisher of a newspaper has no special immunity from the application

11 See, e.g., Paul A. LeBel, *The Constitutional Interest in Getting the News: Toward a First Amendment Protection from Tort Liability for surreptitious Newsgathering*, 4:3 William & Mary Bill of Rights Journal 1145 (1996). See also, Note: *Privacy, Photography and the Press*, 111 Harv. L.Rev. 1986 (1998).

12 This analysis coincides generally with the views expressed by Professor Raymond Wacks, *Privacy and Press Freedom* (Blackstone, 1995); see chapter 5: *Media Intrusion*, pp. 124-143.

13 *Cohen v. Cowles Media Co.* (a 5:4 decision) 501 U.S. 663 (1991) at 669-70.

of general laws. He has no special privilege to invade the rights and liberties of others'.¹⁴

Therefore, both because of the imperatives of the rule of law and because the public interest theory is generally derived from legal protections that protect expression, the public interest defence should apply only in relation to disclosure.

CHAPTER 3: THE PRIVACY PROBLEM AND THE INADEQUACY OF EXISTING LAW IN IRELAND

3.1 In this chapter we review briefly the nature of the problem posed by surveillance and the inadequacy of domestic law to cope. We then proceed in the next chapter to build the case for reform in the shape of fresh legislation.

1. The Existence of a Privacy Problem

3.2 We distinguish between two levels where intrusion can occur. The primary level - the core focus of this Report - concerns particular acts of surveillance including, for example, the use of long-range telephoto cameras or listening devices. The secondary level - which is not our core focus but which is nevertheless implicated by our core focus - concerns the publication of information obtained as a result of privacy-invasive surveillance.

3.3 As already indicated in detail in section 3 of Chapter 1 of this Report our answer to the question whether there is a privacy problem with respect to the **primary level** - i.e., acts of privacy-invasive surveillance - is an unqualified yes.

3.4 Surveillance and interception activities are often unobtrusive and, for that very reason, difficult to notice and detect. Most people are (and remain) ignorant of the fact that they are - or have been - the subject of privacy-invasive surveillance. This is through no fault of their own but is a function of the nature of the technology in question which is as unobtrusive as it is highly intrusive. Easy assumptions about ease of mind in public places are no longer as well-founded today as in the past.

3.5 Furthermore, the very existence and widespread availability of sophisticated technology - technology designed to scrutinise private life - renders it highly implausible to think that it is not used (and, in the absence of legislation to control its use, abused on occasion) by a variety of actors. This problem is likely to get worse and not better given the free availability of the technology (including through mail order delivery) and in the context of a legal vacuum where the use of that technology is not comprehensively regulated. Moreover the list of monitoring devices contained in chapter 1 above makes it clear that many of the devices are capable of, or are even specifically adapted for, spying on people in private places.

3.6 As is natural in any process of rapid change, society has tended to passively acquiesce in the introduction and use of new technology without a full

appraisal of its dangers as well as advantages. The result has been uncertainty about the reach of the existing legal regime and the creation of a legal vacuum. For example, there are no legal safeguards dealing specifically with the installation of surveillance devices in public places. The Gardaí are not required to undergo any form of due process requirements before resorting to surveillance. This is not to say that this power has been misused by the Gardaí - but it is to say that there is a privacy problem in as much as satisfactory assurances in law against misuse are not presently provided for.

3.7 It must be added that modern technology is not the only reason why protection under the law is required against privacy-invasive surveillance. Surveillance including privacy-invasive harassment by more traditional methods remains a continuing source of serious problems.

3.8 When the possibilities which flow from the use of highly sophisticated privacy-invasive technology are added to the use of such more traditional methods, the case for protection under the law becomes all the more imperative. This is a case of technology outpacing the capacity of the law to cope and is a classic case for law reform. The number of proven instances of abuse is not determinative. The crucial variable is the element of almost helpless exposure and insecurity introduced by new technology.

3.9 In response to the question whether there is a problem at the **secondary level** - i.e. publication as a result of privacy-invasive surveillance - our answer is a qualified yes.

3.10 There arises the temptation, so far generally resisted in the Irish media, to follow the example of sensationalist and privacy-insensitive foreign media imports in order to match circulation. This temptation is likely to grow and not diminish as the penetration of foreign media into Ireland increases. Ireland is already one of the most open markets in the world for foreign media penetration and is therefore more vulnerable than most to these kinds of market pressures. It is entirely prudent to seek to maintain high standards and, in so doing, to take full account of the growing threat posed by some elements of the foreign media.

3.11 A general law to which all media outlets are equally bound would deny any one actor a competitive advantage in succumbing to this temptation. Such a law would introduce a genuine level playing field where any deviation from high standards would not confer a commercial advantage.

3.12 Any process of self-regulation which merely administers a rebuke after the fact is not likely to prove robust enough to maintain standards in the face of increasing market temptation in our view. The enactment of a law forbidding privacy-invasive surveillance is, in our view, as much in the interests of the media as it is in the interests of the right of privacy.

3.13 It is doubtless true, as was pressed on the Commission in submissions, that there has been a low level of official *complaints* about invasions of privacy - and especially as a result of surveillance - in Ireland.¹

3.14 In view however of the availability in particular of the sophisticated surveillance technology already described, and of copious reports from the media that it is being used², we consider that it would be an error to draw the conclusion that there is no problem which requires to be addressed in this country. As stated in paragraph 2.4 of our Consultation Paper, the precise extent to which surveillance occurs in Ireland is unknown, but media reports suggest that surveillance by both public and private actors (including the media themselves) is not uncommon. When one takes also into account the established existence in Ireland of a substantial and so far unregulated private investigation and detective industry (which however is responsible for a part only of the surveillance which takes place) it seems to us that it would be extremely naive to conclude otherwise than that there is a real threat to the human right of privacy in this country.

3.15 There is no shortage of potential human subjects from all walks of and stations in life for privacy-invasive surveillance in today's Ireland. Some but by no means all of these are seen to belong to the rich, powerful and influential classes, both Irish and foreign. Surveillance of ordinary people is well capable of yielding highly profitable material. In the absence of privacy-protective legislation there are now many inviting targets for gratuitous surveillance by both national and international media and other interests.

3.16 While many, perhaps most, of the actors who use surveillance technology may have some legitimate reason for doing so, there is in our view a clear necessity to regulate surveillance and so provide adequate assurances to the public in the form of remedies, both civil and, where appropriate, criminal, which are likely to prove effective to prevent abuses before they occur or compensate adequately for or penalise intrusions after the fact.

1 In the specific context of the track record of the Irish media see the valuable work of Boyle & McGonagle, *A Report on Press Freedom and Libel (1988)*; and *Media Accountability: The Reader's Representatives in Irish Newspapers (1995)*.

2 For a spread of recent media reports on the subject see Roisín Ingie, *Technology erodes privacy by stealth*, *The Irish Times*, 13 April, 1998; Lucille Redmond, *Suddenly there came a tapping...*, *Sunday Business Post*, 9 March 1998; Padraig Yates, *Urgent Meeting sought over secret camera*, *The Irish Times*, 23 April 1997; Padraig Yates, *Baggage handlers at airport vote to strike*, *The Irish Times*, 13 May 1997; *Spy cameras firm refuses to apologise*, *Irish Independent*, 11 March 1997; Aine de Paor, *Ryanair using detectives to spy on us*, *The Irish Times* 7 March 1998; Catherine Cleary, *No Spying on customers, says Dunnes Stores*, *The Irish Times*, 13 February 1998; *Cork Choir paid for surveillance*, *The Irish Times*, 28 February 1998; Barry O'Kelly, *Video Doc to Face First of 40 Charges*, *The Star*, 1 May, 1997; Richard Balls, *Rape victim photo criticised*, *The Irish Times*, 8 December, 1997; Geraldine Kennedy, *Bishop's calls in Mexico taped secretly by author*, *The Irish Times*, 13 April 1997, and related article in same issue by Lorna Siggins, *No obvious legal redress open*; John Waters, *No redress against invasion of privacy by the press*, *The Irish Times*, 29 October 1996. See also *Watching the Detectives*, *Law Society Gazette*, January/February 1997.

3.17 If there is a problem regarding surveillance then there is, at least *prima facie*, a corresponding problem to be addressed regarding the disclosure or publication, where this occurs within the State, whether by the media or others, of the fruits of such surveillance. When one takes into account the openness of the Irish market to penetration by low-priced tabloid newspapers from the United Kingdom in particular it becomes difficult to escape this conclusion. The fact that there is no legislation in the United Kingdom in the area covered by the recommendations in this report does not alter the fact that British Governments over the past thirty years or more have commissioned reports from a number of expert committees as to the need for such legislation and have repeatedly been advised, having regard to experience in that country of privacy-invasive behaviour by the media in particular, that such legislation, covering both intrusions into personal privacy and the disclosure and publication of information thereby obtained, is called for. Although it is accepted that the standards observed by the media in Ireland have in general been considerably higher than those of some of their counterparts in the United Kingdom, it would to say the least be imprudent to ignore the potential influence on standards in Ireland of those of the media in the United Kingdom.

3.18 In short, Ireland can no longer be taken to be an "island" either in the surveillance sense or in the sense of disclosure and publication of information obtained by surveillance, but is part of a larger information market in which, for reasons which we make clear in this Report, it has already been widely (if not universally) accepted that legislation to protect the right of privacy is necessary. Unfortunately, the supply of the fruits of media intrusion into people's private lives tends to create its own demand and to offer a premium for further such intrusion and publication. We are firmly of the view that the time is now ripe for measures to control this situation in the interests of the general public. As far as these measures would affect the media we would seek to buttress high standards there while not taking away from the liberty of the media to champion the people's right to know in suitable cases.

3.19 In remainder of this Chapter we review briefly the constitutional template supporting a general right of privacy and the question whether it is sufficient without legislation.

2. The Constitutional Template

The Constitutional Right of Privacy

3.20 Irish constitutional law does place great emphasis on human dignity and strongly supports a right of privacy. But, as will be seen below, we are of the view that reliance on constitutional means of redress alone is insufficient. There is a palpable need to move beyond general constitutional protection to create effective means of redress in positive law. Irish positive law fails to deliver a comprehensive and effective means of protection at present. The glaring gap

between high constitutional promise and practical legal provision needs to be closed.

3.21 The right of privacy is now well established in Irish constitutional law. Although it is nowhere specifically mentioned in the text of the Constitution, its existence has been implied by the courts from several textual sources including Article 41 (the Family) and Article 40.3.1. (unenumerated rights of the person).

3.22 There are at least two general anchorage points to privacy in Irish constitutional law - both of which offer strong and positive support for the recommendations of this Report.

3.23 The first anchorage point turns on the implication of a right of privacy from a variety of rights already protected explicitly in the text of the Constitution. These include textual rights dealing with

- the Family (Article 41) and the Family in the context of Education (Article 42);
- the inviolability of the dwelling (Article 40.5);
- the right of private property (Articles 43 and 40.3);
- the freedom to form associations and unions, to assemble peaceably and without arms (Article 40.6);
- the freedom of conscience and the free expression and practice of religion, etc. (Article 44);
- the guarantee of privacy in voting under Article 16.1.4° (the secret ballot)³.

3.24 The courts typically imply privacy in or from these textual rights in order to give them a heightened measure of efficacy.

3.25 *The family based on marriage* is a special and highly valued kind of human association under Article 41. It was felt necessary by the Supreme Court in *McGee v. Attorney General*⁴ and its progeny to imply privacy into Article 41 in order to advance the interests of the family and its members and to more fully honour the social functions it serves. Some confusion seems to exist over whether privacy should be conceptualised exclusively as a "shield" that immunises decision-making capacity or autonomy over certain "matters" from outside intrusion or whether it attaches more to those "matters" themselves that lie behind the shield. If the latter approach is correct then the question naturally arises whether those "matters" should more properly be the subject of separately denominated constitutional rights (e.g., the right to beget children within the family). This confusion merely reflects the more general distinction alluded to earlier in this Report between viewing privacy as a shield and/or viewing it as

3 See McCarthy J., *McGee v. Attorney General*, [1984] I.R. 36 at p. 100.

4 [1974] I.R. 284.

attaching to certain "matters" (and only those "matters") that lie behind that shield.

3.26 Regardless of whichever approach one takes, it is clear that marital privacy receives quite strong protection under Article 41. This constitutional anchor is of relevance to this Report. It points strongly in favour of a presumption that, with respect to the intimacies of marital life, and absent a compelling and clearly established case, such intimacies ought to be immune from unwarranted intrusion through surveillance and any resulting publication.

3.27 *The inviolability of the dwelling* as protected by the Constitution (Article 40.5) is also of particular relevance to the subject of this Report. This may be conceptualised as a way of protecting privacy albeit in the limited context of a private dwelling. This, no doubt, reflects the value placed by the common law on property and on the associated right to enjoy the amenities of private property in privacy. It thus forms an added element of the overall privacy "shield". However, it was not "constitutionalised" under the rubric of property but instead under Article 40 which deals more generally with the fundamental rights of the person. Hence, although the protection afforded by the right attaches to a dwelling, it primarily avails persons who inhabit or simply visit dwellings. Such persons need not have any property interest in a particular dwelling to benefit from this right. This points to a presumption of a very strong protection of privacy within the confines of a "private dwelling". The right would seem to be equally capable of violation whether by physical intrusion or by using long-range audio or video devices.

3.28 *The right of private property*, which is protected under a combination of Articles 43 (property) and Article 40.3.1° (the guarantee to protect and vindicate rights against unjust attack), further bolsters the right of privacy. The legal concept of property relates primarily to relations between persons with respect to things. To denominate property as private means to establish a relationship of relative exclusivity between an owner of a thing and others in relation to that thing. The right or prerogative to exclude is bound up with the concept of property and is therefore, *inter alia*, one more way of protecting privacy. This points to, and further augments, the protection of the inviolability of the dwelling and arguably extends it to cover other real property including a garden, curtilage or office. Indeed Article 8 of the European Convention is now been interpreted to apply in an office and commercial setting (see chapter 5).

3.29 The **second** anchorage point for privacy in the Constitution turns on a consideration of human personhood - on what it means to be a human being and the need for some islands of withdrawal in which the person may flourish. Hence, some judges in *McGee* let privacy rest on the more general provisions dealing with the unenumerated rights of the person under Article 40.3.1°. In this vein one judge in a later case viewed privacy as necessary for the "expression of

the individual personality"⁵ and as flowing "from the Christian and democratic nature of the State".

3.30 This anchor rests on a much more plenary view of the person detached from any particular relationships he or she may have. Furthermore, it is not tied to property or a dwelling. It therefore presumptively creates personal space that can follow the person from context to context and stands to be calibrated (but not extinguished) as the person passes through different spaces (public and private or *vice versa*). This anchor is of relevance to this Report since it makes it plain that privacy may be violated outside the intimacies of personal relationships by, *inter alia*, intrusions into purely personal space.

3.31 In this context it is relevant to recall the words of Hamilton P. in *Kennedy v. Ireland* where he wrote 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.⁶

3.32 It is this connection to dignity that affords privacy such a potentially expansive character. This finds strong echoes in the jurisprudence of the European Court of Human Rights which premises the Article 8 conception of privacy on the "physical and moral integrity of the person" (see chapter 5).

3.33 This points to a personal right of privacy that exists no matter the context (albeit affected by the context) and regardless of whether privacy is already indirectly protected e.g. through property or the inviolability of a dwelling. It gives rise to a "reasonable expectation of privacy" even in public places.

3.34 From the above it can be fairly deduced that

- the protection of the Family (Article 41) points strongly toward protecting the intimacies of marital life;
- the protection of private life through the inviolability of the dwelling (Article 40.5) renders the dwelling off limits to all forms of intrusion save "in accordance with the law";
- the protection of property (Articles 43 and 40.3) subserves privacy and perhaps extends this to cover real property not used as a dwelling;
- the personal right of privacy (Article 40.3) rests on an expansive view of human dignity and presumably has the capacity to follow the person into public space. (It would be reasonable to assume that it covers marital intimacy, intimacy with others,

5 per Henchy J. in *Norris v. Attorney General*, [1984] I.R. 36 at 71-72.

6 [1987] I.R. 587 at 593.

- sexual orientation and history and personal diaries. There has, however, been little clarification so far of the issues which arise from the constitutional caselaw on surveillance.);
- the constitutional right/s to privacy remain to be given clear and practical content in the day to day life of the citizen. The process of developing caselaw depending as it does on the happenstance of relevant litigation arising before the courts seems an uncertain, uneven and slow method of achieving this in the absence of specific legislation.

Surveillance in Constitutional Litigation

3.35 The specific issue of surveillance has received some attention in the courts from the perspective of constitutional law.

3.36 For example, in *Kane v. Governor of Mountjoy Prison* the Supreme Court endorsed the police surveillance involved in that case provided adequate justification exists for it on the facts of the case and considering the importance of the duty being discharged by the police (apprehension of a person for whom the delivery of an extradition warrant was imminent) and the extent and nature of the surveillance. This was not a case of covert surveillance but involved overt surveillance where an added concern about personal liberty was in issue. That this issue could be aired before the superior courts is a good thing. However, it would be preferable, in our view, to provide a basis in positive law for such police action especially where it involves covert surveillance. The need for a positive legal basis for such official action is in fact required under Article 8 of the European Convention (see chapter 5).

3.37 In *Kennedy v. Ireland*⁷ the High Court established that a person enjoys a personal constitutional right of privacy in his/her telephone conversations and the right is breached by deliberate, conscious and unjustifiable interference with such communication. Interference might be justified where required on the grounds of the protection of the constitutional rights of others, the common good and public order and morality. No such grounds arose properly on the facts of the case. This case was one of the factors that led to the introduction of comprehensive legislation governing telephone interception in 1993⁸.

3.38 In *DPP v. Kenny*⁹ the High Court held that it was not a breach of privacy for those who have lawful custody of a person to observe him. Common sense alone would dictate that a person's right of privacy is drastically altered (though not eliminated) whilst under lawful incarceration. This case finds echoes

7 [1987] I.R., 587.

8 *The Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993* (See Ch. 6 of our Consultation Paper).

9 [1992] 2 I.R. 141.

in the jurisprudence of the European Court of Human Rights. The limits of the privacy-intrusive prerogatives of those who are in lawful custody were not adumbrated but undoubtedly exist under Irish constitutional law.

3.39 More problematically, the High Court in *Nason v. Cork Corporation*¹⁰ the High Court ruled that photographic evidence that tended to show that the plaintiff in a personal accident case had not in fact suffered the injuries complained of was admissible. The Court rationalised the admissibility of the evidence on the ground that the plaintiff had a reduced expectation of privacy even when in her own home with the curtains undrawn and on a public street and furthermore that it would be anomalous to require answers to questions in court that opened up the plaintiff's private life and yet not to allow for far less intrusive photographic evidence. In a sense, the greater power of the court to compel answers was taken to include the lesser power of a photographer to take photographs in public or semi-private places. It might have been preferable to handle the privacy issue presented in this case in terms of the strength of the countervailing rights, powers and duties of the defendant (and its agent, the investigator-photographer) rather than simply assume that the greater power of the court always includes the lesser power of the private investigator. In its own way this case shows the need for detailed legislation governing the kinds of activities involved.

3.40 In *Devoy v. The Right Honourable Lord Mayor, Aldermen & Burgesses of Dublin, Beattie, Heavey & Brooks*¹¹ the High Court allowed the admission of a secret tape recording of a workman into disciplinary proceedings by analogising it to a photograph. This was a form of participant-monitoring. An issue of this kind could be handled under our present proposals by announcing (or rejecting) a "reasonable expectation" of privacy against such secret taping of a conversation, having balanced the intrusion against other individual rights and interests.

Conclusion

3.41 The existing caselaw of our Superior Courts contains clear statements of a constitutional right of privacy and of freedom from unjustified surveillance. Nonetheless, the content and limits of this right are unclear and do not permit the citizen, the media or others concerned to determine with even reasonable certainty their rights and obligations in this sphere. How can this uncertainty best be addressed? In our view, expansive judicial interpretation of the Constitution or judicial reform of the common law are likely to remain a poor substitute for legislative change in the sphere of privacy. To say this is neither to criticise the role of the courts nor to criticise the judiciary. Judge-made law is entirely dependent on the claims that happen to make it to court. Only those parties with sufficient resources are likely to have the wherewithal to test the

10 *Ex tempore* judgment of Keane J., High Court (Unrep., 12 April 1991). See our Consultation Paper, para. 3.21.

11 Judgment of the High Court (unreported, 13 October 1995).

outer limits of the law. The fact that impecunious plaintiffs, in particular, can sometimes succeed in securing legal representation does not alter the general truth of this statement. The kinds of claims that make it to court will be narrowed down to a series of net points which may not adequately capture the full spread of concerns (and competing rights) at play in the field. This merely points to the weakness of the adversarial processes as a way of engaging in rational law reform. Furthermore, standing will be allowed only for those directly involved in the case at bar. In an area of such public importance as this, it is surely better for the law to evolve in a manner that allows maximum public debate and participation.

3.42 There is then, in our view, a need to translate constitutional guarantees into prescriptive detail and a need to go beyond the piecemeal evolution of the common law. This is a situation which calls for legislation to give specific content and effect to the constitutional principles concerning the constitutional and civil right to privacy which have been enunciated by the courts while providing for certain specific defences to any complaint of infringement of these rights and also providing that the proposed new statutory right to privacy would not purport to override any relevant constitutional rights of the defendant nor indeed that the limitations in the proposed legislation would not override any such rights in the plaintiff. The recommendations contained in this Report are intended to do this.

3. The Inadequacy of Domestic Law

3.43 In this section we review briefly

- (a) the inadequacy of relevant aspects of existing civil law to provide comprehensive protection without legislation; and
- (b) the inadequacy of existing criminal law to reach the most egregious of violations.

Fuller details are contained in our Consultation Paper.

3.44 We furthermore refer, for completeness, to

- (c) data protection legislation;
- (d) the impact of the recent freedom of information legislation;
- (e) broadcasting regulation; and
- (f) non-statutory codes of practice.

(a) Existing Civil Law Protections

3.45 Several common law torts play a part in protecting privacy or at least certain aspects of privacy. These are listed below. Commentary which appears

in our Consultation Paper is not repeated here, but reference to the relevant paragraphs of that Paper is given below.

Trespass to Land

3.46 [See Par. 4.4 - 4.8 of our Consultation Paper]

Trespass to Chattels

3.47 [See Par. 4.17 - 4.18 of our Consultation Paper]

Trespass to the Person

3.48 [See Par. 4.13 - 4.16 of our Consultation Paper]

Private Nuisance

3.49 [See Par. 4.9 - 4.12 of our Consultation Paper]

Breach of Statutory Duty

3.50 [See Par. 4.29 - 4.32 of our Consultation Paper]

Defamation

3.51 [See Par. 4.19 - 4.21 of our Consultation Paper]

Malicious Falsehood

3.52 [See Par. 4.22 - 4.24 of our Consultation Paper]

Passing Off

3.53 [See Par. 4.25 - 4.28 of our Consultation Paper]

Breach of Confidence

3.54 [See Par. 4.33 - 4.63 of our Consultation Paper]

As we explained in our Consultation Paper, the three basic requirements for the application of the equitable doctrine of breach of confidence are (1) that the information is itself of a private nature, (2) that it is imparted in circumstances giving rise to a duty of confidentiality and (3) that its dissemination was unauthorised. There has been a considerable loosening of the second requirement over the past few years which allows the courts to effectively impose a duty of confidentiality in some circumstances in the absence of a specific relationship of confidentiality (indeed any relationship at all) between the parties. So much so that one English judge has stated, albeit *obiter dicta*, that

"if someone with a telephoto lens were to take...a photograph of another engaged in some private act, his subsequent disclosure of the photograph would in my judgment...amount to a breach of confidence...In such a case the law would protect what might reasonably be called a right of

privacy, although the name accorded to the cause of action would be breach of confidence"¹².

3.55 No one is quite sure as to the outer boundaries of the law of confidence nor as to the extent to which it might adequately supply for the place of a full privacy tort. As will be seen, the fact that there appears to be some movement in England toward a more creative judicial interpretation of the outer boundaries to the law of confidence was the main reason why the European Commission on Human Rights rejected the application of Earl Spencer as manifestly ill-founded for failing to exhaust domestic remedies¹³.

Conclusion

3.56 The civil law provides a fragmentary protection of the privacy "shield". It does not add up to the comprehensive protection privacy deserves in the context of surveillance and interception.

3.57 The most obvious gap in the first three torts enumerated above has to do with the use of long-range sensing devices. Most of the other enumerated torts, which deal with informational privacy, do not protect privacy holistically by tackling the subsequent publication of private information. While confidence law has potential, its overall utility in the sphere of this Report is as yet unclear. It is preferable in our view to accelerate and crystallize this trend for organic growth in the common law - if indeed the trend is well founded - through appropriate legislation.

(b) Existing Criminal Law Protections

3.58 A web of common law crimes and statutory offences exist that is of considerable relevance in the context of surveillance and interception. These are listed below. Commentary which appears in our Consultation Paper is not repeated here, but references to the relevant paragraphs of that Paper are given below.

Breach of the Peace

3.59 [See Par. 5.2 - 5.8 of our Consultation Paper]

Harassment

3.60 Section 10 of the *Non-Fatal Offences Against the Person Act, 1997* provides as follows:

"Any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently

12 Per Laws J., *Hellewell v Chief Constable of Derbyshire*, [1995] 4 All ER 473 at 476. For commentary see Helen Fenwick & Gavin Phillipson, *Confidence and Privacy: A Re-Examination*, 55(3) Cambridge L.J. 447.

13 *Earl Spencer and Countess Spencer v. United Kingdom*, No 28851/95, decision on admissibility of 16 January, 1998. See chapter 5 *supra* for further commentary.

watching, pestering, besetting or communicating with him or her, shall be guilty of an offence."

3.61 Harassment is further defined as arising where

"(a) he or she, by his or her acts intentionally or recklessly seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and

(b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other."

3.62 This combines both a subjective and an objective approach to the definition of harassment. Not only must the requisite mental state exist but a reasonable person must apprehend the acts, etc., as violative of peace and privacy, etc. The term "privacy" is also explicitly included but left undefined which allows courts to consider a reasonable view of what constitutes a violation of privacy through harassment.

3.63 Injunctive relief in various forms is available under Section 10 where an offence has been established. Penalties include a fine not exceeding £1,500 or imprisonment for up to 12 months on summary conviction and an indeterminate fine or imprisonment for up to 7 years for conviction on indictment.

3.64 The explanatory memorandum accompanying the Bill stated that the aim of section 10 is to get at the form of behaviour commonly known as "stalking". Section 10 is however quite capable of having many different applications that are of relevance in the context of this Report. It could apply, for example, to persons who persistently follow others in pursuit of photographs. Harassment is defined explicitly to include invasions of privacy by any means including the use of the telephone.

3.65 Section 10 allows for the defence of "reasonable excuse" which is left undefined. It is only applicable where there has been an element of "persistence" involved in the acts in question - it does not therefore apply to once-off situations which can be most damaging to privacy.

3.66 In our Consultation Paper, we requested submissions with respect to the possibility of creating an offence of group harassment¹⁴. We are not convinced that group harassment should amount to a separate offence (i.e., in addition to that created by the 1997 Act) since the criminal law should only be used to penalise behaviour for which the person is individually culpable and section 10 of the 1997 Act in any event covers all forms of proven harassment. It could prove difficult, if not impossible, to determine exactly when an individual bears

14 *op. cit.*, para. 8.29.

criminal culpability for the actions of a group especially where that group forms spontaneously and without any collusion. We do, however, recommend the enactment of a civil tort directed against harassment.

3.67 Where the commission of the tort involved a group of two or more and the presence of the group itself brought added elements such as menace, intimidation and fear we believe that the court could under existing law take this into account in assessing damages.

Eavesdropping

3.68 [See Par. 5.9 - 5.12 of our Consultation Paper]

Statutory Offences to Protect the Mail and Telecommunications

3.69 [See Pars. 5.13 - 5.69 of our Consultation Paper]

Statutory Offences Connected with Computer-Based Information and Communication

3.70 [See Par. 3.92 - 3.95 of our Consultation Paper]

Conclusion

3.71 As with the civil law, the protection of privacy by the criminal law is piecemeal and does not meet the present-day need for protection from surveillance.

(c) *Data Protection Legislation*

Data Protection Legislation and the Transposition of Directive 95/46/EC

3.72 The *Data Protection Act, 1988* advances the interest of the individual in "information privacy" in the context of automatically processed personal information. It was intended to give effect to Ireland's obligations under the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981). An outline of the Act is given in our Consultation Paper, at Par. 5.70 - 5.73.

3.73 *Directive 95/46/EC* of the European Parliament and Council of 1995 must be transposed into the domestic law of the Member States by October 1998. This will apparently be done by amending the 1988 Act. The stated purpose of the Directive is to give further substance to, amplify and modernise the norms contained in the 1981 Council of Europe Convention. It is relevant in the context of this Report in the following respects.

3.74 The Directive applies to personal data which is wholly or partly processed by automatic means (Article 2 (b)). It breaks new ground by extending coverage to personal data processed in such a way as to form part of (or which is intended to form part of) a "filing system". In other words, manual files containing personal data for manual processing are covered. This has implications for the media which has traditionally relied on manual files. Even

without such an extension of coverage to embrace manual filing systems the media were likely to be within the embrace of the Directive in any event. This is so because of the growth in the introduction of new technology (e.g., document management and retrieval systems) into the media sector over the past few years which means that much more automatic processing of personal data is now taking place in that sector.

3.75 The directive itself is divided as follows. Chapter I is general (Articles 1-4). Chapter II relates to general rules as to the lawfulness of the processing of personal data (Article 5-21). Chapter III relates to judicial remedies, liabilities and sanctions (Articles 22-24). Chapter IV relates to the transfer of personal data to third countries. Chapter V relates to the elaboration of codes of conduct (Article 27) and Chapter VI relates to an obligation to establish a national supervisory authority at Member State level and the institution of a standing Working Party at Community level under the Convention (Articles 28-34). Such a Working Party with wide ranging advisory functions has already been established.

3.76 Significantly, the "processing" of personal data is stated by the Directive to include collection and recording of such data (Article 2 (b)). On its face, this would appear to apply to video, audio and photographic surveillance. This would be clearly so in the case of digital cameras whose images could later be uploaded into computerised systems (manually or by direct internet connection). It is also probably true of ordinary still cameras since the stills themselves can be scanned and otherwise used in both automatic and filing systems. This interpretation is fortified by reference to recital 16 which explicitly excludes sound and image data such as video surveillance carried out for the purposes of public security. Put the other way around, recital 16 gives the very clear impression that non-security uses of surveillance lie within the protective embrace of the Directive.

3.77 The substantive protections of the Directive are laid down in Chapter II thereof. Within that Chapter, Article 6 lays down certain principles with respect to data quality including the requirement that the data shall be processed (including obtained or captured) fairly and lawfully, collected for specified and legitimate purposes, that it is adequate for those purposes and not excessive and that it is accurate, etc.

3.78 Article 11 provides that, where data has been obtained without the consent of the data subject (as will nearly always be the case where surveillance has been used), a disclosure should be made as to its existence and related details (e.g., identify of the data controller, the purpose of the processing, recipients of the data, etc.) at the point where any disclosure of the data to third parties takes place. This would potentially include manual or automatically processed files used for journalistic purposes and subsequently published. Article 12 creates a right of access. Independent of disclosure to third parties (through, for example, publication) the data subject shall have the right to obtain from the controller confirmation as to whether or not data relating to him is being processed as well as communication to him in an intelligible form of the data

undergoing processing and of any available information as to their source, etc. (Article 12(a) 2nd indent.). This potentially gives a person the right to demand from a newspaper or broadcaster an account of the information held about him. The data subject has a related right of rectification, erasure or blockage of the data the processing of which does not comply with the provisions of the Directive in particular because of the incomplete or inaccurate nature of the data (Article 12 (b)).

3.79 Quite obviously these provisions are geared toward enhancing the protection of "information privacy". It was, however, realised that their strict application might have deleterious effects on legitimate journalistic activity carried out in the public interest. Particular apprehension seems to have been felt about the right of access to data where the data has not been obtained from the data subject and where it is subsequently published (Article 11). It is to be noted that Article 12 creates a much more general right of access (absent publication) and further provides that such a right includes the furnishing by the data controller to the data subject of "*any available information as to their source*" (Article 12(a), 2nd indent).

3.80 Article 9 was inserted with a view to tempering the full rigour of the data protection rules in the specific context of legitimate journalistic activity. It provides:

"Member States shall provide for exemptions or derogations from the provisions of this Chapter [General Rules on the Lawfulness of the Processing of Personal Data], Chapter IV [Transfer of Personal Data to Third Countries] and Chapter VI [Supervisory Authority and Working Party, etc.] 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.*"¹⁵

3.81 According to the Working Party established under Chapter VI of the Directive, the authority for the insertion of Article 9 was Article F paragraph 2 of the Treaty on European Union (TEU) which states that the Union shall respect fundamental rights as guaranteed by the European Convention on Human Rights¹⁶. At issue was the balance to be struck between Article 10 of the European Convention (freedom of expression) as applied in the context of journalistic activity and Article 8 (right to respect for "private life").

3.82 The following points are noteworthy about the above formulation. First, Article 9 refers to journalistic activity which phrase includes - but sweeps broader than - the activities of the journalistic profession. So although Article 9 will be of benefit to the journalistic profession its full sweep is in fact broader. Secondly,

15 emphasis added.

16 Recommendation 1/97, Data Protection Law and the Media, adopted by the Working Party on 25 February, 1997.

it *requires* appropriate exceptions to be carved out under domestic law. No discretion is left as to whether such exceptions should be created. Thirdly, Member States may carve out appropriate exceptions "*only if they are necessary*". The test of necessity qualifies considerably the scope for exceptions. Fourthly, Member States may carve out exceptions only if necessary in order to reconcile two particular rights- namely, privacy and freedom of expression. Fifthly, the exceptions can touch on matters covered under Chapters II, IV and VI. As such, an Article 9 exception might theoretically reach Article 6 governing the obligation to process (including obtaining or capturing) personal data fairly and lawfully.

3.83 We make no formal recommendation as to the extent of Ireland's margin of appreciation under Article 9 of the directive since "information privacy" is, strictly speaking, beyond the scope of this Report. We do, however, make the following observations which seem to us warranted by our own research and relevant to the subject matter of this Report.

3.84 It would appear that the main intent behind Article 9 is to immunise the internal processing of data within the media sector. As the Working Party established under the Directive has stated:

"Data protection law does in principle apply to the media...Derogations and exemptions may cover only data processing for journalistic (*editorial*) purposes including electronic publishing. Any other form of data processing by journalists or the media is subject to the ordinary rules of the directive."¹⁷

3.85 In particular Article 9 appears geared toward limiting individual rights of access to information held about them by the media. Despite the fact that an Article 9 exception can theoretically reach Article 6 issues concerning, for example, the obligation to process (including obtain and capture) data fairly and lawfully, it does not appear to have been explicitly designed to reach back into and immunise aspects of the information-gathering process as such. Or at least if it has a backward reach it can only do so to the extent necessary to reconcile privacy with freedom of expression as *per* Article 9. The question whether such a reconciliation requires the immunisation of information-gathering activities to advance freedom of expression can only be answered by referring outward to the balance already struck by the European Court of Human Rights between Articles 8 (right to respect for private life) and 10 of the European Convention on Human Rights. As will be seen in chapter 5 and Annex I, the European Court of Human Rights has not yet interpreted Article 10 of the European Convention on Human Rights as granting directly or by necessary implication any broad or plenary immunity from the ordinary rule of law as it applies to information-gathering activities. It is true that limited immunities relating to information-gathering (e.g., presumption of a right to refuse to disclose sources) have in fact been recognised by the Strasbourg Court (see analysis of *Goodwin v. UK* in

17 Conclusions of the Working Group at p. 5 [emphasis added].

Annex I) but the point remains that no broad immunity as such has yet been sanctioned as necessary to balance privacy with freedom of expression. That being so, Article 9 of the directive does not place any insurmountable obstacle in the way of surveillance legislation of the sort we recommend.

3.86 Issues also arise under Article 9 at the other end of the continuum (from information-gathering to data-processing to publication) concerning publication.

Our main ancillary recommendation is to the effect that publication that results from acts of privacy-invasive surveillance should be made subject to civil sanction. Again, we see nothing in Article 9 that undermines this recommendation even though "processing" of data is defined, *inter alia*, to include disclosure. In any event, even if Article 9 were deemed to reach issues connected with publication we consider that the public interest defence we propose would adequately perform the task of reconciling privacy with freedom of expression and fully in line with the case law of the European Court of Human Rights.

3.87 In short, we do not view the Article 9 exception as going directly to the general law - both as it stands and as it may evolve - governing the legality of information-gathering acts. Even if it does it can only do so to the extent necessary to reconcile privacy with freedom of expression and the European Court of Human Rights has not so far carved out any general exception to the ordinary rule of law with respect to information gathering activities. In as much as Article 9 might reach publication we consider that the public interest defence we propose already adequately reconciles privacy with freedom of expression.

(d) Freedom of Information Legislation

3.88 Information privacy is also protected in the context of freedom of information law. The *Freedom of Information Act, 1996* creates a statutory presumption that officially held information should be made available to the public and creates a mechanism and appeals system for obtain the same. Like most such legislation worldwide the Act exempts the disclosure to third parties of personal information held officially (section 38). Personal information is defined in section 2 as

"...information about an identifiable individual that

- (a) would, in the ordinary course of events, be known only to the individual or members of the family, or friends, of the individual, or
- (b) is held by a public body on the understanding that it would be treated as confidential."

3.89 Without prejudice to the generality of the above, such information is stated to include, *inter alia*, information relating to the educational, medical, psychiatric or psychological history of the individual, information relating to his

financial affairs, information relating to his employment or employment history, information relating to a criminal record, etc. It is stated not to include the name of a person who holds office as a director or occupies a position as a member of staff of a public body, etc..

3.90 Section 28 of the Act directs that a request for access to officially held information shall be refused if, in the opinion of the responsible head, access to the record would involve disclosure of personal information (including personal information relating to a deceased individual). Subsection (3) of section 28 goes further to create a discretion to refuse access to certain medical information to a requester where that information concerns the requester and which might, in the opinion of the head concerned, be prejudicial to his or her mental health, well-being or emotional condition.

3.91 Sub-section 5 of section 28 creates a discretion to grant access to personal information if the head decides, on balance, that the public interest in disclosure outweighs the public interest that the right to privacy of the individual to whom the information relates should be upheld. The "public interest" concept is left undefined by the Act and no guidance or general statement of understanding on the notion has so far emanated from the newly established Office of the Information Commissioner. The notion will likely have to be adumbrated through specific appeals to the Office and perhaps in the High Court on points of law.

(e) *Broadcasting Regulation*

3.92 As outlined in our Consultation Paper the *Broadcasting Authority Act 1960* was amended by the *Broadcasting Authority (Amendment) Act 1976* to place RTÉ under a statutory duty not to encroach unreasonably on the privacy of an individual.¹⁸ RTÉ has issued its understanding of this statutory duty to its staff in its *Broadcasting Guidelines for RTÉ Personnel*¹⁹. These Guidelines are quite commendable and compatible with our core recommendations. We go beyond them, however, to recommend harder remedies. A similar statutory duty is created for private broadcasters under the *Radio and Television Act, 1988*²⁰ and in fact forms part of the broadcast contract. Under that Act the Independent Radio and Television Commission (IRTC) is empowered to draw up a code of practice in relation, *inter alia*, to privacy²¹. As part of its work programme for 1998 the IRTC hopes to provide such a code by the end of this year²².

18 The question remains open whether an action for breach of statutory duty might lie in respect of this Act.

19 Published by RTÉ, 1989.

20 Section 9 (1)(e).

21 Section 9(3).

22 Information from the IRTC.

3.93 The Broadcast Complaints Commission is empowered to entertain complaints that the above privacy provisions have been breached. Decisions of the Commission receive some publicity. Apart from being reproduced in the Commission's *Annual Reports* they are forwarded to the Government Information Service for circulation to the national newspapers and, where relevant, are published in the *RTÉ Guide*. The IRTC has to power to terminate the contract of an independent broadcaster for serious or repeated breaches of its statutory obligations.

3.94 The first striking thing is that such statutory regulation exists, in contrast to the situation obtaining with respect to the print media. Secondly, the "remedies" take the form either of a "decision" that attract a degree of publicity or the discontinuance of a broadcasting contract. However, more publicity is not necessarily what the average complainant whose private life has been exposed may want. The suspension or termination of a contract is an extreme remedy that is not likely to be utilised except in the most outrageous of cases.

3.95 It is an open question whether a cause of action for breach of statutory duty might lie in respect of the *Broadcasting Acts*.²³ Regardless of this, however, it would not be appropriate to exclude any group such as broadcasters from the general privacy legislation which we propose.

(f) Non-Statutory Codes of Practice

3.96 In very recent times a variety of self-regulating actors have adopted voluntary codes of practice for themselves.

i. Garda Code of Practice Governing CCTVs, 1995

3.97 The Garda Síochána adopted a *Code of Practice for the Use of Closed Circuit T.V. Monitoring Systems in Temple Bar* in 1995. The Temple Bar system in Dublin was the first to be operated and under the control of the Garda Síochána. A series of fixed cameras are mounted at strategic points and are operated and controlled remotely by the Gardaí²⁴. Since then Garda CCTV systems have commenced on the O'Connell Street area of Dublin²⁵. An Advisory Committee has been established by the Garda Commissioner to help establish priorities in selecting applications for CCTV systems from different locations around the country. At least twenty such applications have been made. Funding is on a shared partnership arrangement with local business community interests although the absence of such funding is not in itself the sole criterion in determining whether an application should be granted.

23 At least one eminent commentator is of the view that such a cause of action would lie: see Eamonn G. Hall, *The Electronic Age: Telecommunication in Ireland* (Dublin, 1993) at p. 271.

24 On Garda CCTV systems see generally Justin Comiskey, *Someone to Watch Over Us*, in special supplement to *The Irish Times* concerning the 75th anniversary of an Garda Síochána, 18 June, 1997 at p. 3 of the supplement.

25 See Press Release, Minister of Justice, 11 April, 1997.

3.98 The Temple Bar Code applies, as the title suggests, to the Temple Bar CCTV project. It is, however, used as a template for projects in the rest of the country although it has not been formally generalised to serve in this way. Its primary function is to reassure the public that the system will be used only for the legitimate purposes of preventing and detecting crime and that basic rights of the citizen will be safeguarded. The Temple Bar system is operated exclusively by the Gardaí and monitored from Store Street Garda Station²⁶. The cameras are stated to be in clear view of the public.²⁷ There is no requirement to notify the public that they are entering an area where they may be subjected to surveillance (although notices have in fact been put up).

3.99 Street activity is monitored and recorded²⁸. Video tapes are to be held in a secure environment within the Garda station and remain at all times under the control of the member in charge of the station²⁹.

3.100 Videos will be re-used after thirty one days unless required for crime investigation and evidential purposes³⁰. All requests to view video tapes or hard copies of tapes must be authorised by the Superintendent in charge of the District and will be confined to the investigation of "specific crimes, activities and evidential matters". The grant of authority will be recorded in the record book of the member in charge of the station. The making of hard copies of video tapes is subject to the written authority of the Superintendent in charge of the District. All authorisations of this nature must be recorded in the record book of the member in charge of the station.

3.101 Video tapes may not be removed from the custody of the member in charge of the station without his authorisation. All authorisations as well as the purpose for which they are granted must be recorded and signed by the member in charge. This record will be made available for inspection by the Superintendent in charge of the District and other superior Officers of An Garda Síochána. Any inspection of the record must itself be recorded and signed.

3.102 A separate section in the Code requires individual Gardaí involved in operating the system to be conscious of the individual rights and freedoms of the person and to take all precautions and safeguards necessary to ensure that these rights and freedoms are protected³¹. Supervisors are mandated to ensure that all uses are appropriate and authorised in the public interest. The member in charge of the Station is affixed with overall responsibility for the orderly use of the system. Individual Gardaí who transgress the provisions of the Code may be

26 Para 2.1.

27 Para 2.2.

28 Para 2.3.

29 Para 2.4.

30 Para 2.5.

31 Para 3.1.

subjected to disciplinary proceedings³². The provisions of the *Data Protection Act, 1989* are stated to apply to video recordings which relate to identified or identifiable individuals³³

3.103 The Code of Practice does not, because it cannot, confer legal rights of redress on those who may have been the victim of a misuse of the system in the event that such misuse is detected. A periodic review is required every three months which involves the Garda Commissioner. It is unclear whether this involves a close review of the appropriateness of the use of the system in the preceding period or whether it is a paper-based exercise preliminary to renewal.

3.104 A consideration of the application of data protection legislation to the use of CCTV systems is contained in Annex III of this Report.

ii. *Code of Practice within the Private Investigators Industry, 1995*

3.105 Private investigators are generally hired by a variety of actors including insurance companies, private businesses, retail outlets, wholesalers, factories and private litigants for a variety of reasons. The interests pursued on behalf of such clients are, in the main, perfectly legitimate. Indeed, we make explicit provision for such legitimate activities under Head 3(1)(ii) subject to a principle of proportionality as to the means used and the degree of privacy invaded.

3.106 There is no umbrella organisation covering private detectives in Ireland. Private detectives are not presently obliged by law to associate with or acquire accreditation from any professional body. We are aware that at least one body - the Confederation of Irish Detectives - has adopted a Code of Ethics which emphasises the responsibility of members to conduct all investigations within the bounds of legality, morality and professional ethics³⁴. The Code mentions privacy explicitly in the context of client's rights and in the operation of services³⁵. The Code of Ethics is incorporated into the By-Laws of the Confederation a breach of which may trigger disciplinary proceedings. Complaints may be made concerning alleged breaches from "whatever quarter" which presumably includes a member of the public who apprehends an invasion of his/her privacy³⁶.

3.107 The recommendations of the *Report of the Consultative Group on the Private Security Industry* will, if acted upon, make a significant difference in the organisation of the industry. The core recommendation of that Report concerns the establishment under statute of an *Irish Security Authority* whose primary

32 This is not part of the Code as such. This information was forwarded by the Department of Justice, Equality and Law Reform.

33 Para 4.4.

34 Rule 6 of the Code of Ethics.

35 Rules 3 and 4 of the Code of Ethics.

36 Schedule 1, Paragraph 1 (a) of the Memorandum and Articles of Association of the Confederation of Irish Detectives Ltd dealing with Disciplinary Procedure.

purpose would be to introduce, control and manage a comprehensive licensing system for the broad security industry. One of the functions of the Authority would be to set minimum standards for certain sectors which presumably includes the private investigators' industry. We do not view the setting of such standards as conflicting with our legislative proposals in any way. On the contrary, we view the elaboration of industry standards as usefully complementing the bedrock legislation we propose in this Report.

iii. Code of the National Newspapers of Ireland (NNI), 1996

3.108 Since our Consultation Paper the National Newspapers of Ireland (NNI) has adopted a Code of Practice on Privacy in July 1997. In essence, the new Code makes a serious and laudable effort at reconciling the human and constitutional right of privacy with matters that lie within the public interest and with respect to which the people have a right to know. We consider that this balance has now been appropriately struck in our own recommendations particularly with respect to the proposed "public interest" defence.

3.109 The major difference between our approach and that contained in the Code is that we provide for a right of recourse to the courts in order to obtain preventive relief or compensation for violations. The main qualification is that our recommendations do not go to all cases of media intrusion on privacy but only those intrusions that result from unlawful surveillance.

4. Summary

3.110 Our view, in short, is that - notwithstanding the existence of a substantial volume of domestic positive law which, in some cases by design but more often by default, addresses problems arising in the sphere of privacy - the law is at present inadequate to afford protection for privacy against unjustifiable acts of surveillance. Nor is it adequate or comprehensive enough to provide the needed ancillary protection against the dissemination or publication of any information that results from privacy-invasive surveillance.

3.111 Codes of Practice (including those outlined above), while valuable, do not give the citizen the protection of the Courts.

3.112 It is against this backdrop of haphazard and uncertain protection that we make our recommendations for a new law against privacy-invasive surveillance. This would encompass but not replace the protections already provided by the patchwork quilt of existing law. More importantly, by focusing on all methods of surveillance it would offer a closure of coverage that is not possible under the present law.

CHAPTER 4: IS LEGISLATION CALLED FOR ?

1. General

4.1 In the previous chapters we looked at the nature of the privacy problem and the inadequacy of the existing domestic law to cope with the problems that result from surveillance. As asserted in Chapter 1, *prima facie* a legislative solution would appear to be called for. However, various arguments have been advanced against adopting a legislative solution. We now examine these.

2. The Arguments Against a Legislative Solution

4.2 We received written submissions from a wide variety of interests including media interests in response to our Consultation Paper. It appears to be accepted by all (and indeed it could not be disputed) that the privacy of the individual including the right of freedom from privacy-invasive surveillance is a constitutional right. This, of course, has to be balanced against other constitutional rights including freedom of expression. It also appears to be generally accepted or at least not disputed that the wealth of new technology now poses a significant threat to the privacy of the individual. It was however argued (both in written submissions and at our "listening exercise") that the media in Ireland have a good record of respect for privacy of the individual and that the appropriate remedy, at least as far as *their* activities are concerned, is self-regulation by means of a code of conduct rather than legislation.

4.4 Our view is that legislation of the type we recommend is both necessary in principle and workable in practice.

4.5 We review below the main arguments put to us against legislation and our evaluation of them.

i. Should the Market - Not the Law - Determine Boundaries ?

4.6 It was variously asserted in some submissions that social *mores* change through time and that these changes affect the boundaries of privacy. We have no difficulty in recognising the essential truth of that assertion. Whether there is a "reasonable expectation" of privacy depends on the particular context (see Chapter 2 above), but the right itself rests on autonomous ethical and legal principles.

4.7 However, the real thrust of the submissions on this point was to the effect that if the right of privacy is open-ended, then its outer boundaries should be determined by the market. Market forces are, it was asserted, sensitive and finely-tuned to public opinion. In sum, market judgments are preferable to legal judgments.

4.8 We reject this approach. It is of course theoretically possible that a "perfect" market will simply reflect and respect implicit boundaries in culture. However, it is just as likely, in our view, that the market itself will alter the boundaries. Furthermore, market mechanisms tend to respect no inherent limitations other than what the market might bear at any point in time. Every society must decide where to place principled limits on the market.

4.9 Moreover, to allow the boundaries of a human right to vacillate in accordance with the market of public opinion is to abandon the position that the right has an autonomous core of meaning. The recognition and policing of boundaries is, in our view, a task of the law and not a task of markets.¹

4.10 This is not to say that courts should not take due account of the way boundaries shift in response to changes in social mores. Indeed we create ample room in our draft Heads of Bill to allow for this. We do not provide an exhaustive definition of privacy but rather provide a list of indicative factors that a court will advert to in determining whether a "reasonable expectation" of privacy exists on the facts of any given case (Head 1(3)(i)). In short, we insist that human rights do have a core of meaning and that, while the inevitable task of adjusting the boundaries of rights is undoubtedly influenced by changing social *mores*, it should be a matter for the courts and should not be abandoned to market forces.

ii. *Is Self-Regulation Sufficient ?*

4.11 It was also pressed on us that appropriate mechanisms of self-regulation, in particular by the media, are both necessary and sufficient.

4.12 In short, it was claimed that the rights of privacy which we now propose are liable to conflict with freedom of the press. Instead of legislating for these rights so that alleged infringements by the media would be adjudicated upon by the courts with appropriate remedies including injunctions and damages, it should be left to the media themselves, in the form of a voluntary body such as a Press Council, to deal with complaints under a voluntary code of press conduct and to determine thereunder what, if any, redress the aggrieved party should receive.

4.13 In opting for a legislative solution we do not intend in any way to decry the valuable role played, or potentially to be played, by the process of self-

¹ See, e.g., David A. Anderson, *Fundamental Issues in Privacy Law*, Clifford Chance Lectures, London 1996.

regulation in this field. Nor, indeed, must our views be taken as negative comment on the content of such voluntary codes as have already been adopted. We greatly welcome self-regulation and the further strengthening of such regulation where it already exists. It is a laudable and necessary effort to take civic responsibilities seriously.

4.14 However, while we view self-regulation as vitally necessary, we do not view it as sufficient, especially in the context of protecting and vindicating fundamental rights. Our reasons are as follows.

4.15 **First** of all, the self-regulatory process does not presently cover all actors who may potentially intrude on privacy. Private investigators are, for example, not presently subject to any compulsory licensing regime and need not belong to any self-regulating affiliation. We are aware of the recommendations of the *Consultation Group on the Private Security Industry*² (which body was established by the Department of Justice) in this regard and assume that its proposals with respect to mandatory licensing would apply to this sector.

4.16 **Secondly**, the self-regulatory process does not typically offer strong remedies in the form of compensation, fines or other preventative measures. The key remedy in our view is not compensatory but preventive. Only a court can provide for such a remedy.

4.17 **Thirdly**, the field to be regulated implicates very profound matters both of human rights and of their interaction with the public interest in publication. These may be in mutual conflict. We cannot agree that the interested parties who would normally be defendants to a court action should instead be allowed to judge for themselves what are a complainant's legitimate expectations of privacy, whether these have been infringed, and whether there is a countervailing justification for the infringement based on the "public interest". In our view, these issues, concerning as they do the fundamental rights of the citizen as well as the freedom of the media, are so important in modern democratic culture that their definition - and policing - cannot be left in the hands of the very sectional interests they purport to regulate. We stress that this is in no way to slight the interested parties concerned but it is to say that the definition and policing of the relevant issues including the "public interest" is of such importance that it calls for a form of regulation that is, *and is seen to be*, neutral with respect to the various interests and rights that compete. Legislation that creates the possibility of legal redress in the courts is the only way to achieve this.

4.18 **Fourthly**, self-regulation, no matter how effective, normally takes place against the backdrop of market forces which, if unchecked by law, have the potential to undermine the whole process of self-regulation. Maverick elements within an industry can always circumvent the self-regulatory process and discredit the good intentions and laudable track record of the majority. We are of the

view that it is entirely plausible to assume that sooner or later, competition for marketable copy within the media tends to result in self-regulation breaking down, and that ultimately if the citizen cannot look to the courts (as opposed to voluntary self-regulation by the media) for protection then the citizen will have little or no effective protection. The courts cannot accord such protection unless it is provided for by the law.

4.19 **Fifthly**, it must always be remembered that law serves other purposes besides making redress available and practicable. The fact that a law exists protecting a particular right does much to symbolise the importance to society of that right. It also serves an educative function for society at large. From this perspective, the fact that infringements might be rare is beside the point. What matters is that the right is considered important enough to deserve both the symbolic imprimatur of the law and the provision of practicable means of redress.

4.20 **Sixthly**, and finally, we note the approach of the European Court of Human Rights which forbids States from absolving themselves of answering for their Convention responsibilities by delegating them (*de jure* or *de facto*) to subsidiary private bodies³. This is not a bar to delegation as such but it does preclude States from thereby absolving themselves of answerability under the Convention. The best way of doing this in our view is to enact a broad statutory framework with effective remedies attached.

4.21 At the end of the day, while we applaud and encourage the trend toward self-regulation, we do not consider it to be a sufficient answer with respect to the subject matter of this Report.

4.22 We have also considered but rejected the concept of "enforced self-regulation". Such a concept entails delegating the drafting of regulations to the very bodies regulated by a framework statute. Such regulations become the legal benchmarks against which the regulated entities must conform their behaviour if approved by a statutory authority. Notwithstanding the undoubted utility of "enforced self-regulation" in other contexts, we do not think that the question of how a fundamental human right should be protected and balanced with other sensitive human rights is a matter that should be delegated to entities that will be affected by the rules eventually adopted.

iii. *Is the Concept of Privacy Amenable to Legislative Expression ?*

4.23 It was also contended that, while there could be no doubting the status of privacy as a human right, its very generality made it unsuitable for expression in statutory language. We reject this argument for the following reasons.

4.24 **First**, the argument about vagueness is something that would go to the expression of privacy at a Constitutional level as well as in the context of legislation. If vagueness were a key determinant of whether a right exists - or deserves enhanced protection - then it might similarly be argued that the right should be withdrawn from the constitutional template, which no one seriously suggests.

4.25 **Secondly**, the very generality of the right at the constitutional level is itself, in our view, an argument *for* legislation. The abstract generality of the right (which is an unwritten right) is a very powerful argument indeed that the State should move beyond vague and somewhat unclear guarantees to set out in clear legislation where it thinks the parameters of the right lie and to provide guidance to courts in reaching conclusions in concrete cases.

4.26 **Thirdly**, and more on point, all principles deemed important enough to warrant legislation prove to be complex and difficult to pin down. The issue is *not* whether they are complex and difficult - *that* can be assumed - but whether sufficient certainty can be found to guide the actions of private parties. In this regard it is to be noted that the Calcutt Committee⁴ in the U.K. was satisfied that there were no insuperable problems of definition. The National Heritage Committee of the House of Commons proceeded to provide its own definition⁵ as did the Lord Chancellor in a Consultation Paper issued in 1993⁶. We believe that the indicators we provide in our draft Heads of Bill in determining whether a "reasonable expectation" of privacy arises on the facts of any given case will yield clear answers in most cases. The mere fact that there will be borderline disputes highlights the need for a court and not the inadvisability of legislation in the first place.

4.27 **Fourthly**, the existing vagueness in constitutional texts is in no one's interests least of all the interests of the person whose privacy is affected. Nor is it in the interests of the various actors who engage in various acts of surveillance that may be held violative of privacy. Indeed, it is not in the interests of the news media which require much greater clarity as to where lines are to be drawn. Private investigators and the media risk the *ad hoc* and unpredictable development of the law through constitutional litigation. Far better to clarify the law through legislation.

4.28 Our recommendations are not designed to deepen or broaden the constitutional protections of privacy. We do not attempt constitutional law reform through the back door. Indeed, our draft Heads of Bill explicitly preserve all constitutional rights to the contrary (if any or to whatever extent). Rather, we seek to give particularity to the bedrock constitutional right of privacy.

4 Report of the Committee on Privacy and Related Matters (Calcutt I), CM 1102 (1990), para. 12.17.

5 National Heritage Committee, Fourth Report, *Privacy and Media Intrusion*, 241-1 (1992-3), para. 48.

6 Lord Chancellor's Department and the Scottish Office, *Infringement of Privacy: Consultation Paper* (July 1993).

iv. *Can the Law Provide an Adequate Balance between Privacy and other Competing Rights and Interests ?*

4.29 It was also asserted that the law is peculiarly incapable of handling with sufficient sensitivity the balancing of privacy with other reckonable rights and interests. This argument goes to a more general debate about the nature and appropriateness of balancing tests in both public and private law. It assumes particular importance in the context of the competition between privacy and freedom of expression. When this argument is reduced to its essentials it amounts to an assertion that no satisfactory formula can be found to reconcile privacy with freedom of expression. We reject this argument - both in general and as it applies in the context of freedom of expression - for the following reasons.

4.30 **First**, it must be acknowledged that legislation, by its nature, must not merely protect a right but also calibrate that primary right with other rights and interests. The mere fact that a right has boundaries and the consequential necessity for spelling out in legislative language how those boundaries are to be identified in individual cases is not in itself a good argument against legislation. If it were then the legislature should never legislate for the protection of important - yet undeniably complex - civil rights.

4.31 **Secondly**, it is conceded that difficult borderline cases will arise. But of all institutions the courts are well used to weighing up in a rational and principled manner the sensitivities involved in balancing competing rights and interests. Indeed this discipline of rationality and principle is one of the distinguishing features of the legal order. It does, of course, take time to develop a fully coherent jurisprudence. But if this factor were to be the deciding one then there would be precious little scope for the legislature to enact laws where the competing rights at stake were of comparable importance. That would not be in the public interest.

4.32 **Thirdly**, our recommendations aim to insert privacy into a balancing equation where no such possibility has effectively existed in the past. In the absence of such a balancing exercise, privacy might be consigned to a rhetorical side-stage and freedom of expression allowed to triumph without the discipline of a contest.

4.33 **Fourthly**, it must be emphasised that the defences we enunciate are broad enough in our view to embrace current legitimate uses of surveillance technology. The benefit in legislating is to reassure the public and to provide accessible remedies where there have been unjustifiable violations of privacy.

4.34 **Fifthly**, we fully realise that freedom of expression is different. It goes to the existence and quality of the marketplace of ideas that is so fundamental in a healthy democracy. That is why we now embrace a conception of the "public interest" defence. We see our conception of the public interest defence as expansive enough to cater for the people's legitimate "right to know" certain

matters whilst protecting against the impulse to intrude beyond that point for purely commercial or other reasons.

4.35 **Sixthly**, we envisage that, where appropriate, the courts may, in advance of the full trial of a claim in tort arising from our proposed legislation, issue interim or interlocutory injunctions to restrain the acts complained of including allegedly unlawful publication. We fully realise that in the context of publication this implies imposing a "prior restraint". It is to be noted that the imposition of prior restraints on publication is not inherently contrary to the European Convention on Human Rights. We feel that the possibility of applying for and obtaining a prior restraint is entirely appropriate in trying to prevent damage before it happens rather than compensate for it after the fact. In our view, privacy is as much, if not more, a perishable commodity than news. Reliance on damages as an exclusive remedy is not appropriate in this context. The threat of prior restraint in narrow and carefully delineated circumstances is appropriate. In our recommendations, where the defendant makes out a good arguable case for the "public interest defence" which we propose, the court may refuse to grant an interim injunction where the justice of the case so requires. The restraint itself will be temporary pending a decision on the merits.

v. *Is Privacy Legislation Futile?*

4.36 Another objection takes the form that legislation in this area is futile. Put another way, privacy - while important - cannot be adequately protected. This, in our view, is a counsel of despair. It is a view which has been rejected by the vast majority of Member States of the European Union. It should not be beyond the ability of the legislature to find an appropriate formula to balance all the competing rights at stake. To give up the effort because of the difficulty of the task is not to take the effort seriously enough.

4.37 The thrust of this argument rests on the fact that the Irish media market is heavily penetrated by foreign outlets. This is undoubtedly true. We seek to counter this by inserting a provision in the Draft Heads (Head 2(iv)) that would subject media imports to the same standards as domestic media outlets subject to certain prudent defences. It would, of course, be preferable to see a multinational - or even regional - convention setting down baseline standards on the subject. Short of that, we see nothing wrong in principle with subjecting foreign outlets to the same law as domestic outlets provided the necessary protections are added for innocent publication.

vi. *Will Privacy Legislation be Exploited by Powerful Parties?*

4.38 The protective regime we recommend will inure to the benefit of all individuals. We do not subscribe to the view that "public figures" abandon their right to privacy merely by entering "public life". We agree with the view

expressed by the Royal Commission on the Press in 1977 (the McGregor Commission) a follows:

"It is sometimes argued that the only true opposition to publication of details about people's private lives comes from those who have something to hide. We do not agree. We believe that everyone has a right to privacy, and that newspapers should only breach it where there is a clear connection with a demonstrable and important public interest."⁷

4.39 We consider that the "public interest" defence we envisage with respect to disclosure through publication will adequately deal with cases where aspects of a person's private life are directly relevant to matters lying squarely within the public domain. Even so, we still insist on a principle of proportionality and on adequate safeguards for the privacy rights of innocent third parties.

3. The Report of the Commission on the Newspaper Industry (the Finlay Report) Considered

4.40 We have had regard to the terms of the *Report of the Commission on the Newspaper Industry* which was issued in June 1996. That Report deals with a wide range of issues affecting the newspaper industry, most of which have nothing to do with the subject matter of our present Report. However, in one respect the terms of reference under which that Report was drawn up do touch in part upon the matters with which we deal in this Report. This is Term of Reference No. 7, appearing in Chapter 7 of the Report of the Commission on the Newspaper Industry, which reads as follows:

"The correct balance between privacy and press freedom including consideration of the desirability of a mechanism for complaint and adjudication and of changes in the libel laws."

In paragraph 7.2 of its Report the Commission on the Newspaper Industry stated that it had reviewed the desirability of a mechanism for complaint and adjudication "within the general context of the maintenance of press standards and ethics."

4.41 The Commission on the Newspaper Industry was not asked to consider the desirability or otherwise of legislation to clarify the legal rights of the citizen *vis à vis* the newspapers in the matter either of privacy generally or of surveillance. Nor were they asked to consider the desirability of legislation to clarify the legal rights of the citizen in respect of surveillance generally, whether carried out by private persons, detective agencies, the State, the newspapers, the other news media or anyone else. It is with the latter, which goes far beyond the

7 *op.cit.* para. 10.136.

subject of Chapter 7 of the *Report of the Commission on the Newspaper Industry*, that we are concerned in the present Report.

4.42 We believe that there is a convincing case for the necessity for legislation of a general kind, applicable to all persons, to control privacy-invasive surveillance including the disclosure of information obtained thereby. In recommending such legislation we would be abdicating from our function of objectively assessing the need for and proposing appropriate reforms of the law if we were to suggest that while the obligations to be imposed by such legislation should be applicable to the citizens as a whole, either the newspapers or the wider news media should be exempted from these obligations on the basis of some separate regime of self-regulation, or the creation of a newspaper or media ombudsman, or such like. To exempt the media from the legislation would not merely be unjustified; it might well be constitutionally vulnerable. In saying this we do not in any sense denigrate any proposal for self-regulation or even for a newspaper or media ombudsman; we consider that such regimes of self-regulation have a valuable part to play in securing compliance, without the need for litigation, with a privacy law conferring legal rights and creating legal obligations. Ultimately however, such legal rights and obligations can only be interpreted and enforced by the Courts.

4.43 It is true that in their Report the Commission on the Newspaper Industry found, as a result *inter alia* of a survey which they undertook, that the standards of Irish newspapers with regards to the proper respect for privacy are generally good, though there is a fear expressed in these findings that these standards may decline because of the perceived lower standards of imported tabloid newspapers. This is a danger to which we also refer in this Report. In our view there is nothing in the Report of the Commission on the Newspaper Industry which would warrant the exemption of the newspapers (or indeed any other news media) from the application of the privacy surveillance law which we propose or which in any way undermines the recommendations which we make in this Report.

4. Conclusions

4.44 The case for law reform in this area rests on the existence of a privacy problem with respect to surveillance, the inadequacy of existing positive law, the prevailing uncertainty as to the content and limits of the constitutional right of privacy and the need to alleviate such uncertainty and inadequacy by legislation. Legislation is the appropriate option for reform since it opens up a process that allows all potential parties to represent their interests and affords an opportunity for a rational and comprehensive framing of the public interest.

4.45 With respect to the arguments put in the context of publication, to leave market forces to their own devices is not an adequate response. Markets are not ends in themselves but serve as a means to certain ends. We value the end of privacy just as much as we do the means of the market and for that reason are

willing to see principled limits on market forces. We acknowledge that the media is not simply a service providing a commodity in a marketplace. It is also a vital tool in keeping the public informed on matters of public interest. It is precisely because of this that we now respond positively to the various submissions made to us and recommend an appropriate "public interest" defence to what would otherwise be wrongful publication in our recommendations.

4.46 Nor are we convinced that self-regulation is a complete answer. The issue calls for hard remedies - and especially preventative remedies - which the self-regulatory process is not likely to provide. As a matter of principle we view the question of the public interest to be of such transcendent importance in this field that its application should be placed in the hands of the courts.

4.47 Like Calcutt and the National Heritage Committee in the United Kingdom we agree that the reduction of the privacy concept to a workable statutory formula is difficult but certainly not impossible. More particularly, we are of the view that the difficulty of finding an appropriate balancing formula between privacy and other rights (especially freedom of expression) is not a good answer against trying. We feel confident that our overall approach - including particularly the public interest defence - adequately reconciles all the principal rights at stake and gives the necessary breathing space for the media in a democratic society.

4.48 Lastly, we do not agree that legislation is futile. It is natural to expect that ways will be explored for circumventing the legislation. That reality is not a good argument against legislation but speaks powerfully to the need to anticipate these efforts and try to provide for them as far as possible. We seek to do this under draft Head 3(1)(iv) with respect (among other things) to publication in the State of information obtained by privacy-invasive surveillance abroad no less than such information obtained by such methods at home.

PART II - INTERNATIONAL BENCHMARKS FOR REFORM

CHAPTER 5: THE PROPOSED PRIVACY LEGISLATION AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS

5.1 Many reservations were expressed both in written submissions and orally at our listening exercise concerning the compatibility of privacy legislation in general - and particularly of the sort we provisionally recommended in our Consultation Paper - with the European Convention on Human Rights. Since these reservations raised issues of principle we decided to do some further research on the matter. Our Consultation Paper did not deal explicitly with the interplay between Article 8 (right to respect for private life) and Article 10 (freedom of expression) of the Convention. The impact of Article 10 was in fact the main point of concern expressed to us.

5.2 We summarise below the main conclusions of our extra research. These conclusions should be read in light of the detailed research paper on this topic contained in Annex I.

1. Article 8 - right to respect for "private life"

5.3 Article 8 reads as follows:

- "1. Everyone has the right to respect for his private and family life, his home and 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."

5.4 The Court has held that the term "private life" encompasses and protects the "physical and moral integrity" of the person¹. The Commission has explicitly interpreted the idea of "physical integrity" to encompass freedom from harassment.²

5.5 The term "private life" has been held to have a dynamic as well as a passive rendering. It is interpreted not merely to protect a person in his isolation or to protect matters pertaining to his "inner circle" but can also create space for the forging of personal relationships³. The Court has recognised that, since such relationships can be forged outside as well as inside the home, the right can potentially adhere to business premises⁴.

5.6 An "interference" will not readily be found with the right where surveillance merely entails the casual observance of people as part of the ordinary and natural incidences of everyday life⁵. This, however, begs the question whether the deliberate targeting of persons even in public places must be tolerated by society. As some learned authors have pointed out, the mere formal denomination of a place as either public or private is not necessarily the deciding factor⁶. In support of that view it can be pointed out that the Court has in fact begun to use the language of "reasonable expectation" of privacy. The use of this language implies a nuanced approach - one that does not presume in a conclusory manner that privacy cannot exist in public places⁷. One factor that might tip a case over the borderline (from an act that one has to tolerate to an "interference" requiring a justification) appears to be the use, or intended use of any information that may result⁸.

5.7 The Court has found positive obligations to arise on the part of states under Article 8. Significantly, it has stated that:

"These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves."⁹

5.8 In determining the kind of measure needed a state enjoys a certain margin of appreciation. This margin is different to the one normally enjoyed by states under the Convention. The "normal" margin of appreciation grants space

1 *X & Y v. The Netherlands*, (1985) 8 EHRR 235. See generally, David Feldman, *The Developing Scope of Article 8 of the European Convention on Human Rights*, [1997] EHRLR 265.

2 *Whiteside v. United Kingdom*, No. 20357/92 76A DR 80 (1994).

3 *Niemitz v. Germany*, (1993) 16 EHRR 97.

4 *id.*

5 *Friedl v. Austria*, (1996) 21 EHRR 83.

6 DJ Harris, M O'Boyle, C Warbrick, *Law of the European Convention on Human Rights*, (Butterworths, 1995), p 309.

7 *Halford v. United Kingdom*, (1997) 24 EHRR 523 at para 45.

8 See generally, S N Naismith, *Photographs, Privacy and Freedom of Expression*, [1996] EHRLR 150.

9 *X & Y v. The Netherlands*, (1985) 8 EHRR 235 at para 23.

to a state to *intrude* upon or regulate the exercise of right. On the other hand, the kind of margin of appreciation here affords a certain amount of leeway to Contracting States to take extra measures to *advance* or *protect* a right in the context of private behaviour.

5.9 Whether legislation is *required* or *permissible* to meet this positive obligation would appear to depend on a web of factors including the aspect of the right at stake, the nature of threat/s posed by third party behaviour, the adequacy of existing legal remedies considered cumulatively, the consequences for the individual of leaving the loss lie where it falls, the prevailing views and practices among the Contracting States, and the finding of an appropriate balance between private life and other competing rights and interests.

5.10 We consider that the kind of legislation we propose lies well within Ireland's margin of appreciation when considered as an aspect of a *positive obligation* of States under the Convention to take measures to advance the right of privacy against the threat posed by third party action. There can be little doubt that the right is fundamental as applied in the context of surveillance. The threats posed are real not least because of the insecurities felt in the complete absence of tailored regulation. Existing remedies capture some claims but not others. The European Commission, which once seemed to inveigh heavily against the law of confidence as substituting for the absence of more direct protections for privacy¹⁰, now seems to genuflect to the apparently expanding nature of this remedy under English law¹¹. This reliance on remedies by proxy merely postpones the day when the limits of such law are clearly reached and when the Commission (or the future unified Court) will have to address squarely the compatibility of the absence of a tailor-made privacy remedy with the positive obligations imposed by Article 8.

5.11 Moreover, the consequences in allowing the *status quo* to persist for the individual and indeed for society at large are severe. Prevailing views and practices (especially in Continental Europe) tend towards - and not away from - legislative responses. In our view, appropriate balances can be struck with other rights and interests. Simply put, our legislative proposals would allow an applicant to claim an "interference" with privacy which would require a justification to be pleaded and proved. Our legislative proposals do not preclude the possibility of such justifications and indeed *widen* the range of justifications by adding on a wholly novel one under Irish law; namely a "public interest" defence to publication under certain circumstances.

5.12 The case law under Article 8 also establishes a need for a legislative basis whenever an "interference" is perpetrated by the State or its agents. Again, this is not to preclude the possibility of pleading a successful defence justifying

10 *Winerv. United Kingdom*, No. 10871/84, 48 DR 154 (1986).

11 *Earl Spencer and Countess Spencer v. United Kingdom*, Nos. 28851/95 & 28852/95, Decision on admissibility, 16 January, 1998.

an "interference" - but it is to say that the process whereby state "interference" takes place must be one that is clearly referable to (and subsumed under) a positive legal regime possessing certain attributes such as clarity, accessibility, etc.. State surveillance is only different in that the very fact that it takes place must in most cases (though not all cases) be kept secret in order to facilitate the detection and prevention of crime¹². This does not entail a *carte blanche* since the case law demands the effective presence of an independent element (usually a judge) in an ongoing supervisory process and the possibility of bringing applications before an independent body (usually a court or tribunal) for review on an *ex post facto* basis.

5.13 At present, all the essential requirements of the Convention, as interpreted in case law, are being met with respect to telephone interception carried out by the state in Ireland (*Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993*). The one significant area of state activity left wholly unprovided for is covert police surveillance. To say that such state action must be governed - permitted and regulated - by positive law is not the same as prescribing the level of due process protections which ought to obtain. The necessity for flexibility in this regard is frankly acknowledged and catered for in our recommendations.

2. Article 10 - Freedom of Expression and its Implications for Privacy Legislation

5.14 Article 10 reads as follows:

- "1. Everyone has the right of freedom of expression. That right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

12

Klass v. Germany, (1978) 2 EHRR 214 at para 58.

5.15 Freedom of expression is implicated by the enactment of privacy legislation of the sort we recommend. However, the clash, such as it is, between freedom of expression and the legislation we recommend occurs most obviously at a level once removed from the core focus of this Report. Our core focus concerns prior acts by which privacy is invaded through surveillance and interception. Our secondary focus is the subsequent misuse of the resulting information, images etc., through disclosure, dissemination or publication.

5.16 Even though the clash between privacy and expression occurs most obviously at a secondary level for the purposes of this Report it is still a clash that requires careful attention. This is so because the various concerns expressed regarding the compatibility of privacy law with freedom of expression raise very serious issues concerning the quality of democracy. Freedom of expression is not merely of importance in its own right but also because it is an essential precondition for effective political accountability. Political speech - and the vital role of the media in providing material information and ideas of relevance to the political arena - is normally afforded the strongest measure of protection under traditional protections of expression. The political function of free speech is, if anything, even more pronounced under the European Convention since that convention was drafted with a keen eye to establishing and maintaining open democratic systems of governance in the aftermath of World War II.

5.17 The European Court is fully alive to the political rationale¹³ of freedom of expression and has given quite expansive protection to such expression. In cases where the expression in question is colourably political or serves a public interest the Court is extremely slow to find any interference as being "necessary in a democratic society". This is so regardless of the legitimate interest at play under Article 10.2. (e.g., maintaining the authority of the judiciary, protecting reputation or rights of others). Any interference is closely scrutinised to assess whether it responds to a pressing social need, whether it constitutes a proportionate response to that need, and whether it possesses clarity, accessibility and predictability.

5.18 The question naturally arises whether privacy legislation in general - or of the type we propose - is inherently violative of Article 10. The Court has never in fact ruled on a direct clash between Article 8 and freedom to publish under 10¹⁴. If a suitable case were to arise, it would be fair to surmise that neither right would be held to be absolute since to do so would effectively amount to negating one Convention right for the sake of another. It would be much more reasonable to expect the European Court to carefully evaluate whether an appropriately sensitive balance had been struck between the two rights concerned under national legislation. Precisely because of the vital role played by freedom of expression in making political accountability real it is likely that the Court would very closely scrutinise any privacy legislation. However, this

13 See, e.g., *Handyside v. The United Kingdom*, (1976) 1 EHRR 737.

14 See, e.g., *Lingens v. Austria*, (1986) 8 EHRR 407 at para 38.

is not the same as concluding that freedom of expression must always prevail over the right to respect for private life.

5.19 The protection afforded to freedom of expression is at its strongest when connected to matters that are squarely political or colourably in the public interest¹⁵. It is entirely reasonable to assume that not all matters relating to a person's private life (even the private life of a prominent public figure) satisfy this criterion. It follows that it would be reasonable to demand some nexus between the matter disclosed and political life or issues that are squarely of public concern. Our view is that the "public interest" defence which we envisage is broad enough to allow for the flourishing of the "people's right" to know certain information while at the same time ensuring that private life is in all other respects fully protected. The "public interest" concept therefore provides a bridging link between private information which, by definition, should normally remain private and the legitimate demands of the democratic marketplace of ideas.

5.20 It also follows in our view that, even with respect to those matters that are of political relevance or relate to matters of genuine public concern, a principle of proportionality would apply as to the degree of intrusion into private life through disclosure. We detect nothing in the case law of the Commission or Court that dictates otherwise.

5.21 Out of deference to the role played by the media in democratic society, the European Court will very closely scrutinise any prior restraints on expression such as a preventive injunction¹⁶. This is not, however, the same as saying that such injunctions are inherently violative of Article 10. In defence of such remedies it could surely be forcefully argued that preventive remedies are preferable to *ex post facto* remedies since privacy is just as much, if not more, a perishable commodity than is news. Such preventive remedies are without prejudice to the right to publish and ought to be handled expeditiously to enable publication to take place if no satisfactory claim of privacy can be made out or if the "public interest" in publication is clearly stated. Furthermore, preventive remedies in general are preferable to damages.

5.22 Of course, publication is but the end-point in a chain of events that commences with information-gathering and that involve much processing and editorialising. Obviously, success at one end of the continuum (publication) depends in no small measure on success lower down the ladder of activities that precede publication. The preconditions for this success are many and varied and include ensuring that legal impediments are imposed only where strictly required to meet the just claims of competing rights. In logic, at least, any solicitude

15 See, e.g., *Castells v. Spain*, (1992) 14 EHRR 445 (limits of permissible criticism are wide with respect to members of a sitting Government) and *Thorgier Thorgjerson v. Iceland*, (1992) 14 EHRR 843 (matters of public concern broadly construed).

16 See, e.g., *Observer & Guardian v. United Kingdom*, (1992) 14 EHRR 153.

toward publication entails at least some solicitude toward the *milieu* in which news is gathered and processed.

5.23 Under the rubric of Article 10 and guided strongly by its democratic philosophy, the European Court of Human Rights is now beginning to reach issues that pertain more to the preconditions for successful publication than to publication itself. The net issue posed in the leading case in this regard, *Goodwin v. The United Kingdom*¹⁷, was whether a court order for disclosure of the identity of a journalist's sources was compatible with Article 10 in circumstances where the necessity for such disclosure had not been convincingly established to the satisfaction of the European Court.

5.24 The Court took the opportunity to enunciate a strong presumption leaning against such disclosure in general in order to better facilitate the functioning of legitimate journalistic activity. It then proceeded to let its ruling against the UK rest on an application of its traditional doctrine on proportionality.

5.25 *Goodwin* is not therefore authority for the proposition that journalists enjoy an absolute right to refuse to disclose. The Court merely found that the justifications proffered in that case were insufficiently compelling. It greatly increased the weight to be ascribed to expression where it is to be balanced with other rights but does not preclude that there may be occasions where those other rights take precedence. More to the point for our purposes, *Goodwin* does not stand as authority for the proposition that journalists have a right, or implicit liberty, or special privilege to violate existing law as it relates to the legality of particular news-gathering acts (e.g., telephone interception or trespass). Indeed the advocates for *Goodwin* were themselves at pains to point out that their client was "claiming no special privilege by virtue of his profession because journalists are not above the law"¹⁸. Put another way, there is nothing in *Goodwin* that requires a Contracting State to make exceptions to any new legislation dealing with news-gathering acts such as the tort of privacy-invasive surveillance we propose.

5.26 An important point to bear in mind is that the secondary torts we recommend which relate to publication apply to *all* information whether private or otherwise obtained as a result of privacy-invasive surveillance. There is a clash not merely between "information privacy" and expression but also between personal space (as protected by the privacy shield) and expression.

5.27 If States choose to delegate the exercise of their responsibilities - or allow traditional mechanisms of self-regulation to continue through acquiescence - they cannot thereby avoid answering for their obligations under the Convention. Ultimately the state is responsible and answerable under the Convention for

17 (1996) 22 EHRR 123.

18 This aspect to the case was referred to by Mr Justice Walsh in his dissenting opinion; see p 151.

securing respect for privacy for all persons and for all mechanisms that purport to do so.

3. Conclusions

5.28 We are satisfied that the right to respect for private life under the European Convention is broad enough to permit the enactment of domestic legislation providing for an enforceable right of privacy. We are also satisfied that such legislation can safely proceed on the assumption that privacy - or a residuum of privacy - may exist in even public places provided a "reasonable expectation" of privacy can be found to subsist therein. The indicators determining whether such a "reasonable expectation" arises are necessarily loose.

5.29 We are further satisfied that harassment can be brought into the overall equation since it implicates both the physical and moral integrity of the person which is central to the concept of private life.

5.30 States do have a positive obligation under Article 8 to secure the right to respect for private life to persons with respect to the actions of third parties. In discharging this obligation states enjoy a certain margin of appreciation in determining which measures are appropriate to achieve this. This is not the same kind of margin of appreciation normally enjoyed and is limited where the measures in question bump up against other convention rights. In our view, privacy legislation of the sort we recommend is permissible in principle under the European Convention as lying within Ireland's margin of appreciation in discharging this positive obligation.

5.31 Any interference with private life by the State must be regulated under positive law. There is a persuasive case to be made, in our view, that Irish law and practice currently fall short of this requirement in the context of covert state surveillance.

5.32 Furthermore, we are of the view that Ireland would be acting within its margin of appreciation under Article 10 in enacting a prohibition against the publication of material obtained as a result of privacy-invasive surveillance. Freedom of expression does not invariably cancel out other rights. The legislative response we envisage would be an acceptable and principled way of reconciling the people's right to know with the imperative of protecting privacy. This is not least because of the 'public interest' defence which we endorse.

5.33 The case law shows that injunctions against publication or prior restraints are not inherently violative of Article 10 and we are confident that the limited prior restraint we propose is justifiable under the Convention.

5.34 Lastly, the solicitude shown by the European Court toward publication is beginning to make its presence felt in activities that are connected to publication. However, there is nothing in the case law to suggest any special

privilege with respect to the extant law (e.g., interception, harassment, trespass) where there is a connection with news-gathering. Still less is there any requirement that fresh (and general) legislation designed to enhance the protection of privacy with respect to surveillance must necessarily make exceptions for journalistic activity.

5.35 In short, we are of the view that the legislation we propose would be compatible with Ireland's obligations under the Convention. We are fortified in our analysis of the need for legislation, and of the kind of legislation required, by the terms of the Resolution on Privacy recently adopted by the Parliamentary Assembly of the Council of Europe which is analysed in Chapter 1 above (full text reproduced in Annex V below).

CHAPTER 6: THE PROTECTION OF PRIVACY IN COMPARATIVE LAW

6.1 In the previous chapter we looked at whether legislation of the sort we recommend is permissible in principle with particular reference to the European Convention on Human Rights. In this chapter we briefly highlight the salient features of the relevant legislative and regulatory measures enacted in other countries.

This chapter should be read against the backdrop of the extensive comparative research carried out and published in our Consultation Paper¹.

6.2 This overview is broken down as follows:

Civil liability for surveillance.

Civil liability for intrusion on privacy through publication.

Criminal liability for invasions of privacy.

General regulatory safeguards.

Due process protections in the context of covert police surveillance.

6.3 While some of the legislation surveyed is general in its nature many laws were in fact tailored to meet the privacy problem posed by surveillance. In most cases (with the exception of the UK) the relevant privacy clause in the domestic constitution either animates or supports the legislative measures adopted.

6.4 Most of the British legislation relates only to interception and covert police surveillance. Additional information on the evolution and current state of the British debate on whether civil and criminal remedies should be enacted is contained in Annex II.

1. Civil Liability for Surveillance

6.5 In many of the countries surveyed the civil law has been used to enhance the protection of privacy in the context of surveillance conducted by private parties.

1

See chapters 10 and 11 of our Consultation Paper.

Germany

6.6 In Germany an invasion of privacy is actionable under section 823(1) of the German Civil Code. Case law has broadened the scope of the protection and the courts are now prepared to award damages for non-pecuniary loss. Damages for non-pecuniary loss caused by unlawful surveillance may be awarded where the infringement of the right is serious and where there is no other means of satisfaction for the plaintiff². Further remedies include an order for the seizure of the surveillance equipment used and an injunction. The scope of the protection now extends to a person's name or likeness.

6.7 Under German law privacy may be protected in public places under certain circumstances³.

France

6.8 In France Article 1382 of the Civil Code imposes civil liability for breach of the right of privacy. In 1970 a right to 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 of Article 9 of the French Civil Code 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 of private life.

6.9 French law also protects against the exploitation of the human personality, that is, unauthorised use for gain of elements of personality such as a name, image or voice⁴. 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 generally⁵. False light presentation is also prohibited.

United States

6.10 In the United States the Federal Courts have developed the common law to the point that a tort protecting privacy is now recognised⁶. This tort is generally refracted into four separate but related torts:

- (1) Intrusion on the plaintiff's seclusion or private affairs;
- (2) Publication of private information about an individual;
- (3) Publication of material that puts an individual into a false light position; and
- (4) Appropriation of someone's personality for commercial use.

2 See, e.g., 26 BGHZ, *Neue Juristische Wochenschrift* 1958,827; and 35 BGHZ 363, *Neue Juristische Wochenschrift* 1961, 2059.

3 NJW 1996, 984.

4 See P Kayser, *La Protection de la vie privée*, 2nd ed, Economica, Presses universitaire d'Aix-Marseille, 1990, pp. 75-81.

5 See P Kayser, *op.cit.* pp.120-144.

6 See generally David W. Leebron, *The Right of Privacy's Place in the Intellectual History of Tort Law*, 41 *Case Western Res. L. Rev.* (1991) 769.

6.11 Intrusion upon the seclusion of another has been interpreted by the courts to cover activities such as eavesdropping on private conversations by wire-tapping and microphones, the conduct of "peeping Toms", and the use of telescopic lenses⁷. The taking of photographs of a person in a public place does not constitute intrusion for the purposes of the tort⁸. Filming a person who is in a private place from a public vantage point does not amount to an intrusion so long as the general public would be presented with an identical view⁹. What this aspect of the tort protects against is, in essence, invasions of territorial privacy.

Canada

6.12 In Canada a number of Canadian provinces have enacted a tort of breach of privacy (British Columbia, 1968; Manitoba, 1970; Saskatchewan, 1974; Newfoundland, 1990; Quebec, Civil Code, 1994). 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."

6.13 The various Canadian Acts do not contain a definition of privacy, but they do stipulate that certain actions are *prima facie* breaches of privacy and among the list given are invariably instances of visual and aural surveillance¹⁰. Saskatchewan, British Columbia and Newfoundland use a "reasonable expectation" of privacy type of test in determining whether a claim properly arises.

6.14 The cause of action does not generally require proof of damages. In British Columbia, Saskatchewan and Newfoundland it must be established that the invasion was intentional and without any claim of right.

6.15 In provinces that do not have privacy legislation the courts appear more willing than hitherto to accept the notion of a common law tort of privacy¹¹.

New Zealand

6.16 Several courts have recently taken steps toward the full recognition of a common law tort of privacy in New Zealand¹².

7 See, e.g., *Rhodes v. Graham*, 1931, 238 Ky.225, 37 S.W.2d46; *Roach v. Harper*, 1958, 143 W.Va.869, 105 S.E.2d 564; *La Grone v. Ohio Bell Telephone Co.*, 1961, 114 Ohio App. 299, 182 N.E.2d 15; *Dietmann v. Time Inc.*, 1971, 449 F.2d 245.

8 *Galella v. Onassis*, 487 F.2d 986 (1973).

9 *Marks v. King Broadcasting*, 618 P.2d 333 (8 Cir. 1984).

10 See, e.g., s.1(4) of the British Columbia *Privacy Act*; s.4(a) & (b) of the Newfoundland *Privacy Act*; and ss.3(a) & (b) of the Saskatchewan *Privacy Act*.

11 See generally, Roger D. McConchie's contribution on Canada in Christian Campbell, (ed.), *International Media Liability: Civil Liability in the Information Age* (Wiley, 1997) 57 at 89.

12 See, e.g., *Bradley Wingut Films Ltd.*, [1993] 1 NZLR 415 and authorities cited in the contribution by Tracey Walker on New Zealand law in Christian Campbell, *Loc. cit.* at 299-303.

2. Civil Liability for "Intrusion" on Privacy through Publication

6.17 Many countries also impose civil sanction against the unjustified publication of private information, images or other material¹³. We do not, of course, propose such a tort in this Report. We merely recommend the enactment of an ancillary tort prohibiting the disclosure, dissemination or publication of any information (whether private in its nature or otherwise), etc., that *results* from privacy-invasive surveillance.

Germany

6.18 Illegally obtained information can be published in Germany only under very limited circumstances. In general terms the German courts take into account the interrelationship of a variety of indicators under three different headings¹⁴:

1. the sphere of privacy exposed;
2. the status of the person in question;
3. the strength (or otherwise) of the public interest in publication.

6.19 The public interest element which is closely tied to the functioning of democratic institutions depends on the level at which the first two elements interact.

6.20 The realm of personal privacy is conceptualised by the courts as divided into three parts; (1) the *intimate sphere* which relates to, e.g., health status, sexual habits, confidential letters and personal diaries; (2) the *private sphere* which relates to family, home or friendships; and (3) the *individual sphere* which relates to a person's public or economic life.

6.21 Status is evaluated by the courts on a three-point scale; (1) "absolute persons of contemporary history" including a person holding a public office or function¹⁵, (2) "relative persons of contemporary history" including someone in the public eye for a specific reason or event usually situated within a definite time-frame (3) a private person who is neither of the above.

6.22 The general rule is straightforward. Even absolute public persons have a right to privacy and their *intimate sphere* is considered beyond scrutiny. Matters connected to their *private sphere* (as understood above) are potentially publishable if the information relates to their public function and contributes to public debate in society. Matters relating to the *individual sphere* of an absolute private person can be reported. Pictures or recordings of public persons taken secretly may only be published if this is absolutely necessary in the public interest.

13 For an overview see Christian Campbell (Ed.), *op. cit.*

14 See Gregory Twalite & Wolfgang Brehm, *German Privacy and Defamation Law: The Right to Publish in the Shadow of the Right to Human Dignity*, [1994] 8 EIPR 338.

15 *Oberlandesgericht, Hamburg AfP 1995, 685.*

6.23 The publication of private information relating to "relative persons of contemporary history" must be confined to the context of that which places them in the public eye. It follows that only those aspects of the person's private life directly relating to an aspect of his/her character that affects public life can be covered.

6.24 Pictures - as distinct from information - can generally be shown or published only with the permission of the subject (*Kunsturhebergesetz*, §22). Permission is not required in the following cases:

- (1) Portraits of contemporary history;
- (2) Pictures where the persons are only accessories to the landscape or another locality;
- (3) Pictures of meetings, demonstrations and similar events in which the depicted persons participated; and
- (4) Portraits which have not been ordered as long as the distribution or exhibition serves a high interest in art.

[*Kunsturhebergesetz*, §23].

6.25 Injunctive relief is available to prohibit publication or continuing publication. Other remedies include, compensation for actual damage and/or an account of profits.

6.26 From an Anglo-American perspective the German situation may appear overly rigid and too easily capable of inhibiting publication in the public interest. However, Professor Markesinis argues that the contrary is the case.¹⁶ In his summary of the relevant caselaw, Professor Markesinis points out that the total number of cases is small and that freedom of expression will, on the whole, prevail over the right of privacy where the publication, broadcast, etc. aims at educating and informing the public rather than pursuing mere sensationalism or trying to satisfy the public's taste for gossip. He points out that the chances of success in a privacy claim tend to decrease as the public profile of the plaintiff increases, that the size of monetary awards is modest, that injunctive proceedings can be quick and that such relief is as often refused as granted, and that investigative journalism nevertheless continues to prosper in Germany.

France

6.27 In French Law persons have generally been regarded as having given tacit consent to the making of enquiries about their public activities and to publication thereof whereas express consent is needed if inquiries and publication relate to private life.

6.28 The taking and publication of a person's photograph in a public place is unlawful except when the photograph is incidental to the overall context of the

16 B.S. Markesinis, *The German Law of Torts* (Oxford: Clarendon P., 1994, 3rd ed.) pp. 410-416.

picture (e.g., being photographed in a crowd at a football match or at a place of natural beauty).

6.29 French law, like German law, makes distinctions between different aspects of privacy and different categories of persons. 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.

Canada

6.30 Canadian law likewise protects against unjustified publication of private information. Canadian law is also sensitive to the public interest defence to publication.

6.31 A number of interesting features arise from the Canadian caselaw generally, as two academic commentators have recently pointed out¹⁷. First of all, the Canadian courts have rejected the notion of a hierarchy of rights according to which one rights (e.g., freedom of expression) must always be deemed superior to another. Rather, as under German law, the relevant judicial task is one of harmonising competing rights in such a way as to ensure that the values underlying both sets are optimised. Secondly, and reminiscent of the approach of the European Court of Human Rights (see Annex I), the Canadian courts predicate the notion of privacy on an expansive theory of the "physical and moral integrity" of the person. Thirdly, the publication of private matter which is in the public interest and which also is newsworthy is publishable because it is in the public interest and not merely on account of its newsworthiness. Fourthly, both the Canadian Courts and the German Courts (as explained above) are at pains to balance in a rational manner the various factors that may arise on either side of the equation as follows:

"In relation to the right of privacy:

the nature of the information at issue (Canada) or the personality sphere to which the information relates (Germany); the public or private status of the individual claiming privacy; and the nature of the place where the alleged violation has occurred.

In relation to freedom of expression:

the value of the information at issue to public debate; the motivation or purpose underlying the publication of the information; and alternatives available to the publisher which would have reduced the impact on privacy."¹⁸

17 See generally, J. Craig & N. Nolte, *Privacy and Free Speech in Germany and Canada: Lessons for an English Privacy Tort* [1989] E.H.R.L.R. Issue 2, 162.

18 *Id.* at p.178.

United States

6.32 As stated above the second component tort in the privacy matrix in the U.S. concerns the publication of truthful private information about an individual. Several factors explain why this remedy is not as strong as it appears.

6.33 First of all, the tort must be operationalised against the backdrop of the First Amendment guaranteeing freedom of expression. For this reason some individual states do not recognise this tort. Indeed, for this reason wherever a redeeming news value can be found in the information the claim will generally be defeated¹⁹.

6.34 Secondly, the tort is actionable only where the disclosure relates to, or is in its nature, highly offensive from an objective standpoint. This means that truthful (but private) information falling short of offensiveness is not covered.

6.35 Thirdly, true (but private) information or images obtained from a public place or which is placed on (and obtainable) from a public record (e.g., judicial records) is not considered private.

3. Criminal Liability for Invasions of Privacy

6.36 The protection of privacy at the constitutional level and through civil law is supplemented in many countries by appropriate criminal liability. The imposition of criminal liability is generally confined to surveillance that is targeted on places where the expectation of privacy is at its highest (i.e. private places) or where the nature of the activity is inherently private (e.g. conversations).

Germany

6.37 In Germany Article 201 of the Criminal Code penalises the recording or using of listening devices for words not spoken in, or for, the public ("non-publicly spoken words"). For example, a private conversation in a public space cannot be recorded by a third person without the consent of all participants. Liability only accrues where a legal interest of the person is invaded. For example, overhearing a conversation about the weather does not attract liability but overhearing a conversation about marital difficulties might.

6.38 It is also an offence to use such a recording including making a recording available to a third person or letting the content of the recording be known to the public at large (subject to a "public interest" defence).

6.39 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. In case of conviction,

¹⁹ See, e.g., *Virgil v. Time Inc.*, 527 F 2d 1122 (1975).

any sound recorder or eavesdropping device used in connection with the offence may be confiscated.

France

6.40 In France from 1970 to 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. Anyone found guilty of this offence was liable to a term of imprisonment, a fine or both. 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.

6.41 The protection afforded by the provisions of the old French Penal Code of 1970 only apply if the person whose picture had been taken was at the time in a private place. The meaning of "a private place" had been elucidated by case law. A photograph taken of a person in the street fell outside the protection since a street is, by its nature, a public place²⁰ (civil liability may, however, lie). Also, a place to which everyone has access, without any special authorization, whether or not access was subject to certain conditions, was not deemed to be a private place.²¹ The photograph does not have to be taken from a private place. It was sufficient if the person photographed was 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.²²

6.42 Article 368 has been replaced by a comparable, but not identical, provision in the New Penal Code,²³ which came into force in 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. 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*"). It is sufficient if they are spoken privately or confidentially (*à titre privé ou confidentiel*). The new penalties also apply to the keeping, disclosure or permitting the disclosure to the public or a third person.²⁴ 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.

6.43 In Article 368 of New French Penal Code the presumption of consent has been tightened compared to the Penal Code from 1970. It has been uncoupled from the situation of a meeting and only applies whenever pictures are taken with

20 See, e.g., Tribunal, chambre correctionnelle, Toulouse, 26 February 1974, D.1974.736.

21 See, e.g., Tribunal de grande instance, Paris, 23 October 1986, Gaz. Pal. 1987.1.21.

22 Court of Cassation, Criminal Division, 25 April 1989, *Bull. crim.* No. 165.

23 Article 226-1.

24 Art. 226-2.

the knowledge of all the persons concerned, without them objecting thereto when they are in a position to do so. When private information is disclosed to the public by members of the press or broadcasting, liability is determined by the law particularly relating to these media.²⁵

6.44 Article 368 also forbade the deliberate invasion of 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 that person's consent. As in the case with visual surveillance, consent was presumed when the listening, recording or communicating occurred at a meeting with the knowledge of all the participants. The sanctions were the same as applied to unlawful visual surveillance. These penalties applied also to anyone who knowingly kept, brought, or deliberately let be brought to the knowledge of the public or a third person, or used publicly or otherwise, any recording or document obtained in a manner contrary to Article 368.

6.45 The replacement provisions in the New Penal Code (Article 226-1) now 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 word "listening" was replaced by the word "overhearing" and, as is the case with visual surveillance, the offence need no longer be committed by means of a device but through "conduct". *Importantly, it is not now necessary that the words be spoken in a private place. It is sufficient that they are spoken privately or confidentially.* Implicit in this is the assumption that a private conversation can occur in a public place and still attract the protections of the Code. Many of the incidental changes made under the New Penal Code (e.g, consent, liability for disseminating, etc.,) also apply in the case of aural surveillance.

Denmark

6.46 In Denmark the Penal Code penalises the unauthorised photography of persons on private property. The following are offences;

- taking photographs of people on private property;
- without consent, spying on people on private property with telescopes and other such optical devices;
- making use of information so obtained; and
- printing in a newspaper a photograph of a person without that person's consent.

Australia

6.47 Many Australian states subject the use of surveillance devices to criminal sanction. Interception is governed by Commonwealth legislation. Criminal sanctions are roughly the same in each state. It is an offence to use a device to

listen in on a private conversation. Conversation, if protected, is protected irrespective of content and regardless of whether it occurs in a public or private place. Private conversation is defined, for example, in the *Listening Devices Act* (1969) of Victoria 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 on which the parties to the conversation ought reasonably to expect that the conversation may be overheard".

6.48 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 is not invariably assumed that a conversation would be overheard in a public place, e.g., where the speakers had deliberately placed themselves beyond earshot. Defences include consent, authorised use under warrant issued by a court to a police officer for purposes of national security or for the investigation of narcotics offences. The consent of only one party to a conversation is generally sufficient.

6.49 In New South Wales, South Australia and ACT the recording of a conversation to which one is a party can be done without the permission of the other party. The Australian Law Reform Commission was divided on the issue of the regulation of participant monitoring, that is, that a person records a conversation to which the person is party. At first the Commission adopted the view that monitoring should not be permitted. But the majority ultimately recommended that participant monitoring should be allowed without the knowledge or consent of any other party and that a third party should be entitled to listen to and record a conversation if at least one of the parties to the conversation agrees to this.²⁶

Norway

6.50 In Norway the use of listening devices to overhear conversations is a criminal offence. Since July 1991 it is an offence punishable by fine to engage in video surveillance in public places without having clearly indicated by way of a notice that the place is under such surveillance²⁷. 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. Similar liabilities apply in Sweden.

26 See Report No. 22 on Privacy, paras. 1128-1132.

27 Article 309b of the Criminal Code.

4. Regulatory Safeguards

6.51 Regulatory safeguards are used in many countries to supplement civil and criminal provisions. The imposition of such safeguards means, by definition, a recognition that the surveillance in question has some legitimate rationale but that its use needs to be confined to that rationale and proper assurances given to the public. The options are many but include in the main -

- i. regulating the import or manufacture of surveillance devices,
- ii. licensing retail outlets for such devices,
- iii. licensing the users or prospective users of such devices,
- iv. confining trade in (or the right to use) certain devices to the police or military in accordance with a periodically revised list of scheduled devices,
- v. tightening up on the self-regulatory processes of the groups who are the heaviest users of such technology (e.g., private investigators),
- vi. regulating the place and manner of use by imposing conditions and restrictions.

6.52 The first three options - which go to the nature of the market for the supply of surveillance devices - are not commonly used. The last option is the one most commonly used.

Denmark

6.53 Denmark was one of the first countries to subject video surveillance to legislative regulation. An Act dating back to 1982 deals with surveillance by private persons. 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. There is a general prohibition on the surveillance of streets, roads, squares and similar areas used by ordinary traffic. The general prohibition does not apply to video surveillance of business premises provided it is carried out by the person in charge of the area and does not apply with respect to real-time video surveillance which is not connected to a recording device and which is carried out as part of the surveillance of a private entrance or cordoned-off area.

6.54 Moreover, any private person in Denmark 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. Under the legislation, the Minister for Justice is empowered to make regulations in relation to those signs but as of November 1997 has not done so. The requirement as to signs does not apply where the camera in question is not connected to recording equipment and where it is carried out as part of the surveillance of a private entrance or cordoned-off area. Implicit in the Danish law is the assumption that surveillance should generally be carried out only by the public authorities.

Sweden

6.55 In Sweden legislation came into force on 1 July 1990 to regulate the use of video cameras: *Act on Surveillance Cameras*²⁸. It applies to remote controlled cameras and other optical electronic devices. The law is targeted at installed cameras and requires a degree of permanency in the location of the camera for its application.²⁹

6.56 Under the legislation a licence is required for surveillance of a place to which the public has access.³⁰ 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 outdoor areas. Thus, 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. A separate licence is required for the retention or editing of any recording of still pictures or video film.³¹ This kind of 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, for example, for security purposes.

6.57 A licence to use surveillance equipment 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.³² In deciding whether or not to grant a licence, the county administrative board must have regard to the implications for individuals' personal integrity. Surveillance in such places as shops, banks, and post offices are regarded as fulfilling a legitimate interest. 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 grant a licence only where the latter completely outweighs the former. Licences may be granted subject to conditions and for a limited period of time³³, 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.

6.58 Easily visible signs alerting persons to the (licensed) surveillance must be displayed.³⁴ Dispensations from the notice requirement may be granted only where there are special reasons.

6.59 The county administrative boards monitor compliance with the conditions of a licence.³⁵ 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.

28 *Act on Surveillance Cameras*, 1990:484.
29 Section 1 of the act.
30 Section 4.
31 Section 6.
32 Section 5 of the Act.
33 Section 10.
34 Section 3.
35 See ss.11-13 of the Act.

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.³⁶

6.60 The Act on Surveillance Cameras is supplemented by the Secrecy Act³⁷. The Secrecy Act applies to the use of cameras by safeguarding from unauthorised disclosure personal information obtained by such surveillance.³⁸

6.61 Under Swedish law licences and dispensations from the notice requirement are granted by the relevant county administrative board.³⁹ 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 authorities⁴⁰. In making its decision, the county administrative board must consult with the municipality concerned and take account of its view.⁴¹ In the event a licence is refused, appeal may be made to the district administrative court.⁴²

Norway

6.62 Norway subjects the use of information, images, etc. obtained through recorded video surveillance to detailed regulation.

6.63 The Norwegian *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 sectors⁴³. 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.⁴⁴ A personal register is understood to be a register where information is systematically stored in such a way that information on a given person can be retrieved therefrom.⁴⁵

6.64 Section 37a of the Data Act 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.

36 Section 15.

37 *Lag om ändring i sekretesslagen* (1980:100) SFS 1990:485.

38 Section 14 of the Act on Surveillance Cameras.

39 Section 7.

40 See para. 3 of the administrative ordinance of 7 June 1990, SFS 1990:487.

41 Section 9.

42 See s.18 of the Act and para. 4 of the administrative ordinance.

43 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.

44 Art. 1.

45 *Ibid.*

6.65 Section 37b of the Data Act 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 or 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.

6.66 A regulation based on s.37b came into force on 15 October 1994. The main provisions of this regulation are that 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. They may not be kept for more than 7 days, but there are a number of exceptions to this time-limit in the case of the security of banks, post offices, the police and institutions of national defence. Recordings should however always be erased when there are no reasonable grounds for keeping them and if they 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.

France

6.67 France regulates the trade in surveillance devices. This regulation is backed up by criminal sanctions.

6.68 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. The manufacture, importation, possession, display, offering, rental or sale of devices on the list was subject to ministerial authorization, the granting of which was also to be subject to conditions laid down in the same decree. However, as of 1 January 1995, no list of devices has been drawn up.

6.69 Manufacture etc. without such authorization or not in compliance with any conditions attaching to authorization was an offence punishable with a term of imprisonment and/or a fine. In case of conviction for an offence involving lack of authorization, the court was to order the confiscation of the devices concerned.⁴⁶ Provisions similar to Article 371 on the regulation of trade in aural devices have been retained in the New Penal Code.⁴⁷

46 Article 372.
47 Articles 226-3.

5. Due process protections of covert police surveillance

6.70 Most states grant wider powers to law enforcement agencies to engage in covert surveillance than they give to private individuals. Nonetheless, since the interference with privacy is effectuated by state agencies such agencies are generally obliged to follow the strictures of due process while conducting surveillance. Due allowance is generally made in the relevant legislation for the peculiar constraints (including those of time and the general - though not invariable - need for secrecy) under which such operations are often conducted.

Norway

6.71 In Norway the police may engage in covert video surveillance subject to a number of conditions set out in the Code on Criminal Procedure as follows:

- there must exist reasonable grounds to suspect the commission of criminal acts which are punishable with at least 6 months' imprisonment;
- the surveillance must be of essential importance for the investigation;
- the surveillance must be authorised by a tribunal;
- authorization 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.⁴⁸

6.72 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 persons.

6.73 As seen above under section 37b of the Norwegian *Personal Data Registers Act* pictures and film taken by private individuals may be handed over to the police in connection with criminal offences or accidents without the consent of the person recorded. Nonetheless this is subject to a statutory duty of professional secrecy. A regulation based on s.37b of the Act sets out that recordings may only be used for the purpose for which they were obtained, but the police may however use recordings in their possession for the prevention or investigation of crime, as evidence in criminal cases, or to verify the facts of an accident. Also the recordings may not be kept for more than 7 days, but there are exceptions to this time-limit in the case of the police and institutions of national defence.

Sweden

6.74 One of the basic principles of Swedish surveillance law is that the individual in question should know that he/she is subject to surveillance. But under the Swedish surveillance laws 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. Additional dispensations from the notice requirement may be granted where there are special reasons.

6.75 In exceptional circumstances the Swedish police may also install a camera without a licence and seek a licence for it within the next 14 days.⁴⁹

Australia

6.76 Australian law enforcement agencies may 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.⁵⁰

6.77 Some safeguards of a formal kind do exist however 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.⁵¹ 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.⁵² 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.

6.78 The *Guidelines* 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. In situations where covert surveillance does not lead to the creation of a record, agencies are encouraged to adopt the *Guidelines* where relevant.

6.79 With respect to the decision to undertake covert surveillance, the main *Guidelines* provide that:

- Covert surveillance may only be undertaken for a lawful purpose which is related to the function of the agency.
- Approval to conduct covert surveillance in any particular case should be made at a senior level.
- In deciding to conduct covert surveillance agencies should be satisfied that there are reasonable grounds for believing that an offence or an unlawful activity is about to be committed, is

49 Section 4.

50 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.

51 On this office see Part IV of the Act.

52 *Covert Optical Surveillance in Commonwealth Administration - Guidelines*, Human Rights and Equal Opportunity Commission, Sydney, Australia, February 1992.

being committed or has been committed, that other forms of investigation have been assessed to be unsuitable and that 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.

6.80 As regards the actual conduct of the surveillance, the *Guidelines* provide that the agencies should be mindful of the following:

- The collection of personal information using a covert surveillance operation should be conducted in a lawful manner.
- The collection should not involve entrapment of the surveillance subject.
- Agencies should avoid any actions which may unreasonably impinge on the privacy and rights of other people.
- Where practicable, only material relevant to the purpose of conducting the covert surveillance should be collected.

6.81 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.

United Kingdom

6.82 In Britain the powers of state agencies to intercept communications or to conduct surveillance of private properties are regulated by different statutes.

6.83 The *Interception of Communications Act* 1985 allows for the police to apply to the Home Secretary to tap telephones or to open mail without requiring a warrant to be granted by a judge. In a similar way the *Security Service Act* 1996 under section 2 extends the Secretary of State's power in section 5 of the *Intelligence Services Act* 1994 to issue warrants to a security service authorising entry or interference with property to facilitate, for example, the bugging or surveillance of it.

6.84 Part III of the *Police Act* 1997 allows the police the same interference with private property as under the *Security Service Act* 1996 if this is necessary to prevent or detect a serious crime and if it cannot reasonably be undertaken by other means (section 93). The authorising police officer has to balance such an interference against the right to personal privacy. In contrast to the other two British Acts authorisation requires the approval of an appointed Commissioner, who is a senior judge of High Court status or above. Under section 97 of the Act an approval by a Commissioner has to be given in cases of interference with property which is used (wholly or mainly) as a dwelling, a bedroom in a hotel, office premises, or actions that are likely to result in the knowledge of matters subject to legal privilege, confidential personal information, or confidential journalistic material. The safeguards in the 1997 Act were added to the draft Bill after controversial discussions in the legal profession and in both Houses of

Parliament. Section 101 of the 1997 Act empowers the Secretary of State to issue a code of practice relating to the performance of functions under Part III of the Act. A draft code of practice was issued in 1997 for consultation purposes. As of March 1998 it had not yet been finalised for presentation to Parliament.

6. Conclusions

The following conclusions are warranted from the above.

6.85 First of all, the mere existence of legislation in the countries surveyed displays an awareness of a privacy problem associated with surveillance and of the need to reassure the public that the benefits of modern technology will not be outweighed by any possible abuses.

6.87 Secondly, most of the countries surveyed have either general or specific provisions in their respective civil laws to afford private remedies against unjustified surveillance. The range of remedies encompasses damages (for pecuniary and even for non-pecuniary loss), sequestration or seizure of equipment and injunctions. French civil law in this regard is directly inspired by Article 8 of the European Convention on Human Rights.

6.88 Thirdly, many countries prohibit (through civil law) the publication of private information or of information obtained through privacy-invasive surveillance. All such countries provide, in their own way, for a public interest defence to publication. German law insists that the intimate life of even the most public of persons is off-limits to publication.

6.89 Fourthly, criminal sanctions are generally confined to covert surveillance under two sets of circumstances: (1) visual surveillance of persons in *private places* where, by definition the expectation of privacy is at its highest and (2) aural surveillance with respect to activities which are generally (through not invariably) essentially private in their nature such as personal conversations. German, French and Australian law goes so far as to protect private conversations in public places so long as it is clear that the conversation in question was in its nature private.

6.90 Fifthly, regulatory safeguards have been enacted or introduced in many countries to supplement civil and criminal remedies. Such safeguards implicitly concede the legitimacy of surveillance but seek to regularise its use by either curtailing the trade in surveillance devices or by imposing appropriate time, place and manner restrictions on use. The requirement of publicly accessible signs (with some exceptions) is one general common denominator. Sweden goes so far as to require the licensing of users. France is somewhat unique in regulating the very trade in surveillance devices.

6.91 Lastly, covert police surveillance is generally brought under the requirements of due process. Several models for achieving this appear from the

countries examined. British law requires prior authorisation from a Commissioner who is a sitting judge; Norwegian law requires prior authorisation from a tribunal; Australian law requires authorisation "at a senior level" within the police; and Swedish law requires a license but grants an exception in emergency cases provided an application for a license is brought within 14 days.

6.92 In short, all the countries surveyed have deployed a web of legal tools - civil, criminal and regulatory - to tackle the privacy problem posed by surveillance.

PART III - RECOMMENDATIONS

CHAPTER 7: CORE RECOMMENDATION - THE CREATION OF CIVIL LIABILITY FOR PRIVACY-INVASIVE SURVEILLANCE AND HARASSMENT

7.01 Chapters 7, 8 and 9 should be read together with our draft Heads of Bill which, together with detailed Explanatory Notes, are contained in Chapter 10 of this Report.

7.02 In this chapter we set out our core recommendations with respect to the enactment of civil liability governing acts of privacy-invasive surveillance. We also outline a related recommendation for the enactment of a tort of harassment.

7.03 In the next chapter we outline our main ancillary recommendation with respect to the enactment of civil liability governing the disclosure or publication of material obtained by or as a result of privacy-invasive surveillance or harassment. We also set out our recommendations with respect to a related tort concerning the publication in Ireland of material, etc., obtained overseas by methods which, if they had been employed in this jurisdiction, would have amounted to the tort of privacy-invasive surveillance or the tort of harassment.

A: Core Recommendation - The Enactment of a Tort of Privacy-Invasive Surveillance

7.04 *We recommend the enactment of a new tort of Privacy-Invasive Surveillance.* [Head 2(i) of the Heads of Bill]

7.05 We are not here recommending the enactment of a *general* privacy tort. Such a tort is generally assumed to be directed at "information privacy" in the main and would embrace the publication of private information no matter how obtained.

7.06 Rather, we recommend the enactment of a tort that protects the right of privacy against the threat posed by surveillance. We therefore aim to enhance the protection provided by the privacy shield against intrusion.

7.07 *We recommend that the new tort should protect a "reasonable expectation" of privacy.* [Head 1(3)(i)(a)-(g)]

7.08 This means that a court will have to weigh up a mix of indicators in any given case. The ordinary and natural incidences of everyday life including, for example, being photographed by a passing tourist, must be tolerated. *Among the many indicative factors are the following* [see Head 1(3)(i), (a)-(g)]:

- (a) *the place (whether public or private);*
- (b) *the object or occasion of the surveillance;*
- (c) *the purpose for which material obtained was intended to be used including publication;*
- (d) *the means employed (long-range or surreptitious devices);*
- (e) *the status or function of the person;*
- (f) *the conduct of the person prior to the surveillance;*
- (g) *the overall context including the relationship between the surveillant/s and the person/s under surveillance.*

These factors are discussed in detail in Chapter 2 as well as in the Explanatory Notes to the Heads of Bill.

7.09 *We recommend that Surveillance should be defined broadly to include acts of aural or visual surveillance irrespective of the means used and should also include acts of interception as well as third party monitoring and participant-monitoring.* [Head 1(1)]

7.10 Surveillance is likely to take many shapes and forms and it is preferable to leave the definition open-ended to enable it to cover new technological developments as they evolve.

7.11 We define surveillance to include aural and visual surveillance irrespective of the means employed. This, of course, excludes casual overhearing of a conversation which is part of the natural and ordinary incidences of everyday life. Normally, some artificial means of aural or visual surveillance will be involved. However, there may well be cases of deliberate spying on people using only the normal human senses that can be considered invasive of privacy.

7.12 We include the interception of communication (whether by electronic means or otherwise) within the definition of surveillance. We also include participant monitoring and third-party monitoring within the definition of surveillance. We define participant monitoring to mean the secret recording of a conversation to which one is a party (i.e., without the consent of the other party or parties to the conversation). We define third party monitoring to mean the recording by the third party of a conversation with the consent of one of the parties thereto but without the consent of another party or parties.

7.13 *The terms "hearing devices" or "optical devices" as used in our recommendations do not include such devices where they are used solely to restore or maintain the normal range of human vision of hearing.* [Head 1(1)]

7.14 This qualification goes to the criminal offences as well as the torts proposed under our Heads of Bill as well as to the regulatory matters specified therein.

B: Subsidiary Recommendation - The Enactment of a Tort of Harassment

7.15 *We recommend the enactment of a related tort of Harassment.* [Head 2(ii)]

7.16 In our view the enactment of such a tort is necessary in order to protect privacy in the round. Acts of surveillance may well be accompanied by acts of harassment. Harassment may, of course, occur for other reasons. But it is chiefly because of the relationship between harassment and surveillance that we recommend the enactment of such a tort. The relationship between harassment and private life has already been alluded to by the European Commission on Human Rights (see chapter 5).

7.17 In our Consultation Paper we asked for submissions on whether there should be a "group" offence of collective besetting (para. 8.29). We are now of the view that there should not. Nor, for that matter, should there be expressed individual liability for participating in the harassing activities of a group. Rather, we recommend that there should be an analogue in tort law to the criminal offence of harassment established under Section 10 of the *Non-Fatal Offences Against the Person Act, 1997*.

7.18 *We recommend that the tort of harassment should be modelled on the definition of harassment provided under Section 10 of the Non-Fatal Offences against the Person Act, 1997.* [Head 1(2)]

C: Defences

7.19 *We recommend that consent, whether express or implied, should be a defence to an act of surveillance or harassment that might otherwise be found to be invasive of a reasonable expectation of privacy.* [Head 3(1)(i)]

7.20 It is conventional to include consent as a defence to privacy-invasive surveillance or harassment although as a matter of strict logic where consent has been proven no tort has been committed and thus no defence is required.

7.21 It is rare for consent to be given expressly and indeed there may well be a point where the law will - and should - deem the person incapable of consenting to the erosion of the entirety of his/her right to privacy or freedom from surveillance and harassment. It is more usual for consent to be implied. Such consent is usually implied by a prior pattern of behaviour that, properly interpreted, gives rise to a fair presumption that the person has waived an aspect

of their right to privacy. A court might well be slow to arrive at this conclusion unless the weight of the evidence points almost ineluctably to an effective waiver.

7.22 It is, in our view, highly unlikely that consent - whether express or implied - will be found by a court with respect to harassment.

7.23 *We recommend that the exercise of a legal duty, power or right of the defendant should constitute a defence to an act of privacy-invasive surveillance.* [Head 3(1)(ii)]

7.24 The law must recognise, and make space for, the exercise of countervailing duties, powers or rights. For example, a person has a right to defend himself in court proceedings and on occasion - though not invariably - this may require surveillance in order to get at material information. This is usually done through private detectives who act merely as the agents of their clients. Having a countervailing duty, power or right does not, however, confer *carte blanche*. The principle of proportionality attaches to, and qualifies, this defence [see Head 3(1)(ii)(b)].

7.25 Nothing in this defence gives the right to engage in means of surveillance that violate any other statute or that justify ignoring procedural or other requirements established under other statutes (e.g., warrant requirements under interception legislation).

7.26 Note that we do not extend this general defence to cover acts of harassment [see Head 3(1)(ii)] given the definition of harassment both in the existing criminal law (*Non-Fatal Offences Against the Person Act, 1997*, section 10) and in our recommendation for a new civil tort.

D: Remedies

7.27 It is important in our view to place a range of remedies at the disposal of the courts. The emphasis in our view should be more on prevention than on *ex post facto* remedies. In this way the law can play its part in fostering a climate of respect for privacy.

7.28 *We recommend that the new tort should be actionable without proof of damage.* [Head 2]

7.29 *We recommend that damages may be awarded for privacy-invasive surveillance and harassment.* [Head 4(a)]

7.30 *We recommend that if damages are awarded with respect to privacy-invasive surveillance or harassment under this Act, such awards may be taken into account in any other proceedings arising out of the same set of circumstances.* [Head 8(2)]

7.31 *We recommend that a plaintiff should be able to seek a preventive injunction or "privacy order" directed against impending acts of privacy-invasive surveillance or harassment.* [Heads 4(c) and 5]

Preventive injunctions are, we believe, a key feature in any strategy to enhance the protection of privacy, as privacy is a highly perishable commodity.

E. Technical Aspects of the New Torts

7.32 *We recommend that the new torts should enure for the benefit of natural persons only.* [Head 2]

7.33 Corporate bodies do not have personal space in the same way as ordinary individuals. No valid human rights objective (protecting dignity, making space for autonomy, setting the terms of co-existence in civil society, or facilitating democracy) impel us to apply the protections afforded by the legislation we propose to corporate bodies. That is not to say that aspects of a person's private life cannot take place in corporate settings and therefore enjoy a degree of protection (see para. 1.4 of this Report).

7.34 *We recommend that the right of action should accrue to the person whose privacy is in issue or to any other person who is legally entitled to act on behalf of that person.* [Head 6(1)]

7.35 *We recommend that an action for relief under our recommendations, other than one for damages or an account of profits, should survive the death of the victim and be available to the personal representative of the deceased or a member of the family of the deceased within the meaning of the Civil Liability Act, 1961.* [Head 6(2)]

7.36 In such cases we envisage under our legislative proposals the full range of remedies including specifically "privacy orders" or preventive injunctions being available with the important exception of damages. Privacy orders in this context will be relevant only with respect to disclosure or publication.

7.37 *We recommend that an action shall be time-barred after a three year period commencing from the date on which the plaintiff became aware or ought reasonably to have become aware of the tort and of the identity of the defendant (- see the relevant provisions of the Statute of Limitations (Amendment) Act, 1991).* [Head 7]

7.38 *We recommend that the rights of action and remedies available under our proposals are in addition to, and not in derogation from, any other right of action or remedy available under the law.* [Head 8(1)]

7.39 *We recommend that the rights and remedies afforded by our proposals should be declared to be without prejudice to the constitutional rights of the plaintiff or defendant.* [Head 14]

CHAPTER 8: MAIN ANCILLARY RECOMMENDATION - THE CREATION OF CIVIL LIABILITY FOR THE DISCLOSURE, DISSEMINATION OR PUBLICATION OF INFORMATION OR MATERIAL OBTAINED AS A RESULT OF PRIVACY-INVASIVE SURVEILLANCE OR HARASSMENT

A: Proposed New Torts of Disclosure of Material Obtained by Surveillance or Harassment

8.01 *We recommend the enactment of civil liability governing the unjustified disclosure or publication of any information or material (which includes images) obtained by or as a result of privacy-invasive surveillance or harassment.*
[Head 2(iii) of the Heads of Bill]

8.02 In conventional terms a privacy law is often taken to mean a law against any unjustified disclosure or publication of information pertaining to a person's private life. As indicated in the last chapter and indeed throughout this Report we do not recommend such a law on this occasion. However, we judge it necessary to take the vital step in prohibiting the unjustified disclosure or publication of any information, material or images obtained by or as a result of privacy-invasive surveillance and/or harassment.

8.03 *We recommend liability for publication in Ireland of information, etc., obtained overseas by methods which, if used to obtain that information in Ireland, would have amounted to privacy-invasive surveillance.* [Head 2(iv)]

8.04 As already explained at Chapter 1, Part 8, this recommendation is intended to address the international dimension of the privacy problem dealt with in this Report.

8.05 The liability we recommend under Head 2 (iii)-(iv) would cover all transactions on a continuum ranging from disclosure following immediately upon the act of privacy-invasive surveillance or harassment to intermediate dissemination and ending in eventual publication (and any possible re-publication) to the world at large.

B: Defences

8.06 *We recommend that no liability should attach to publication that might*

otherwise be unlawful under our recommendations if the defendant can show that he/she did not believe nor had reasonable grounds to believe that the information, etc., in question had been obtained by or as a result of privacy-invasive surveillance or harassment. [Head 3(1)(iii)]

8.07 If the person or entity doing the surveillance is in fact the same (or effectively the same) as the person or entity doing the publishing then this defence will be of no avail [see 2nd proviso (sub-para (b)) to Head 3]. The defence is of potential relevance only where the person/entity doing the surveillance is different to the person/entity doing the publishing.

8.08 *We recommend that consent, whether express or implied, should be a defence.* [Head 3(1)(i)]

8.09 *We recommend that the exercise of a legal duty or power or the maintenance of a legal right should be defences.* [Head 3(1)(ii)]

8.10 *We recommend that no liability should attach to publication that would otherwise be unlawful under our recommendations by reason of having been obtained by privacy-invasive surveillance if such publication is justified by overriding considerations of the "public interest".* [Head 3(1)(iv)]

8.11 *We endorse four specific - but non-exhaustive - strands to the "public interest" defence for the purposes of our recommendations* [see Head 3(3)]:

- (a) *the detection and prevention of crime;*
- (b) *the exposure of illegality or serious wrongdoing;*
- (c) *informing the public on a matter of public importance;*
- (d) *preventing the public from being misled by the public utterances of public figures (broadly defined) where private beliefs and behaviour are directly at variance with same.*

8.12 Our approach to the "public interest" defence is discussed in further detail in Chapter 2 and in the Explanatory Memorandum to the Heads of Bill.

C: Remedies

8.13 *We recommend that preventive injunctions or "privacy orders" should be available as a remedy for wrongful publication.* [Head 4(c) and Head 5]

8.14 Preventive injunctions, as we have pointed out in para. 7.26, might be serviceable in the context of preventing acts of privacy-invasive surveillance or harassment or preventing the continuation of same. In reality, such preventive injunctions will be most often sought to forestall the publication of information or

images, etc., obtained as a result of, or by means of, privacy-invasive surveillance or harassment.

8.15 Genuinely newsworthy items should not be inhibited for any longer than is absolutely necessary to ensure that privacy is not unjustifiably intruded upon. When it comes to a balance between two perishables - privacy or news - we come down on the side of privacy but in a way that allows the newsworthiness of the material in question to be evaluated rapidly and fully.

8.16 We outline several important features to the award of a privacy order under Head 5. For example, such orders should become effective immediately upon notification and may be subsequently varied, stayed or discharged. If an appeal is brought against the award of an order it may be stayed pending the outcome of the appeal.

8.17 In particular, *we recommend that on an application for a privacy order, the court shall take into account the public interest, if any, in disclosure or publication [Head 5(12)]. Furthermore, we recommend that on an interlocutory application for a privacy order, if the defendant makes out a good arguable case for the public interest defence (under Head 3), the court may refuse to grant the order where the justice of the case so requires [Head 5(13)].*

8.18 *We recommend that damages should be available as a remedy for wrongful publication. [Head 4(a)]*

8.19 *We recommend that an account of profits should be available as a remedy for wrongful publication. [Head 4(b)]*

8.20 *We recommend that a delivery up of all material that has come into the defendant's possession by reason of or in consequence of the tort of privacy-invasive surveillance should be available as a remedy. [Head 4(d)]*

CHAPTER 9: PROPOSED CRIMINAL, REGULATORY AND SUPPLEMENTARY PROVISIONS

Introduction

9.01 In this chapter we state our recommendations with respect to

- (A) the enactment of new criminal offences to supplement civil liability;
- (B) defences to the proposed offences;
- (C) the enactment of new regulatory safeguards to accompany State surveillance (covert and overt) in public and private places;
- (D) the power of courts to order proceedings to be held *in camera*;
- (E) the amendment of existing statute law governing interception to bring it up to date with new technological developments and with the recent and ongoing liberalisation of the postal and telecommunications sectors in Ireland; and
- (F) miscellaneous matters relating to CCTV technology.

9.02 All these matters, with the exception of (F), are dealt with in our proposed Heads of Bill (Chapter 10 below).

A: Proposed New Offences

9.03 We are proposing the creation of a number of further criminal offences because, on the basis of the principles and values arising from privacy as a human right which provide the basis for this Report, we are of the view that certain forms of privacy-invasive surveillance are particularly offensive and socially unacceptable and ought to be visited with the sanctions of the criminal law. We so recommend in order to add a deterrent element which can only be added by the criminal law to the mainly preventative and compensatory role of civil law.

9.04 We have listened with great care to the many submissions made to the effect that since the imposition of criminal liability is so drastic a step, care should be taken to ensure that it is tailored narrowly to meet only the most pressing of concerns. That is why we have moved away from the open-ended formula contained in our Consultation Paper concerning criminal liability (proposed offence of infringing the integrity of another through surveillance) to one that targets invasions of privacy in well-defined circumstances where the

expectation of privacy is at its highest (i.e., on a private dwelling) or where the activity in question (i.e., conversations) is inherently private.

9.05 As such, the new offences we recommend would round out the panoply of existing criminal offences that already deal with various aspects of surveillance as set out in our Consultation Paper (Chapter 5, pages 88-120) and would do so in such a way as to target only those kinds of violations that all or most would agree require the sanction and intervention of the criminal law.

9.06 Specifically, we recommend the enactment of three new substantive offences as follows. Ancillary offences dealing with disclosure of the yield of the surveillance are also provided for.

(i) *New Offence of Installing Surveillance Device in a Private Dwelling or Engaging in Surveillance of a Private Dwelling* [Head 9(1)(a)]

9.07 *We recommend the enactment an offence of infringing the privacy of a (natural) person by installing a surveillance device inside a dwelling with a view to surveillance, or using such device from outside a dwelling but with a view to spying on the dwelling.*

9.08 We have bundled together two phenomena under this head - namely (1) the installation of a surveillance device in a private dwelling and (2) engaging in the surveillance of activities taking place in a private dwelling but from outside or afar. The common denominator in both instances is the sanctity of the private dwelling.

9.09 The Legislature may well take the view that these two phenomena should be unbundled and handled by two separate offences. This is so because not every act of surveillance from outside or afar onto a private dwelling may violate a "reasonable expectation" of privacy arising within. For the moment, however, we keep these phenomena together to bring out our concern for the sanctity of the privacy of the dwelling.

(ii) *New Offence of Trespass Done for the Purpose of Surveillance* [Head 9(1)(b)]

9.10 *We recommend a new offence of trespass on private property (either by unlawfully entering thereon or by unlawfully remaining therein) effectuated for the purpose of obtaining information thereon concerning any (natural) person.*

9.11 This new offence governs the type of case which involves a particular kind of trespass on private property. This is the type of trespass which is directed at infringing the information privacy of a person. Unlike the offence outlined at (i) above, no surveillance device need be installed for this offence to apply. Like the offence above, the imposition of criminal liability for such

behaviour is justified since such behaviour aims at the heart of a place which is preeminently private.

(iii) *New Offence of Using Devices to Spy on Private Conversations* [Head 9(1)(c)]

9.12 *We recommend the enactment of an offence of infringing the privacy of a (natural) person by using aural or optical devices to spy on people's conversations in circumstances where a "reasonable expectation of privacy" arises and where the consent of no party to the conversation has been obtained.*

(This offence would not affect the existing criminal law on the interception of telephonic and electronic communications.)

(iv) *New Ancillary Offences aimed at the Disclosure of Information obtained as a result of the new criminal offences* [Heads 9(1)(d), 9(1)(e) and 9(1)(f)]

9.13 The prohibitions which we envisage as outlined above would be deprived of much of their value if those who came into possession, directly or indirectly, of information as a result of the criminal surveillance concerned were free to communicate or use the information with impunity.

9.14 As was seen in Head 1, "disclose" includes communicating, conveying and publishing.

Schedule to the Proposed Heads

9.15 The Schedule which appears at the end of the Heads concerns the proviso to Head 3 (defences in respect of civil liability for privacy-invasive surveillance and disclosure or publication of the yield thereof). The acts referred to in the list contained in the Schedule are consistent with the provisions for criminal offences discussed above.

9.16 Their effect would be to disallow the "public interest" defence provided for in Head 3 in relation to the tort(s) of publication of material or information obtained by privacy-invasive surveillance insofar as such surveillance had involved the commission of any of the acts contained in the Schedule. We believe that it is appropriate to impose such restrictions on the public interest defence because considerations of the public interest involve not only the public interest in publication of information but also the public interest in supporting the enforcement of the criminal law. The enactment, even in the sphere of civil liability, of provisions which might tend to undermine or prejudice such enforcement, should be avoided.

B: Defences

9.17 *We recommend a broad range of defences to the above offences including consent, the necessary protection of one's rights and, with some limitations, the necessary protection of third persons. [Head 10]*

9.18 In many respects the proposed defences mirror those recommended for the civil torts outlined under Head 2 of the Heads. However, it should be emphasised that the existence of a defence in respect of a criminal offence does not necessarily mean that there is a defence in respect of any corresponding civil tort.

9.19 *We recommend that the proposed defences should be:*

- *the consent, expressed or implied, of the supposed victim [Head 10(a)]. This defence applies to all offences under Head 9;*
- *the necessary protection of one's own rights [Head 10(b)]. This defence applies to all offences under Head 9;*
- *the necessary protection of the person (but not the property) of someone other than the alleged perpetrator [Head 11(c)]. This defence applies to all offences under Head 9;*
- *in relation to the offence outlined under Head 9(a), insofar as it catches surveillance of a private dwelling from outside or afar: that such surveillance is done by or under a form of "neighbourhood watch" arrangement, provided that
 - (i) *the complainant is a neighbour of the defendant and is a participant in the scheme or arrangement,*
 - (ii) *the defendant has a reasonable belief that a crime against the complainant (which includes his/her household, its members and property) is being or may be committed and*
 - (iii) *the surveillance carried out was not excessive or unreasonable having regard to that belief and to all the relevant circumstances*[Head 10(d)].*
- *the lawful exercise by a member of the Garda Síochána of powers granted by law for the prevention, detection or prosecution of crime including the lawful arrest of any person [Head 10(e)]. This defence applies to all offences under Head 9;*

- *the existence of lawful authority by or under statute (but not at common law separate from statute) [Head 10(f)]. This defence applies to all offences under Head 9;*
- *in respect of offences (a) and (c), that the listening or recording was done by or on behalf of a lawful occupier of premises, provided that the listening or recording did not involve covert photography or recording of such a nature as to constitute an intentional violation of the intimate and private life of any person on the premises [Head 10(g)];*
- *and, in respect of the offences (d),(e) and (f) in Head 9, which offences all concern the communication of information or material obtained in contravention of other provisions in Head 9, bona fide ignorance of the fact that the information was obtained in contravention of these provisions [Head 10(h)].*

C: Regulatory Provisions Directed at Particular Forms of Surveillance by State Authorities and Others

(i) Police Surveillance of Private Places

9.20 *We recommend that, notwithstanding the criminal offences contained in Head 9 (and notwithstanding the provisions for civil liability in the earlier Heads), surveillance by a member of An Garda Síochána of any private place using any optical or hearing device, without the consent of the occupier, may be authorised either for an initial period (non-renewable) of fourteen days by a Chief Superintendent of An Garda Síochána or for any period of up to three months (renewable) by a Judge of the District Court. [Head 11(2)]*

9.21 *For this purpose we recommend that:-*

(1) Such surveillance may be authorised for the prevention or detection of crime in respect of which a search warrant may be issued to any member of An Garda Síochána under existing statute law including:

- *the unlawful arrest or prosecution of any person,*
- *general intelligence gathering in relation to any such crime, and*
- *the obtaining of evidence for which a search warrant may be granted under section 14 of the Criminal Assets Bureau Act, 1996.*

[Head 11(2)(b)(i)]

(2) A surveillance warrant may authorise the member of An Garda Síochána in question, accompanied by such others as he

considers necessary, to enter private property the subject of the warrant for the purpose of initiating, maintaining or withdrawing such surveillance, and may impose conditions in respect of such surveillance. [Head 11(2)(b)(v)]

- (3) *There should be specific rules of substance as to the justification for the grant of a surveillance warrant of which the court (or a Chief Superintendent) should be satisfied before it is granted [see Head 11(2)(b)(viii)] as well as procedural conditions. A surveillance warrant may not be granted for the purposes of conducting surveillance of communications which are privileged at law [Head 11(2)(b)(ix)].*

9.22 The police must, in the interest of the prevention and detection of crime, have substantial additional latitude over and above that allowed to private interests in the surveillance both of private places and of public places. Otherwise the enforcement of the criminal law which is a special function of the State and its authorities would be prejudiced.

9.23 We do not however believe that it would be justifiable to exempt the Garda Síochána or State authorities in any *general* way from the civil and criminal obligations and liabilities which we recommend; to do so would be to cast aside, in the all important area of State surveillance, the protection of the public from privacy-invasive surveillance which is the aim of this Report. Instead we recommend that a broadly based, flexible and workable system of authorisations, both judicial (granted by the District Court) and administrative (granted by a Chief Superintendent) should be put in place which would give the Garda Síochána the protection they need in carrying out their function of the prevention and detection of crime.

9.24 We note that there may well be a case to be made to extend the above powers to other State officials including particularly customs officers in light of the possible adoption of the draft EU Convention on Mutual Assistance and Cooperation between Customs Administrations¹.

(ii) *Surveillance of Public Places*

9.25 *We recommend that as a general rule, subject only to the special case of owners or occupiers of premises engaging in surveillance for the protection of their own premises (see below), no one should be entitled to use for the purposes of surveillance of public places any fixed optical device designed or suitable for filming or otherwise recording events in such public places, with the exception of a member of An Garda Síochána acting under and in accordance with an authorisation granted by a member of An Garda Síochána not below the rank of Chief*

1

(11089/97), ENFOCUSTOM.

Superintendent [Head 11(3)]. Such an authorisation may be granted for any period not exceeding three months and may be renewed [Head 11(3)(c)]. For this purpose an optical device is fixed if it is installed at a fixed position at or from which it can be used for surveillance, including in a vehicle, whether moving or not [Head 11(3)(b)].

(iii) Surveillance carried on by private persons from their own private premises

9.26 We recommend that as a general rule, private persons should not be entitled to use for the purposes of surveillance of any public place or any private place which is open to the public any fixed optical device designed or suitable for filming or otherwise recording. [Head 11(4)(a)]

9.27 By way of exception to this however we recommend that surveillance of a public place may be carried out by means of a device installed or fixed in premises owned or occupied by the person carrying out such surveillance for the bona fide purpose of protecting the premises (including persons and things therein) provided that a notice, visible to the public, indicating the fact of such surveillance, is fixed to the premises in the vicinity of such surveillance. [Head 11(4)(b)]

9.28 However, we recommend that where surveillance is carried out in a private place which is open to the public, notice of the surveillance should be given at each entrance to the premises which is open to the public. [Head 11(4)(c)]

(iv) Disclosure of Information Obtained by Means of Surveillance

9.29 We recommend that, consistent with the restrictions and requirements of the regulatory provisions mentioned above, there should be clear and strict rules as to the disclosure or use which is to be permitted of information obtained as a result of surveillance authorised under those provisions. Generally speaking such disclosure or use of the information should be permitted only for the purposes of which the authorisation for the relevant surveillance has been granted or for the purposes of compliance with an order of any court [Heads 11(2)(c) and 11(3)(d)]. In the case of private surveillance authorised in respect of private premises (see (iii) above) the information may be used only for the purposes for which it was lawfully carried out by the private person concerned or for compliance with an order of a court [Head 11(4)(e)].

9.30 We further recommend that, where information has been obtained as a result of surveillance contrary to the regulatory provisions mentioned above (at (i)-(iii) above), it should be prohibited to use or disclose such information other than by conveying it bona fide to a member of An Garda Síochána for the purposes of the detection or prevention of crime [Head 11(5)].

(v) *Supplementary Offences*

9.31 *We recommend the creation of a number of supplementary offences necessary to give effect to these regulatory provisions in addition to the offences already proposed under Head 9. Broadly speaking these offences govern the unlawful disclosure or use of information obtained as a result of surveillance authorised under the regulatory provisions [Heads 11(2)(d), 11(3)(e) and 11(4)(e)]; the unlawful disclosure of use of information obtained as a result of surveillance not authorised under the regulatory provisions [Head 11(5)]; and the unlawful use of fixed surveillance devices [Heads 11(3)(e) and 11(4)(d)].*

(vi) *Defence to civil and criminal liability*

9.32 *Persons lawfully carrying out surveillance in accordance with the regulatory provisions or lawfully disclosing or using information obtained as a result thereof should have a full defence in respect of all criminal or civil liability arising under our recommendations. [Head 11(6)]*

(vii) *Judicial Review*

9.33 *We recommend overall judicial review (along the lines of s.8 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993) of surveillance by An Garda Síochána to which Head 11 applies. [Head 11(7)]*

D: The Power of the Courts to Hold Proceedings *In Camera* or to Restrain Publication Relating to Proceedings

9.34 *We recommend that any legislation providing for the civil torts and criminal offences should confer discretion on the relevant court to order that proceedings be held otherwise than in public and/or to place tailored restrictions on publication where, on balance, privacy so warrants. [Head 12]*

The reasons and legal basis for this recommendation are set out in detail in Annex IV to this Report.

E: Technical Amendments of the Postal and Telecommunications Legislation

9.35 *We also propose, in Head 13, certain technical amendments to the Postal and Telecommunications Services Act, 1983 and the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993. These amendments arise, first, from the fact that the provision of postal and telecommunications services is no longer confined to An Post and An Bord*

Telecom, and second, from the fact that since the enactment of these statutes there have been some relevant technological developments which call for matching amendments of the legislation in order to keep them abreast of the latest operating conditions in the market. (See further our Consultation Paper, provisional recommendations 16-18 and paras. 12.08-12.19.)

F: Miscellaneous

9.36 In this final section we make further proposals in relation to the use of CCTV technology. These proposals are not dealt with in our Heads of Bill, but are discussed in Annex III of this Report ("Data Protection Law and the Use of CCTV").

9.37 Specifically, we propose that *the Government should give serious consideration to developing a comprehensive national code governing the use of fixed CCTV systems in public places by the Gardaí*. Such a code should have a firm foundation in legislation whether under a specific enabling provision or under section 13 of the *Data Protection Act, 1988*. Such a code should deal, *inter alia*, with the requirements for notices to alert members of the public that upon entering a certain area their activities are being monitored and recorded.

9.38 We also propose that *serious consideration should be given to the development of codes of practice governing the use of CCTV technology in specific sectors* (e.g. industry, banking, shopping centres, etc.). Again, such codes should have a firm foundation in legislation whether under specific enabling provisions of under the *Data Protection Act, 1988*.

CHAPTER 10: PROPOSED HEADS OF A BILL TO PROTECT THE INDIVIDUAL FROM INTRUSIVE SURVEILLANCE

10.1 As the title of this Chapter implies, what follows is intended as a detailed statement of the content of suggested legislation to give effect to our main recommendations rather than as an actual draft of a Bill. Nonetheless, many of the suggested Heads are in such a form that they could serve as a draft of the appropriate provisions.

10.2 We have taken this course in order to assist in the task of addressing the many complexities involved in drawing up this kind of legislation while recognising that the decision as to what legislation should be promoted is a matter for Government and ultimately the Oireachtas, and that the task of parliamentary drafting is of course not ours.

TABLE OF CONTENTS OF HEADS

Head 1:	Interpretation	Page 120
Head 2:	Causes of action	Page 124
Head 3:	Defences	Page 128
Head 4:	Remedies	Page 140
Head 5:	Privacy Orders	Page 140
Head 6:	Persons entitled to sue	Page 142
Head 7:	Limitation period	Page 143
Head 8:	Other rights of action and remedies	Page 143
Head 9:	Criminal offences	Page 144
Head 10:	Defences in respect of criminal offences	Page 149
Head 11:	Regulatory Provisions: Certain forms of surveillance by An Garda Síochána and others	Page 152
Head 12:	Hearing of proceedings otherwise than in public and related matters	Page 162
Head 13:	Amendments of postal and telecommunications legislation	Page 163
Head 14:	Saver	Page 163
Head 15:	Penalties	Page 164
Schedule		Page 164

PROVIDE as set out in the following Heads for a Bill:

Head 1: Interpretation

(1). In these Heads, except where the context otherwise requires

"disclose" means disclose to any person other than a person aggrieved or claiming to be aggrieved under these Heads by such disclosure and includes communicate, convey and publish, and cognate words shall be construed accordingly;

"dwelling" includes dwelling accommodation in a vehicle or vessel and the bedroom accommodation of a hotel, guesthouse, hospital or similar establishment and associated private accommodation such as a bathroom, as well as the curtilage of a dwellinghouse;

"hearing device" and "optical device" do not include respectively, a hearing aid designed and used solely to restore or maintain the faculty of hearing sounds which are within the normal range of unaided human hearing, and an optical device designed to restore or maintain the faculty of eyesight of the standard of normal unaided human eyesight;

"the Court" shall include the Circuit Court;

"harass" shall be construed in accordance with paragraph (2) of this Head and cognate words shall be construed accordingly;

"privacy order" has the meaning assigned to it by Head 5;

"surveillance" includes aural (hearing) and visual (optical) surveillance, irrespective of the means employed, and the interception of communications, whether such communications are effected by electronic or other means, and, without prejudice to the generality of this definition, includes -

- (a) the recording by means of any electronic or technical device of a conversation where such recording is carried out by a person who is not a party to that conversation without the knowledge of a person who is such a party but with the knowledge of another person who is such a party; and
- (b) the recording by means of any electronic or technical device of a conversation where such recording is carried out by a person who is a party to that

conversation without the knowledge of another person who is such a party.

- (2) (i) There is harassment where any person, without lawful authority or reasonable excuse, by any means, including by use of any communicating device, harasses another by persistently following, watching, pestering, besetting or communicating with him or her.**
- (ii) For the purposes of subparagraph (i) a person harasses another where-**
- (a) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other, and**
- (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other's peace and privacy or cause alarm, distress or harm to the other.**
- (3) (i) In determining under Head 2 whether the privacy of a person has been invaded by means of surveillance, the Court shall consider the extent to which that person was reasonably entitled to expect that he or she should not be subjected to such surveillance having regard to all the relevant circumstances, including, where the Court considers it appropriate:**
- (a) the place where such surveillance occurred;**
- (b) the object and occasion of such surveillance;**
- (c) the purpose for which material if any obtained by means of such surveillance was intended to be used, including but not confined to subsequent disclosure thereof; and the use which was in fact made of any such material shall be evidence of the purpose for which it was intended to be used;**
- (d) the means of surveillance employed and in particular the nature of any device or apparatus used for such surveillance;**
- (e) the status or function of that person;**
- (f) the conduct of that person, whether prior to or on the occasion of the surveillance at issue, insofar as it may**

have amounted to a waiver, in whole or in part, of that person's privacy in respect of the surveillance at issue, or invited or encouraged interest in the object of that surveillance; and

- (g) the context of such surveillance, including the relationship, if any, between the person subjected to the surveillance and the person who carried it out.
- (ii) The privacy of a person may be invaded by means of surveillance within the meaning of Head 2(i) irrespective of the content or quality of any material or information actually obtained or sought, and even if no material or information is actually obtained by means or as a result of the act complained of.
- (iii) Paragraph (i) shall apply with the necessary adaptations to the determination by a court under Head 5 of a claim that a tort under Head 2 is being or is about to be committed.

EXPLANATORY NOTE:

General:

The notion of the right of privacy proposed under these Heads is that of a "shield" or "boundary", or perhaps a series of shields or boundaries, aimed at protecting the private life of the individual by requiring that the individual should be left alone and not be subjected to privacy-intrusive surveillance. It is of the essence of the proposals that they set out to protect privacy by creating such a shield or boundary which may not be penetrated by surveillance except under very specific circumstances rather than by directly protecting the right of privacy in private or confidential information as such.

Paragraph (1): *This paragraph of the Heads provides, in the usual form, for definitions of certain matters contained in the subsequent Heads. By contrast, paragraphs (2) and (3) contain special definitions or interpretative provisions concerning the concept of harassment and the invasion of privacy. All definitions in paragraph (1) are applicable "except where the context otherwise requires".*

Concerning the definition of "disclosure" in this paragraph, the Heads recommend the creation both of a tort of disclosure of information or material obtained under certain circumstances, and of criminal offences of disclosure in more specific and narrowly defined cases. "Disclosure" is defined for the purposes of the Heads as a whole to include communicate, convey and publish. It covers both the initial disclosure of the information or material by the person who obtained it, and subsequent disclosures by that person or by others to whom it has been disclosed.

Of course, disclosure may ultimately become so extensive or be made to such a wide audience (e.g. through the news media) that the material disclosed comes, rightly or wrongly, into the public domain, and its subsequent repetition can no longer be correctly said to involve "disclosure" by those who so repeat it. The effect of such subsequent dissemination however may well be to exacerbate the injury resulting from the earlier tort or torts of disclosure.

The provision concerning the "hearing device" and the "optical device" is intended to exclude from the scope of the Schedule to the Heads (which refers to certain acts for the purposes of the second proviso to Head 3), and from the criminal offences which we propose should be created, the use of ordinary hearing aids and ordinary spectacles or contact lenses.

The definition of "surveillance" is not intended to be comprehensive. It leaves open the possibility that there may be forms of surveillance other than those mentioned in the definition. The definition is however used as a vehicle by which to bring two forms of privacy-invasive conduct - what are known as "participant monitoring" and "third party monitoring" where these involve recording of conversations by means of an electronic or technical device - within the ambit of the tort proposed under Head 2.

Surveillance is by its nature a deliberate act.

Paragraph 2: As indicated in our Consultation Paper on Privacy: Surveillance and the Interception of Communications, (1996) there is a clear connection between privacy-invasive surveillance and harassment. The definition of harassment for the purposes of the present proposals has been drawn from the definition of criminal harassment contained in section 10 of the Non-Fatal Offences Against the Person Act, 1997.

It will be noted that in line with the criminal definition, the tort of harassment will not be committed if the act complained of has been done with lawful authority or reasonable excuse. Considerations of as to what degree of interference with the plaintiff was reasonable in the circumstances (in effect considerations of proportionality) would also arise in this context. Given the proposed alignment of the ingredients of the civil tort with those of the criminal offence, we have decided that the defences of legal duty, legal power and legal right (Head 3(1)(ii) below) should not, in addition to those of lawful authority or reasonable excuse, be made applicable to the tort of harassment, and to confine them to the tort of privacy-invasive surveillance and of publication of material obtained by reason or as a result of such surveillance, though it seems inevitable that in practice there must be a high degree of correspondence between these two sets of defences.

Paragraph 3: The interpretative provision contained in sub-paragraph (i) of this paragraph concerning the meaning of the invasion of privacy of a person by means of surveillance is not exhaustive. This is a reflection, first, of the fact that the extent of one's right to privacy will inevitably vary according to what the subject was reasonably entitled to expect in the circumstances of the case. This paragraph also

points to certain factors which, where appropriate, the court, in determining the content and extent of the right to privacy in a particular case, should take into account if the court considers it appropriate to do so. The list of factors indicates the potentially variable boundaries of the right to privacy.

With regard to the first two of these factors, (a) the place where such surveillance occurred and (b) the object and occasion of such surveillance, it is appropriate to stress that although one's reasonable expectations of privacy are considerably less when one is in a public or semi-public place than when one is in a private dwelling, these expectations, and the right of privacy which flows from them, do not by any means cease when one is in a public place. Intrusive, targeted photographing or video-filming of a person without that person's consent (especially but not solely for publication in the media) would be one potential example of this. A clearer and more egregious example would be spying on people's conversations, particularly from a distance or otherwise in a covert manner by means of electronic or other apparatus. As for the object or occasion of surveillance in a public place, there will be circumstances in which persons in public places are particularly vulnerable to objectionable surveillance, such as those in distress because of bereavement or injury. The question whether privacy-intrusive surveillance has occurred will also be influenced in these and other cases by consideration (c) - the purpose of such surveillance or the use to which material obtained thereby is subsequently put, including, in particular, subsequent media publication.

See the more detailed discussion of these factors above at Chapter 2 of this report.

It is considered better to give general non-exclusive guidelines to the courts for the purposes of interpreting the content and extent of the right of privacy in each case than to attempt to formulate rigid rules.

This is all the more the case when one appreciates that the content of the right of privacy is at least to some extent a matter for assessment in the light of the social customs and mores of the time. These must be allowed to develop through jurisprudence rather than be the subject of an attempt (which would be almost inevitably unsatisfactory) to create a rigid statutory definition of the right of privacy.

Sub-paragraph (ii) of this paragraph has its mirror image in Head 9(2) (criminal offences) below.

Sub-paragraph (iii) of this paragraph draws attention to the need for a provision which would adapt sub-paragraph (i) to the case where the court was asked to make a privacy order under Head 5, particularly in a case where a tort of privacy-invasive surveillance was about to be committed but had not yet been committed.

Head 2: Causes of action

It is a tort, actionable without proof of damage, for a person-

- (i) to invade the privacy of another person by means of surveillance; or**

- (ii) to harass another person; or
- (iii) to disclose the purport or substance of information or material obtained by means of privacy-invasive surveillance or by means or as a result of harassment, whether such surveillance or harassment was carried out by or on behalf of the person disclosing such information or not; or
- (iv) to disclose within the State the purport or substance of information or material obtained outside the State by means which, had the information or material been obtained by those means within the State, would have made such disclosure tortious under para (iii) of this Head.

In subparagraph (i) and (ii) of this Head, "person" means natural person.

EXPLANATORY NOTE:

This Head proposes the creation of four new torts. Reference has already been made to the first two of these - invasion of the privacy of a person by means of surveillance, and the tort of harassment. The third and fourth proposed torts are directed to acts of disclosure or publication of the purport or substance of information or material obtained by means or as a result of privacy-invasive surveillance or harassment. They therefore presuppose that the act of surveillance or harassment which would constitute one or other of the first two torts has already been committed and go on to address the disclosure of information or material obtained thereby, such disclosure (perhaps in the form of publication by the news media) very often being the motive behind the commission of the previous tort in the first instance.

The torts created pursuant to this Head would be "actionable without proof of damage". That is to say, in order to succeed in an action for any of these torts the plaintiff would not have to prove either personal injury, damage to property or actual monetary loss of any kind, though such injury, damage or loss, where they had occurred as a result of the commission of any of the torts, would be compensatable under the ordinary rules governing damages. Since the torts in question all involve or are derived from either encroachment upon people's private lives or from harassment, the insult, outrage and injury to feelings resulting from their commission are considered to make them appropriate for actionability irrespective of whether there has been any personal injury, damage or loss. (See Heads 4 and 8 concerning Remedies.)

Except in the case of the fourth of these torts which is aimed at the international dimension of the problem, it is assumed that the relevant surveillance or harassment has occurred within the State. Where disclosure is at issue, this must in all cases have occurred within the State.

In these Explanatory Notes the torts (Head 2) and the special defences to those torts (Head 3 below) are considered separately.

THE FIRST TORT - Head 2(i)

The first of the four proposed torts is the invasion of the privacy of another person by means of surveillance. The concepts of "privacy" and "surveillance" in this context are discussed above in the explanatory note to Head 1. As has already been stated this tort sets out not to protect directly secret, confidential or private information but rather to recognize that each individual enjoys a right to his own privacy or private life and to the protection of that right by means of the creation of a "shield" or boundary the penetration or crossing of which by means of surveillance is prohibited by law except under very specific and exceptional circumstances. (In the present proposals these circumstances are set out in the defences contained in Head 3.) The commission or otherwise of the tort of privacy invasive surveillance does not therefore depend on the defendant's having actually obtained, still less used, any information of a kind which the plaintiff could legitimately regard as private or confidential or secret. Prime examples of this would be the act in itself of invading the privacy of the plaintiff's private dwelling by the use of bugging devices or camera surveillance or even by listening at a door or window. Another would be the use of audio devices or even the method (whether artificially aided or not) of lipreading in order to divine the content of private conversations, however inconsequential, between individuals, even where they are held in public places. The systematic following of a person without lawful excuse for the purpose of ascertaining his or her movements, even in public places, would also be an example. This concept of privacy as a right to be let alone rather than the right to have specific information protected is at the heart of the proposals.

THE SECOND TORT - Head 2 (ii)

The second tort (harassment) embraces actions and activities which, though they are conceptually distinct from privacy-invasive surveillance, are often closely connected with it (a fact which is acknowledged by, among others, the European Commission of Human Rights), and which are therefore particularly appropriate for inclusion in the present proposed legislation. People's privacy may be invaded by pursuing them or pestering them in the streets with a view for example to photographing or filming them against their will or to pressurising them to answer questions or to give information when they do not wish to do so, no less than by covert surveillance. In the Consultation Paper to which this Report is a sequel it was suggested (paragraph 8.29) that consideration should be given to creating a new tort of group or collective besetting. On further consideration we have decided to recommend the creation of a simple tort of harassment which would of course include besetting or harassment carried out by persons acting in groups. Although harassment in the context of privacy may therefore be regarded as closely connected with surveillance, even in that context it goes beyond surveillance in that it is liable to be and frequently is of the nature of intimidation or of a disturbance or threat to the peace by reason of the element of physical intrusion upon the person of the victim which it is liable to involve. The tort of harassment would mirror the criminal offence of harassment created by section 10 of the Non-Fatal Offences Against the Person Act, 1997.

It is arguable that section 10 of the 1997 Act is sufficient in itself to create a tort of harassment. However, even if this is so, we recommend the inclusion of this

provision in these Heads in order that the supplementary provisions of these Heads (in particular Head 3(1)(iii), Heads 4,5,6 and 7) may be applicable.

THE THIRD TORT - Head 2 (iii)

The third tort is that of disclosure (which, as defined in Head 1, would include communicating, conveying and publishing) of information or material obtained by means of privacy invasive surveillance (tort no.1) or by means or as a result of harassment (tort no.2). There would be a fundamental gap in the proposed legislation if, having prohibited privacy-invasive surveillance or harassment, it did not also prohibit the disclosure of the purport or substance of information obtained thereby, given that the disclosure of such information is often the very reason for the surveillance or harassment in the first place. It should be noted that this tort covers both the original disclosure or passing on by the surveillor or harasser of the information gained thereby and any subsequent disclosure by or between third parties, including disclosure by publication to the general public, of that information. However, in the case of such third parties it will (among other possible defences) be a defence to the action of disclosure for them to show that at the time of such disclosure they did not believe and had no reasonable grounds to believe that the information had been obtained by means of privacy-invasive surveillance or by harassment (Head 3 (1)(iii) below).

Subject to this last-mentioned defence, it will in general make no difference to the commission or otherwise of this tort whether or not the surveillance or harassment was carried out by or on behalf of the person disclosing the information -e.g., a media publisher. This is of importance to this part of the proposals. Surveillance and harassment designed to invade privacy may well be carried out by persons who, at the time of the surveillance or harassment, have no legal or other relationship with subsequent publishers of the information or of material gained thereby. (Where the public interest defence (Head 3(1)(iv)) is relied on, that defence will be defeated if the defendant cannot show that he was not party or privy to the unlawful surveillance (Head 3, Proviso)).

THE FOURTH TORT - Head 2 (iv)

The fourth proposed tort is that of disclosure within the State of information obtained outside the State by means which, had they been used to obtain such information within the State, would have involved either (or both) of the torts of privacy-invasive surveillance or harassment within the meaning of the proposed legislation. The prohibitions of privacy-invasive surveillance and of harassment contained in Head 2 (i) and (ii) are applicable only within the State. Yet, because of the international dimension which has been clearly demonstrated to exist in the province of information or newsgathering and its subsequent dissemination and publication, often involving the payment across transnational boundaries of very large sums of money by, for example, the tabloid press in one country to paparazzi in other countries, it is essential to have such a provision if there is not to be a serious gap in the legislation.

It is of course fully recognized that ideally, this is a matter which would best be addressed by international agreement between States in this sphere. Such

international agreement however does not seem likely to be achieved in the short run and if and when it is achieved it seems likely that it will, at least initially, support rather than displace national legislation.

Although, therefore, the surveillance or harassment will have taken place outside the State, the publication within the State of information gained thereby will be a tort under this Head of the proposed legislation. Properly understood, this is not a case of extra-territorial jurisdiction in tort; the gathering of the information, even by privacy-invasive surveillance or harassment, outside the State will not be legally actionable under the legislation; only the act of disclosing it within the State will be so actionable.

It should also be understood however that the persons protected by this provision as proposed would potentially include persons who are neither citizens of nor resident in, nor persons having any particular connection with, the State, as well, of course, as Irish citizens or others resident in or having a definite connection with Ireland. After careful consideration we consider that this broader scope of the new tort created by paragraph (iv) of this Head is justified given the international dimension of the problem. Persons who have no interest of substance in suing here are unlikely to do so; those who have such an interest, whether or not they are connected with this country, should be entitled to do so.

The obligations imposed by this proposed tort would, as far as the media are concerned, apply equally to the non - Irish media as they would to the Irish media, and would accordingly confer no competitive advantage on non-Irish media products marketed in this country.

Head 3: Defences

(1) It is a defence -

- (i) to an action under Head 2(i), 2(ii), 2(iii) or 2(iv) to show that the plaintiff, or some other person legally entitled to give consent on behalf of the plaintiff, consented, either expressly or impliedly, to the invasion, harassment, or disclosure as the case may be;**
- (ii) to an action under Head 2(i), 2(iii) or 2(iv), as the case may be, to show**
 - (a) that the person by whom or on whose behalf the surveillance was carried out, or (as the case may be) the person by whom or on whose behalf the information or material was disclosed was fulfilling a legal duty, or exercising a legal power, or defending or maintaining a legal right of that person (other than a legal right which but for Head 2, that person would have enjoyed); and**

- (b) that the surveillance or disclosure, as the case may be, was justified by and was not disproportionate to the legal interest pursued;
- (iii) to an action under Head 2(iii) or 2(iv) to show that at the time of such disclosure the defendant acting in good faith did not know and had no reasonable grounds to believe that the information had been obtained in breach of Head 2(i) or Head 2(ii);
- (iv) to an action under Head 2(iii) or 2(iv) insofar only as those provisions refer to the disclosure of the purport or substance of information or material obtained by means of privacy-invasive surveillance (excluding disclosure of such information or material obtained by means or as a result of harassment)
- (a) to show that disclosure of the purport or substance of such information or material was justified by overriding considerations of the public interest;
- or, if it could not be shown to have been so justified,
- (b) to show that the defendant had reasonable grounds to believe and did bona fide believe that such disclosure was justified by overriding considerations of the public interest; in deciding whether the defendant had such reasonable grounds the court shall where appropriate have regard to the care (including enquiries) as to the accuracy of any material or information upon which the defence is based which in the opinion of the court ought to have been, and which was in fact, exercised by the defendant, in the circumstances.
- (v) to an action under Head 2(iii) or 2(iv) to show that the disclosure was made in circumstances in which, had the action been for defamation, the defendant would have enjoyed absolute privilege in respect of such disclosure.
- (2) For the purposes of this Head, the disclosure of the purport or substance of information or material obtained by means of privacy-invasive surveillance is not in the public interest merely because the object of such surveillance, or such information or material, is or would be newsworthy.
- (3) In deciding whether a defence under paragraph (1)(iv) of this Head has been established, the court shall have regard to all the relevant circumstances, including, where the court considers it appropriate -

- (a) whether such disclosure was justified in the interests of the detection or prevention of serious crime;
- (b) whether such disclosure was justified in the interests of the exposure of serious illegality or other serious wrongdoing;
- (c) whether such disclosure was justified in the interests of the need to inform the public on a matter of public importance;
- (d) whether such disclosure was justified in the interests of preventing the public from being misled by public conduct (including statements) of a person having or seeking a public office or function or in or seeking to be in a position of leadership, influence or importance in the eyes of the public, where the true facts, in the light of such conduct or otherwise, are relevant to the situation of that person (including that person's suitability, capacity or credibility) in relation to that office, function or position.

PROVIDED THAT

- (a) where the disclosure was of the purport or substance of information or material obtained by means or as a result of privacy-invasive surveillance contrary to Head 2(i)
 - (i) which surveillance, in the opinion of the court, involved the commission of any of the acts specified in the list contained in the Schedule to these Heads, irrespective of whether, at the time of such disclosure, such involvement was known to the defendant, or
 - (ii) to which surveillance the person relying on the said defence does not show that he was not party or privy

the defence for which paragraph (1)(iv) of this Head provides shall be disallowed; and
- (b) where, though disclosure of information concerning the particular subject was justified in principle by overriding considerations of the public interest, the particular disclosure which was actually effected, by reason of its detail or salaciousness, or of the extent of its intrusiveness into private life, or otherwise, and having regard where appropriate to paragraph (1)(iv)(b) of this Head, was excessive, the defence for which paragraph (1)(iv) of the Head provides shall only be allowed to the extent that such disclosure was not so excessive.

- (4) **The information, to the obtaining or disclosure of which the defence mentioned in paragraph (1)(ii) of this Head applies, shall not be used as evidence in court proceedings or in proceedings before any tribunal or other body having power to compel the giving or production of evidence for the purpose of any proceedings before it unless, a reasonable time in advance of its being so used, the person or persons who have been subjected to such surveillance is or are informed of the fact, date, place and manner of the surveillance and of the material or information obtained thereby.**

EXPLANATORY NOTE:

Paragraph (1): This paragraph of the Head sets out the defences available to a defendant which would permit the defendant to defeat the plaintiff's action for the tort specified in each respective defence notwithstanding that but for the defence the commission of the tort would be established in the evidence. This would not of course prevent the court's trying as a preliminary issue the question as to whether the defendant had a defence under Head 3 in advance of the issue whether the plaintiff had otherwise a good cause of action under Head 2 if the Court thought fit. It remains correct to say however that the legal function of the defences under Head 3 is to defeat a cause of action which would otherwise have been established.

It is important to note that an act which is a tort under Head 2 may also be a criminal offence under Head 9 (or indeed Head 11). In applying the civil defences under this Head (Head 3) to a case where this possibility arose, a court would presumably be anxious to avoid a construction which, in the light of Heads 9 and 10, would mean that the same act was a criminal offence but not a tort. It is considered that the Heads leave sufficient room for the courts to avoid such a seemingly anomalous result.

These defences should be considered in the light of the State's international obligations under Articles 8 and 10 of the European Convention on Human Rights, to which the State is a party even though that Convention is not part of domestic law in this country.

The interpretation and application of Articles 8 and 10 of the Convention and the inter-relationship between them are discussed in Chapter 5 of the main text of this Report, and detailed new research on this question is fully set out in Annex I. We are confident that the present proposals would pass muster under these Articles of the Convention.

THE FIRST DEFENCE - Head 3(1)(i) - CONSENT

The first defence, which is expressed as being applicable to all of the torts proposed under Head 2, namely privacy-invasive surveillance, harassment and the two respective torts of disclosure, is that the plaintiff consented to the tort. This provision does not need explanation; if the plaintiff consents then there is no tort. It is arguable that strictly speaking it is not necessary to provide for consent as a

defence, but it is commonly provided for in the privacy legislation of other common law jurisdictions which we have considered, and hence it is included. Consent may be expressed or given implication according to the circumstances.

THE SECOND DEFENCE - Head 3(1)(ii) - LEGAL POWERS, DUTIES OR RIGHTS

In fact, there are three distinct, if related, defences grouped here under one heading. They would allow the defendant by whom or on whose behalf an act which would otherwise be a tort has been committed to show that he was exercising a specific legal power or legal duty, or enforcing or maintaining a specific legal right, of the defendant, and that the act was justified and proportionate in the circumstances. Thus, for example, if the relevant information, albeit properly required, could reasonably be expected to have been obtained without invading the privacy of the subject or by means less invasive of that privacy than those actually used, the court may disallow the defence in relation to the particular acts of privacy-invasion actually employed.

The defences are available to the person by whom or on whose behalf the surveillance was carried out (in the case of an action under Head 2 (i)) and to the person by whom or on whose behalf the material or information was disclosed (in the case of an action under Head 2 (iii) or (iv)). They will also be available to the person who actually performs the surveillance or effects the disclosure where this is done on behalf of another and where that other in having the surveillance carried out or in having the disclosure made on his behalf was fulfilling a legal duty, or exercising a legal power, or defending or maintaining a legal right of that other. This would include for example the case of a defendant or a plaintiff employing a private detective to make enquiries or keep persons under observation for the purposes of defending or maintaining a civil action. The plaintiff or defendant (as the case may be) and the detective would be covered provided they stayed within the limits of justification and proportionality in the pursuit of their legitimate purpose.

In each case the legal right concerned must be one which exists independently of any right affected by the prohibition in Head 2. The defendant will not be able to say that "but for Head 2 I would have had a legal right to do such and such; therefore I have a defence under Head 3 (i) or (ii)".

An example of a person acting under a legal duty would be a member of An Garda Síochána lawfully obeying a lawful order of his superiors to carry out surveillance of a person in the interests of the prevention or detection of crime; equally, the reference to a "legal power" would encompass the exercise of lawful police powers whether conferred by common law or by statute; and an example of the defence based on a person's defending or maintaining a legal right of that person would be that of a person using reasonable means (including the engagement of an agent such as a private detective-see above) to discover evidence for the purposes of civil proceedings to be brought or defended by that person.

The defences of "lawful authority, lawful power or lawful right" must be read in the light of Heads 9 to 11 below which propose that subject to certain exceptions or

qualifications certain forms of surveillance should be made criminal, and that certain forms of surveillance by An Garda Síochána should be subject to a prior authorisation procedure, initially involving a superior officer but with subsequent judicial confirmation where surveillance is continued beyond a specified, short period. Surveillance of a kind covered by any of these provisions which was carried out in contravention of them, whether by the Garda authorities or by others, could not benefit from any of these defences.

It will be noted that none of these defences under Head 3(i)(ii) is expressed to be available in respect of the tort of harassment. That tort, as defined in Head 1(2) (consistent with the crime of harassment created by Section 10 of the Non-Fatal Offences Against the Person Act, 1997), will not be committed where the defendant had "lawful authority or reasonable excuse" for the acts which otherwise would have constituted harassment. It was considered inappropriate to extend the defences under this Head to harassment but it should be kept constantly in mind that by virtue of the definition of the tort of harassment, defences closely analogous to the defences under Head 3(i)(ii) will be applicable to harassment in any event.

THE THIRD DEFENCE - Head 3(1) (iii)-DISCLOSURE IN IGNORANCE OF THE FACT OF PRIVACY-INVASIVE SURVEILLANCE OR HARASSMENT

The defendant disclosing information in circumstances covered by Head 2 (iii) or 2(iv) will have a defence if he or she can show that at the time of such disclosure he or she bona fide did not know and had no reasonable grounds to believe that the information had been obtained in contravention of Head 2(i) or (ii) (i.e. by means or as a result of the tort of privacy-invasive surveillance or the tort of harassment). It is fair in such a case to place the onus of proof of this knowledge on the defendant who wishes to rely on this defence since his state of knowledge and belief is by definition within his sole knowledge and the plaintiff could not reasonably be visited with the onus of adducing evidence, let alone establishing proof, in this regard. The defence does not as a general rule put the discloser on enquiry as to the circumstances in which the information has been obtained. Circumstances alter cases, however, and the court may take the view that in some circumstances, enquiry is called for. The courts would, it is anticipated, be particularly vigilant in the event of suspicion of collusive behaviour between persons involved in obtaining and publishing information.

It is emphasised that this defence of disclosure in bona fide ignorance would apply to the case where the information had been obtained by means of the tort of harassment no less than where it had been obtained by the tort of surveillance. This is important in view of the exclusion from the proposed public interest defence, which would be applicable to the torts of disclosure above, of cases where the published information has been obtained by harassment.

THE FOURTH DEFENCE - Head 3(1)(iv)-DISCLOSURE IN THE PUBLIC INTEREST

The Law Reform Commission has decided, having regard to the submissions it has received and to representations made at the "oral hearing" held in the wake of those submissions, that the inclusion in the legislation of a "public interest defence" to the

torts of disclosure created by Head 2(iii) and (iv) is not only warranted but necessary. Once again, however, for the reasons already stated, the disclosure of information or material obtained by means of or as a result of harassment is excluded from this defence. A person disclosing information obtained by means of harassment will not be able to rely on the public interest defence though he will be able to avail of the defences of consent (Head 3(1)(iv)) or of bona fide ignorance (Head 3(1)(iii)) if he can establish them in evidence.

Although disclosers of information obtained in contravention of Head 2(i) will escape liability if they can prove that such disclosure was in the public interest, the act of privacy-invasive surveillance (or, ex hypothesi, of harassment) which resulted in the obtaining of the information will remain actionable torts under the legislation. It is not the purpose of this defence to permit privacy-invasive surveillance or harassment in the public interest; its purpose solely is to give a defence based on the public interest, subject to certain limitations set out in a proviso to this Head, to persons subsequently disclosing such information. (See Chapter 8, paras. 8.17-8.34 of the main Report.)

The onus is on the defendant in an action for the tort of disclosure of information or material obtained by means of privacy-invasive surveillance to establish the public interest defence. Under the proposals this could be done either by showing to the satisfaction of the court that disclosure of the material or information was objectively justified by overriding considerations of the public interest, or (even if this could not be established) by showing to the satisfaction of the court that the defendant, in disclosing the information, believed and had reasonable grounds to believe that disclosure of the information or material was or would be so justified.

This second alternative would introduce a subjective element into the "public interest defence". In cases involving the media, it would cover both assessments by media editors of the quality of facts relied on as providing justification for publication in the public interest, although in the event such assessments were held by the courts to be erroneous having regard to the true interpretation of the public interest, and, insofar as they might arise, errors of fact as to the grounds for publication in the public interest where the media editor had shown that reasonable care including the making of appropriate enquiries had been taken to get the facts right. It is considered therefore that the "facts" in question here would primarily be those relating to the justification for publication in the public interest rather than those relating to the truth or otherwise of the information published, though they might include the latter as well. Of course, the law of defamation would in any event apply where the published information was incorrect and defamatory.

This (subjective) wing of the public interest defence would perhaps be of greatest assistance to media editors while case law was being developed by the courts on the interpretation and application of the public interest defence under the legislation; the provision envisaged would help to mitigate any uncertainty regarding the availability of that defence which would exist while this was taking place.

At the same time the provision ought to be sufficiently rigorous to avoid a situation in which it would become a means whereby a "coach and four" could be driven through the prohibition in tort of disclosure of information obtained by privacy-invasive surveillance.

Although the public interest defence does not expressly mention the media it is clear that its main purpose and effect would be to give a measure of protection based on the public interest to the media subject to the limitations just mentioned, if they publish information obtained by privacy-invasive surveillance.

The phrase "overriding considerations of the public interest" is not exhaustively defined but indicative examples are given under paragraph (3) of this Head as to what it means, for the benefit of the public and the Courts.

***Paragraph (2)** of this Head is intended to make clear the distinction between matters whose publication is justified by overriding considerations of the public interest on the one hand, and matters about which the public or some of its members would be interested to be informed i.e. matters which are merely newsworthy on the other hand. Matters falling into the latter category might include the most intimate details of the private lives of either private or public persons or other forms of private scandal in which there is a prurient interest on behalf of some members of the public which can be exploited for commercial purposes by some sections of the media; i.e., they may be eminently "newsworthy" - but this does not mean that their publication is called for in the public interest. The public interest in this latter sense is a reference to the common good as opposed to the gratuitous satisfaction of the appetites of some for information about the private lives of others.*

***Paragraph (3)** of this Head sets out certain non-exhaustive "pointers" for the assistance of the courts in deciding whether or not a particular disclosure of material was justified by overriding considerations of the public interest. In considering the application in practice of this defence it should be recognised that where the public authorities are defendants, they will normally rely on the defence that they acted under a legal power or duty, where necessary with the benefit of a judicial order or warrant or other statutory authorisation, under the second defence specified in paragraph (1) of this Head rather than on the broader "public interest" defence. The exercise by and performance of public authorities of their powers and duties, respectively, vis-à-vis the citizen are of course also subject to judicial review as to their legality by the High Court under existing law.*

With regard to the list of considerations (a) to (d) set out in paragraph (3) of this Head, the following observations are offered:

***Point (a) - the detection or prevention of serious crime** - may, depending on the circumstances, be of somewhat limited application inasmuch as *prima facie*, where a person is in possession of information which is relevant in this regard his first duty is to bring it to An Garda Síochána so that they may follow it up. This will not however necessarily mean that disclosure or publication of the information, for example by publication in the media, is to be ruled out of the "public interest*

defence"; for example, there may be circumstances in which a person in possession of such information will be justified in taking and acting on the view that the prevention or detection of crime by the public authorities will benefit from the stimulus of public concern generated by publication of the relevant information to a wider audience than that of the public authorities alone. See in this regard the recent majority judgment of the Supreme Court in National Irish Bank limited and another -v- R.T.E., judgment of Lynch J. (O'Flaherty J. and Barrington J. concurring) delivered on 20 March, 1998. (A minority judgement indicating a contrary view on this issue was delivered in this case by Keane J., Hamilton C.J. concurring.) One might also envisage such a case arising, for example, where it is the conduct of the public authorities themselves which is at issue.

Point (b) - "serious illegality or other serious wrongdoing" - is intended to enable the public interest to be protected in respect of matters of legitimate public concern while protecting individuals from being pursued for matters which, though newsworthy in the eyes of some, are not of legitimate public concern. As with the other provisions it will be a matter for the courts to decide on which side of the line a particular case falls.

Point (c) - the need to inform the public on a matter of public importance - Although public figures as well as purely private persons have rights of privacy and should be free from gratuitous surveillance of their private lives, there can be no doubt that the private affairs of persons in public life - and even, sometimes, of purely private persons - are liable to be such that if known they would properly be regarded as matters of considerable public importance, reflecting perhaps on the fitness of persons to hold public office or on the true motives or effects of the conduct of such persons while in public office. The true state of health of a person, where this was relevant to that person's ability to perform a public function, would be one example of this. Such considerations are not of course confined to persons in public office; they might apply also to persons prominent in the business community or exercising influence in one or other way on national life. For example, a person's past conduct (not necessarily involving fraud or other illegality) in a private business firm might be relevant to that person's suitability to manage a public corporation or a charity. The holding of public enquiries is not of itself a sufficient guarantee that such matters will be brought to the attention of the public; indeed, decisions to hold such public enquiries are not infrequently stimulated by the prior publication of information of the kind to which this paragraph refers.

Point (d) - the correction of misleading information (including information about their private lives) conveyed to the public by persons having a position in the public eye - is perhaps more controversial and sensitive, since it may involve the more intimate facts and details of the private lives of such persons, which in our view would normally not without good reason be a legitimate subject of surveillance and publication in the public interest. However, such persons sometimes, for the sake of their own advantage in their public positions or otherwise in the eyes of the public, in one form or another present false pictures to the public of their private lives or publicly criticise others for conduct of which they are privately guilty themselves. Many people would consider that there is a strong case for saying that

publication of at least sufficient information to expose such falsity or hypocrisy, even where that information has been obtained by privacy-invasive surveillance, should be permitted. This is not to say however that the publication of salacious or intimate details going beyond what is reasonably required to expose the falsity or hypocrisy will be justified under this defence. Moreover, not every failure to live up to one's own professed standards is per se hypocrisy. The purpose of this consideration with regard to the public interest defence is to save the public from misleading information put about in public by "public people" themselves, not to provide an open licence for reverse judgmentalism by the media or others. The consideration is expressly confined to preventing the public from being misled about a matter which is relevant to the position in the public eye of the person in question. Such relevance may, for the reason already mentioned, arise from the misleading actions or statements of that person.

As already stated, we propose that the public interest defence should not be available where the information disclosed was obtained by means or as a result of harassment. Harassment will having regard to existing legislation and to our proposals be a crime as well as a tort and we are of the view that publication of its fruits should not be given a "public interest" protection. This is consistent with our proposal, which is next discussed, also to disallow the public interest defence in respect of disclosure or publication of information or material obtained by certain types of surveillance which are specified in the Schedule to the Heads.

PROVISO TO THE PUBLIC INTEREST DEFENCE - Head 3(3)

The contents of the Proviso in general:

The "public interest" defence to the tort of publication of information which has been obtained by means of unlawful surveillance (though not of harassment) is among other things intended to prevent the privacy legislation which we recommend being abused by persons whose behaviour is contrary to the common good or in order to keep secret material which in a democratic society ought to be made known to the public. However, we have concluded that the defence must be subject to limitations. We have come to the conclusion that the appropriate limitations, which are set out in the Proviso, are the following three:-

- **Limitation No.1:** that the discloser must not himself or herself have been party or privy to the illegal surveillance; otherwise, the defence would indeed become a "coach and four" to be driven through the right of privacy (clause (a)(ii) of the Proviso;

- **Limitation No.2:** that the acts of surveillance by means of which the material or information was obtained did not constitute any of a number of specified acts set out in the Schedule to the Heads, all of which are or would be criminal offences under our Recommendations to which privacy-invasive surveillance is particularly relevant (clause (a)(i) of the Proviso).

The particular acts which we set out in the Schedule to the Heads (which appears at the end of the Heads) are as follows:-

- (i) *Interception of the post or unlawful interception or monitoring of electronic communication contrary to the Postal and Telecommunications Services Act, 1983 and the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 (we are proposing certain amendments to these Acts to bring them up to date having regard to present circumstances).*
- (ii) *Obtaining data by means of acts constituting illegal surveillance under Head 2 which acts also constitute a contravention of the Data Protection Act, 1988.*
- (iii) *Unlawfully accessing data by means of the operation of a computer contrary to Section 5, Criminal Damage Act, 1991.*
- (iv) *Placing an optical or hearing device in a dwelling, or using such a device from outside a dwelling to spy on persons, matters or events within a dwelling, contrary to the proposed criminal Head 9(1)(a) below.*
- (v) *Trespassing on premises in pursuit of personal information contrary to proposed criminal Head 9(1)(b) below.*
- (vi) *Spying on the conversations of individuals by means either of a hearing device or an optical device adapted or used for such spying e.g. by lipreading, contrary to the proposed criminal provision in Head 9(1)(c) below. (Hearing and optical devices do not include ordinary hearing aids for deaf persons or spectacles or contact lenses designed and used solely to restore or maintain normal standards of hearing or eyesight - see Head 1.)*

*- **Limitation No.3:** that the disclosure must not have been of such a nature or degree that it exceeds what was required to satisfy the public interest; in such a case the "public interest defence" should be disallowed to the extent that publication was excessive (clause (b) of the Proviso).*

Excessive publication:

Clause (b) of the Proviso is directed to cases where, although publication of information obtained by privacy-invasive surveillance is justified in the public interest, the actual publication effected in the particular case, by reason for example of its extent or detail, goes beyond what is so justified. The public interest defence is not intended as a charter for the gratuitous publication of salacious or otherwise excessive details of people's intimate or private lives going beyond what is reasonably necessary to satisfy the public interest. It is intended solely to enable the public interest (in the sense of the common good) to be served.

The legitimate public interest in knowing certain facts which would ordinarily be protected by the privacy "shield" in relation to the private life of a person may be

satisfied by information of a more or less general nature, for example, concerning the family or other private life of a person in the public eye who in public has been projecting a false image, without going into the intimate details of that person's private life. There is a point at which the true public interest (as explained above) is satisfied, beyond which further disclosure has nothing to do with the true public interest but lies in the realm of the exploitation of scandalous material for the satisfaction of prurient interest and the profit of the publisher.

At the same time, there would be cases in which the publication of full details would genuinely be in the public interest. For example, publication of the details of financial or business scandals or of the commission of criminal offences may well be as much in the public interest as publication of the bald facts of the case, since knowledge of such details may be of the utmost importance in ultimately satisfying the public that the matters in question have been properly investigated by the public authorities (where such investigation is called for) and that the necessary measures have been taken to prevent a recurrence. And the need to demonstrate the truth of published material may well call for details going beyond mere general statements. Thus, not all publication of detail is to be regarded as excessive; the issue will depend on the nature, facts and circumstances of the case, the assessment of which will be a matter for the courts.

We recommend however that even where such excessive publication occurs, where there is a public interest in the publication of information, perhaps of a more general nature, concerning the matter at issue, the public interest defence should be disallowed, not in its entirety, but only to the extent that such publication has been excessive.

It is already conceded in paragraph (1)(iv) of this Head that media editors should be allowed a degree of discretion in deciding what it is reasonable to publish in reliance on the public interest defence; the existence this discretion is expressly recognised for the purposes of clause (b) of the Proviso.

It is also important to note that even where the public interest defence is excluded or defeated, in whole or in part, upon any of the grounds contained in the Proviso, the person publishing the information will still have a defence if he or she can establish that he or she did not know and had no reason to know that the information published had been obtained by means of privacy-invasive surveillance or harassment [paragraph (1)(iii)]. This would be the case even where such means involved the commission of one of the criminal offences mentioned above or indeed any other criminal offences.

We believe that these provisions would strike a fair and proportionate balance between the necessity to protect the right of privacy and the necessity to allow the media in particular to perform their task.

***Paragraph (4)** of this Head provides that information obtained by surveillance which is lawful on the basis of the second defence may not be used as evidence in court or other comparable proceedings unless reasonable notice involving full particulars*

of the surveillance carried out and of the information obtained thereby is given to the party against whom the surveillance was carried out in advance of the material being so used in evidence. The purpose of this provision is to require that the person against whom surveillance has been carried out should be given a reasonable opportunity both to contest the legality of the surveillance if he or she thinks fit and in any event to contest the veracity of the information alleged to have been obtained as a result thereof.

Head 4: Remedies

In an action under Head 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.**

EXPLANATORY NOTE:

Not every tort committed in contravention of Head 2 will sound in damages. A range of remedies is open to the plaintiff and ultimately to the courts. These will include an account of any profits made as a result of the tort - a consideration which may in particular arise where there has been publication of material obtained by means of privacy-invasive surveillance or harassment. It must be borne in mind however that since the torts enumerated under Head 2 are, it is proposed, to be actionable without proof of damage, damages can in the appropriate case be ordered by the court even where there has been no actual financial loss or personal injury to the plaintiff. Damages may include aggravated damages for the injury to the plaintiff's feelings by reason of the manner or circumstances in which the tort has been committed - a consideration which is liable to arise in the sphere of privacy-invasive surveillance or harassment.

Head 5: Privacy orders

- (1) The Court may, if it is of opinion that a tort contrary to Head 2 has been committed or that there are reasonable grounds for believing that a tort is being or is about to be committed contrary to Head 2, by order (in these Heads called a "privacy order") prohibit the defendant from invading the privacy of or harassing the other person or disclosing 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 at any time be varied by the Court on the application of either the plaintiff or the defendant.**
- (3) A privacy order may at any time be discharged by the Court on the application of either the plaintiff or the defendant if the Court is satisfied that the privacy or protection from harassment 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 paragraph (5) of this Head, 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 paragraphs (6) and (7) of this Head 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 paragraph (9) of this Head 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.**
- (12) On an application under this Head for an order restraining the disclosure or publication of information the Court shall take into account the public interest, if any, in disclosure or publication.**

- (13) **On an application under this Head for interlocutory relief to restrain the disclosure or publication of information, where the defendant makes out a good arguable case for a defence under Head 3(1) to (3) inclusive in the public interest, the Court in addition to any other discretion vested in the court may refuse to grant the injunction where the justice of the case so requires.**

EXPLANATORY NOTE:

This Head consisting of eleven paragraphs is intended to address the powers of the court to make what is described as a "privacy order" in paragraph (1). It should be noted that a "privacy order" encompasses the commission or anticipated commission of any tort under Head 2, including harassment of the plaintiff. At the same time it is not proposed to extend the jurisdiction of the court to make a privacy order under the legislation to any matter not prohibited by Head 2 - i.e. to any matter which, though falling into the sphere of protection of privacy in its wider sense, falls outside the boundaries of Head 2.

On the making of a privacy order the provisions of paragraphs (2) to (11) inclusive of Head 5 which are largely though not entirely procedural in nature come into play. These procedures cover such matters as the right of a party to apply for the variation or discharge of a privacy order, the question of appeals, the question of the giving of notice of such orders to parties affected thereby, and the power of a court where there is an appeal to stay the operation of a privacy order if it sees fit.

Paragraphs (12) and (13) are intended to give the court maximum discretion in the granting (or refusal) of both interlocutory and final privacy orders; and paragraphs (2) and (3) give the court power at any time even after the conclusion of proceedings to vary or discharge a privacy order.

Head 6: Persons entitled to sue

- (1) **A right of action under Head 2 accrues to the person whose privacy is alleged to have been or to be about to be invaded or who is alleged to have been or to be about to be harassed, in contravention of Head 2, and to any other person who is legally entitled to act on behalf of that person.**
- (2) **An action or right of action under Head 2, in so far as concerns the remedy of damages or an account of profits, is extinguished by the death of the person whose privacy is alleged to have been invaded or who is alleged to have been harassed. An action or right of action under Head 2, 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 or who is alleged to have been harassed.**

EXPLANATORY NOTE:

Paragraph (1) of this Head indicates the persons who would have a right of action under the proposed legislation. An example of "any other person who is legally entitled to act on behalf of" the person whose privacy is alleged to have been or is about to be invaded would be a parent acting on behalf of a child who is not of full age.

Paragraph (2) of this Head provides that an action or right of action for damages or an account of profits (i.e. monetary relief on account of a tort under Head 2) is extinguished by the death of the person whose privacy is alleged to have been invaded or who is alleged to have been harassed. On the other hand, a claim for a privacy order, the delivery up of material which has come into the defendant's possession by reason or in consequence of the tort (such as private or confidential documents) or any other relief remains a matter in which the family or estate of the deceased injured party may continue to have an interest and the cause of action under the legislation in these respects would survive the death of the person concerned.

Head 7: Limitation period

Provide that an action under Head 2 shall be commenced within three years from the date on which the person who claims that his or her privacy has been invaded or that he or she has been harassed became aware or ought reasonably to have become aware of the surveillance, harassment, or disclosure, as the case may be, and of the identity of the defendant, with supplementary provisions along the lines of the *Statute of Limitations (Amendment) Act, 1991*.

EXPLANATORY NOTE:

The limitation period is based on the limitation period for personal injuries in tort fixed by the Statute of Limitations (Amendment) Act, 1991. The three year period of limitation for bringing an action under the proposed legislation does not begin to run until the injured person (or other person, such as his or her successor, entitled to bring the action) became aware or ought reasonably to have become aware of the commission of the tort and the identity of the defendant.

Head 8: Other rights of action and remedies

- (1) The rights of action and the remedies under this Head are in addition to, and not in derogation of, any other right of action or remedy available otherwise than under this Head.**

- (2) This section shall not be construed as requiring any damages awarded in an action under Head 2 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 Head 2.

EXPLANATORY NOTE:

Paragraph (1) of this Head preserves, in cases where a right of action exists under the legislation, the existence of other rights of action not provided for by the legislation, i.e. causes of action which have an independent existence. Examples of these would be trespass to land or nuisance or assault, all of which are liable to exist alongside, for example, a right of action for privacy-invasive surveillance or harassment.

Paragraph(2) of this Head however means that where such rights of action coexist on the basis of the one set of facts, the damages awarded to the successful plaintiff in an action for a tort created by Head 2 may if the court considers it appropriate be taken into consideration in assessing the damages to which the plaintiff may be entitled in respect of a cause of action not created by Head 2. It is in justice to the defendant that the court should be allowed to do this; otherwise plaintiffs might obtain double or even multiple compensation in respect of matters which, though they constituted separate causes of action, were so closely related that they should be covered by a single award.

Head 9: Criminal Offences

- (1) Provide that the following shall be offences:-
- (a) **Infringement of the privacy of a person by installing in a dwelling or using, whether inside or outside a dwelling, with a view to observing, overhearing or recording any matter in that dwelling, any optical (including still camera) or hearing device, including recording device.**
 - (b) **Trespassing on private property whether by unlawfully entering or unlawfully remaining thereon, where such trespass is effected or done for the purposes of observing, overhearing, or obtaining (including recording) information therein concerning any person.**
 - (c) **Infringing the privacy of a person by intentionally listening to or recording a conversation (including part of a conversation) of that person by means of a hearing device (which expression shall be deemed to include an optical device adapted or used**

to permit lipreading) without the consent of at least one party to that conversation.

- (d) Disclosing information including the purport or substance of information heard or recorded contrary to the prohibition at offence (a) or (b) above.
 - (e) Disclosing information including the purport or substance of information heard or recorded contrary to the prohibition contained in the offence at (c) above without the consent of least one party to the conversation in question.
 - (f) Disclosing information including the purport or substance of information heard or recorded in circumstances to which either of the defences in subparagraph (d) or (g) of Head 10 applies.
- (2) The privacy of a person may be infringed under subparagraph (a) or subparagraph (c) of this Head, and an offence may be committed under subparagraph (b) of this Head, irrespective of the content or quality of any material or information actually obtained or sought, and even if no material or information is actually obtained by means or as a result of the act complained of.
- (3) In subparagraphs (a), (b) and (c) of this Head, "person" means natural person.

EXPLANATORY NOTE:

It should be stated first that the criminal offences for which this Head (and in a more limited sense Head 11) provides are not the only criminal offences in the sphere of surveillance and the interception of communications. As indicated in our Consultation Paper (Chapter 5, pages 88-120) there is already a wide range of criminal sanctions, including common law offences such as breach of the peace and eavesdropping and statutory offences designed to protect the mail, telegraphic communication and personal data, and to prevent "computer hacking" etc.. We are proposing (Head 13 below) that two of the relevant statutes - the Postal and Telecommunications Services Act, 1983 and the Interception of Postal Packets and Telecommunications (Regulation) Act, 1993 - should be amended to bring them up to date with new technological developments and with the recent opening up of the telecommunications industry in Ireland.

In addition we propose under the present Head the creation of six new criminal offences directed to two particular categories of privacy-invasive surveillance and one category of trespass on private property which in our view are especially offensive and repugnant except where they can be justified under one or more of the specific defences for which Head 10 provides or where they are specifically authorised under Head 11.

Proposed offence (a) is that of infringing the privacy of a person by installing in a dwelling or using, whether from inside or outside a dwelling with a view to observing, overhearing or recording in the dwelling, any optical or hearing (including recording) devices. "Dwelling" is defined broadly in Head 1 to include a wide range of dwelling accommodation.

There are a number of points to be noted regarding this proposed offence (a). First, no particular information need be obtained and no actual event or fact need be proved upon for the offence to be committed. Where the surveillance consisted of the installation of an optical or hearing device in a dwelling the rationale for this provision would be clear enough. In such a case, there is a clear infringement of privacy by reason of the intentional installation of the device irrespective of whether any actual information is recorded or obtained as a result. Where the surveillance takes place from outside the dwelling the position is arguably less clear. However, we take the view that subject to the defences in Head 10, the use even from outside a dwelling of an optical or hearing device (which would include binoculars or a still camera no less than any recording or video device) to intrude upon the privacy of a person in respect of his or her dwelling is a socially unacceptable act which calls for criminal sanction in addition to whatever civil sanction may be applicable.

We also include under the rubric of this proposed offence the case of the use within a dwelling of any of the devices in question for the purposes of invading privacy within that dwelling. Thus, a visitor to a dwelling (or still more, a trespasser in a dwelling) who used one of the devices in question in order to infringe the privacy of a person in that dwelling, even though he or she did not install the device there for this purpose, would commit the offence.

This offence applies to a "dwelling" as defined in Head 1 and would therefore include not only a dwelling as that term is traditionally understood, but also the bedroom and other associated (e.g. private bathroom) accommodation of a hotel, guesthouse, hospital or other such establishment as well as the curtilage of a dwellinghouse. It would not however include other private premises such as business premises or the public parts of a hotel or guesthouse. We consider this distinction to be justified because the invasion of a person's privacy in his or her dwelling is a matter which, for constitutional no less than other reasons, is of special seriousness and calls for protection over and above that accorded to other private premises.

We propose that the offence should only be committed where optical or hearing devices are used. Ordinary overhearing or spying with the naked eye are not, we believe, in the same category although they may constitute offences under other legal rules e.g. eavesdropping or conduct likely to cause a breach of the peace, and although they may well involve civil liability under our proposals.

The offence is only committed where the privacy of a person is infringed. Clearly, the existence of expressed or implied consent would remove the case from the grasp of the criminal law no less from than from the prior view of the civil law.

We stress that it is the installation or use of the device rather than the information actually obtained which is central to the commission of the offence. Thus the offence may in principle be committed even though no victim of the invasion of privacy is actually present in the dwelling at the time, or no particular information is obtained.

Proposed offence (b) *is directed to a particular type of trespass on private property (whether a dwelling or not). The object of this proposed offence is not to make all acts of trespass on private property criminally punishable. It is to make criminally punishable those acts of trespass which are committed with the intention of obtaining information therein concerning any person. The particular trespass is therefore directed to information privacy, not to the broader right of undisturbed possession of one's premises. It will be noted that the term "property" is used rather than "dwelling" or "premises". This offence therefore covers trespass on land as well as to buildings and is not confined to dwellings.*

The trespass may consist of unlawfully remaining on private property (e.g. following a request to leave) as well as unlawful entry. No surveillance device need be used for the offence to be committed.

The question whether an entry onto or the act of remaining on premises constitutes a trespass will have to be determined in each particular case where there is a prosecution under this provision. Usually persons who enter a premises by the normal entrance, if there is one, by which the public are intended to enter, for the purpose of transacting lawful business, will not be trespassers. However this may be altered by the gaining of entry through some irregular means such as climbing a wall or forcing a locked gate or door, or even ignoring available means of electronic communication with persons inside the premises in order to effect entry without their knowledge where it is likely that their consent, if sought, would be refused.

Proposed offence (c) *is that of infringing the privacy of a person by using a hearing device to listen to or record a conversation without the consent of at least one party to the conversation. "Hearing device" would include the use of an optical device adapted or used for the purposes of lipreading. We regard the use of such devices for the purposes of spying on people's conversations as a particularly odious and unacceptable form of intrusion on privacy which ought to be criminally punishable.*

It is of course possible to conceive of a conversation which is regarded by one party thereto as a public event but by another party or parties as private. Prima facie, however, conversations conducted in conditions of privacy (which would include many conversations held in public, such as the public street, out of the normal range of hearing of others) are intended by the participants to be, and should be presumed to be, private. It will be for the court trying any case to assess the facts according to the circumstances of that case.

A conversation may be private even though its actual content is utterly banal, and even where an act of surveillance, or even the subsequent publication of the results thereof, is incapable of inflicting actual harm on the participants. The point in this

regard (as is the case for the civil torts which we recommend earlier in this Report) is that people should be entitled to hold conversations, irrespective of their content, without the fear of having them overheard by others using hearing or optical devices. Such surveillance breaks the privacy "shield" which is the fundamental idea behind our proposals in the civil sphere and which for certain acts should we believe be extended also into the criminal sphere.

Conversations are protected under the new offence irrespective of content (as is the case under interception legislation - see Head 9(2)). If criminal liability for the use of devices to spy on people's conversations could be avoided whenever, in the particular case, the content of the conversation was not particularly sensitive or private, the protection of the civil and criminal law from such surveillance which we envisage would in practice be whittled away and would be virtually worthless.

The new offence is drafted widely to embrace optical devices also. This is so because many optical devices have aural capability. It is also so because optical devices can enable lipreading to take place - a not uncommon occurrence in the world of surveillance.

The recommended offence would apply wherever the consent of no party to the conversation to such surveillance has been obtained. Where even one party to a conversation has so consented, this raises complex issues and in our view removes the justification for criminal sanctions although civil liability in tort may still remain [- see Head 2].

It is not essential to the commission of the above mentioned offences that the information obtained or sought be of any particular level or quality of secrecy or privacy, or indeed that any information at all be obtained. The gravamen of the offence is the breach of the privacy shield.

***Proposed offences (d) and (e)** involve communicating information, or its purport or substance, which has been heard or recorded in circumstances involving the commission of offences (a),(b) and (c) respectively.*

It will be noted that offences (c) and (e) are linked to each other; they conclude with the words "without the consent of at least one party to the conversation". In Head 10 it is proposed in defence (a) that the consent of the person whose privacy is alleged to have been infringed should be a defence. This defence does not make the words "without the consent of at least one party to the conversation" in offences (c) and (e) superfluous. The party to the conversation whose consent is given need not be the complainant who alleges that his or her privacy has been infringed.

***Proposed offence (f)** is related partly to the earlier offences (a) and (c) and partly to defences (d) and (g) in Head 10. It arises because otherwise, persons who benefited from either of these defences (which apply to acts of surveillance only) would be able with impunity to communicate the information or material they had obtained by means of such surveillance to anyone they wished with impunity from*

any criminal liability. If defences (d) and (g) in Head 10 are appropriate, as we consider they are, offence (f) is called for.

Head 10: Defences in respect of the criminal offences

- (a) In respect of all offences, the consent, expressed or implied, of the person whose privacy is alleged to have been infringed.**
- (b) In respect of all offences, the necessary protection of one's own rights by means which are justified by and not disproportionate to the importance of the interest to be protected.**
- (c) In respect of all offences, the necessary protection of the person of someone other than the alleged perpetrator.**
- (d) In relation to offence (a) insofar as it concerns infringement of the privacy of a person ("the complainant") by the defendant's using from outside the dwelling of the complainant any optical or hearing device, a defence on the basis that (i) the complainant is a neighbour of the defendant; (ii) both the plaintiff and the defendant are parties to a mutual arrangement for surveillance with a view to the prevention and detection of crime in their neighbourhood and (iii) the defendant has a reasonable belief that a crime against the complainant (which includes his or her household, its members, and property) is being or may be in the course of being committed on the dwelling; and (iv) the surveillance carried out was not excessive or unreasonable having regard to such reasonable belief and the other relevant circumstances.**
- (e) In respect of all offences, the lawful exercise by An Garda Síochána of powers granted by law (including these Heads) for the prevention, detection or prosecution of crime, including the lawful arrest of any person.**
- (f) In respect of all offences, the existence of lawful authority by or under statute including these Heads.**
- (g) In respect of offences (a) and (c), that the listening or recording was done by or on behalf of a lawful occupier of premises and took place in those premises only and did not involve covert photography or recording of such a nature as to constitute an intentional violation of the intimate and private life of any person on the premises.**

- (h) **In respect of offences (d),(e) and (f), *bona fide* ignorance by the defendant of the fact that the information alleged to be the subject matter of the offence was heard or recorded contrary to the prohibition at offence (a), or offence (b), or in circumstances to which either of the defences in subparagraph (d) or (g) of this Head applies, respectively, as the case may be.**

EXPLANATORY NOTE:

It must be borne in mind that all of these defences arise in respect of offences involving spying on people's conversations or infringement of the privacy of their dwellinghouses by means of the use of hearing or optical devices or, in the case of offence (c), trespass to private property motivated by an intention to infringe personal information privacy. In view of the gravity and offensiveness of the kinds of surveillance involved in such offences we have come to the conclusion that insofar as the protection of others is concerned, leaving aside the case where the person who is the object of surveillance has consented thereto, only the protection of the person of someone other than alleged perpetrator (as opposed to the protection of that person's property or other rights) should be a sufficient justification for surveillance in contravention of the relevant criminal provisions [Head 10(c)]. There are however a number of general exceptions to this, and two specific exceptions.

*The first specific exception concerns the case where there is, so to speak, a "neighbourhood watch" relationship between the person whose dwellinghouse is the object of surveillance and the surveillant [Head 10(d)]. Even then, the person carrying out the surveillance must act reasonably and *bona fide*, and the measures of surveillance taken must be reasonable having regard to that belief and to all the relevant circumstances.*

*We conceive of one other "special case" in which surveillance of a dwelling may be permitted. We would allow surveillance by an occupier of his or her own premises (i.e. premises occupied by him or her) even using privacy invasive devices. Indeed, there are a number of instances in which such surveillance is positively justified -viz., cases where the premises are open to the public such as shops, stores, theatres etc. and the occupier has a *bona fide* interest in protecting himself and his premises by means of such surveillance. Where premises are open to the public however we provide in Head 11 that notice must be given to the public at all entrance points to the premises where surveillance is being carried on by means of the devices in question. The carrying out of such surveillance without such notice would be a criminal offence.*

Another perhaps more sensitive case would be that of an employer who deemed it necessary in his or her own interest to maintain surveillance of his employees on his own premises. The recommendations contained in this Report do not attempt to grapple with the special problems which can arise in such cases. Both the defences of "surveillance of one's own premises" and, perhaps, of defence of one's own rights

(Head 10(b)) would be available to such an employer under our recommendations however. These would mirror the defence in respect of civil liability of the protection or maintenance of one's own legal rights.

It is however a condition of the defence which we recommend in respect of surveillance of one's own premises that such surveillance should not involve covert photography or video recording of such a nature as to constitute an intentional violation of the intimate and private life of any person on the premises [Head 10(g)]. This condition would apply to surveillance directed to employees no less than to anyone else and would be designed also to prohibit certain kinds of grossly abusive surveillance which is sometimes carried on surreptitiously by the occupiers of private premises for reasons which are rightly regarded as illegitimate and impermissible, for example, the surveillance of changing rooms and voyeuristic peeping. Moreover, the other relevant proposed defence of "necessary protection of one's own rights" [Head 10(b)] is also subject to a proportionality test.

We consider that in most if not all cases, where there is a defence to a criminal charge, there will also be a defence to civil liability under Head 2. We are however of the view that the civil defences should in principle be so construed as to avoid any case where there is a defence to civil liability but no defence in respect of the same act to criminal liability.

Defence (a): *Consent of the complainant: This needs no explanation.*

Defence (b): *This defence is that the measures taken were necessary for the protection of one's own rights and that the means are proportionate to the interest to be protected. This mirrors the defence in respect of civil liability under Head 3 above.*

Defence (c): *The necessary protection of the person (as opposed to property or other interests) of someone other than the alleged perpetrator is considered to be a sufficient justification for any of the acts which would otherwise be offences mentioned at Head 9. The protection must be (1) necessary and (2) directed to the safety of the person concerned.*

Defence (d): *The "neighbourhood watch" type defence: this defence is directed to the second offence only (infringement of the privacy of a person by unlawful surveillance of a dwelling) both the complainant and defendant are parties to a "neighbourhood watch" type arrangement. The defendant must act in a reasonable belief that a crime against the complainant (including his or her household, and its members and property) is being or may be in the course of being committed on the dwelling. The acts of surveillance complained of must not be disproportionate or excessive in the circumstances.*

Defence (e): *The defence of exercise by An Garda Síochána of powers granted by law (including the Heads) for the prevention, detection or prosecution of crime, including the lawful arrest of any person, speaks for itself. It should be understood from this however that subject to the relevant defences and to the regulatory*

provisions in Head 11, An Garda Síochána and State authorities would be subject to the proposed criminal provisions in the Heads.

Defence (f): *Lawful authority under statute: this applies to all proposed offences and to all persons. The other proposed defences are intended to be exhaustive as to lawful non-statutory authority - i.e. no defence based on non-statutory authority should be allowed if it is not within defences (a) to (e) inclusive.*

Defence (g): *Surveillance of one's own premises: this applies to offences (a) and (b). With some hesitation we have come to the conclusion that there should be a defence in respect of criminal liability in the case of a person who engages in surveillance, even involving hearing or optical devices, on or in that person's own premises. We are of the view that in principle a lawful occupier of premises (including but not confined to a dwelling) must be under a considerable degree of liberty as to what he does in the matter of surveillance, even where surveillance devices are used, on his or her own premises. Nonetheless even this liberty should not be without its limits. We propose two such limits: the first, referred to in this defence, is that this defence is subject to the requirements as to notice at public entrances envisaged by Head 11(4) in respect of private premises which are expressly or by implication open to the public, whether on payment of a fee, by invitation or otherwise. The second limit, contained in the defence itself, is that the surveillance even by an occupier of his premises must not involve covert photography or video recording of such a nature as to constitute an intentional and unjustified violation of the intimate and private life of any person on the premises. This last mentioned qualification of the defence would potentially cover a variety of offensive actions by the lawful occupier, such as surreptitious filming of a guest, customer or client in a state of undress.*

Defence (h): *A defence of bona fide ignorance on the part of the defendant charged with offences (c),(d) or (e) of the circumstances in which information the subject matter of the alleged offence was obtained is consistent with our proposal for a similar defence (in Head 3) in the sphere of civil liability for disclosure or publication of information obtained by tortious means, and seems a fortiori to be called for in the sphere of criminal liability.*

Head 11: Regulatory Provisions: Certain forms of surveillance by An Garda Síochána and others

(1) In this Head,

"private place" means any place in private occupation including a dwelling, irrespective of whether or not the place is open to the public, whether on payment of a fee, by invitation or otherwise;

"public place" means any place which is not a private place;

- (2) (a) **Notwithstanding Head 9, surveillance of any private place using any optical or hearing device, whether equipped for the purposes of recording or not and whether fixed or not, and whether such surveillance is overt or covert, without the consent of the occupier or a person having authority to act on his behalf, may be authorised under this paragraph.**
- (b) (i) **Surveillance by a member of An Garda Síochána under this paragraph may be authorised for the prevention or detection of any crime in respect of which a search warrant may be issued to An Garda Síochána or any member thereof under statute, including for the purpose of the lawful arrest or prosecution of any person for such crime, the purpose of general intelligence gathering in relation to any such crime or suspected such crime, or the purpose of obtaining evidence of the kind and in the circumstances in respect of which a search warrant may be granted under Section 14 of the Criminal Assets Bureau Act, 1996.**
- (ii) **A member of An Garda Síochána may apply to an officer of An Garda Síochána not below the rank of Chief Superintendent for a warrant (hereinafter called a surveillance warrant) authorising surveillance under this paragraph and the said officer of An Garda Síochána may grant such surveillance warrant in respect of a particular private place to be named in such warrant for a period of not more than fourteen days from the date of the issue of such surveillance warrant, or refuse such warrant.**
- (iii) **Such a warrant shall not be issued by a Chief Superintendent if at any time within the period of one month prior to its issue there has been in force a surveillance warrant in respect of the same premises under this paragraph.**
- (iv) **A member of An Garda Síochána may apply to a Judge of the District Court for the grant of a surveillance warrant under this paragraph and the Judge may grant or refuse such application. Such an application may be made to a District Judge whether or not there is currently in force a surveillance warrant issued by a Chief Superintendent in respect of the same premises under clause (ii) of this paragraph; where such a warrant is in force, the Judge shall, if he or she decides to accede to the application, grant a fresh surveillance warrant in its place.**
- (v) **A surveillance warrant granted by a Chief Superintendent or a judge of the District Court under this Head shall specify the place of surveillance, identify the person or persons**

(including class of person) who may carry out the surveillance, and specify the mode of surveillance authorised by the warrant; such a surveillance warrant may authorise the member of An Garda Síochána to whom it is granted, accompanied by such other persons as such member considers necessary, to enter private property surveillance of which is authorised by the warrant without the consent of the occupier for the purposes of initiating, maintaining, or withdrawing such surveillance, and may impose conditions in respect of such surveillance. Such a warrant issued by Chief Superintendent shall be expressed to expire fourteen days after the granting thereof. A surveillance warrant granted by a Judge of the District Court shall be expressed to expire on such day as the Judge shall determine being not more than three months from the grant thereof.

(vi) A surveillance warrant granted by a Chief Superintendent may be revoked or varied by decision of the Chief Superintendent who granted it in any respect other than the duration of the warrant, while the warrant is in force.

(vii) - A surveillance warrant granted by a Judge of the District Court under this paragraph may while it is in force be revoked or varied by order of a Judge of the District Court.

- A surveillance warrant granted by a judge of the District Court may from time to time be renewed by order of a Judge of the District Court for any period not exceeding three months.

(viii) A surveillance warrant may not be granted or renewed under this paragraph unless the Chief Superintendent or Judge of the District Court to whom application is made is satisfied that there is substantial reason to believe that the information or material proposed to be sought by means of the surveillance proposed is necessary for a purpose mentioned in clause (i) of this subparagraph and that the surveillance is justified having regard to the likelihood, if any, that the information or material can be obtained, or obtained sufficiently speedily, by lawful means other than such surveillance, to the likely impact of the surveillance on the rights of any person, and to any other relevant circumstances.

(ix) A surveillance warrant shall not be granted under this Head of it appears to the Chief Superintendent or Judge of the District Court to whom application is made to be directed or substantially directed to the surveillance of communications which are protected by privilege.

- (x) An application to a Judge of the District Court for the grant or renewal of a surveillance warrant under this paragraph may be made ex parte and, if so made, shall be heard and determined otherwise than in public.
- (xi) An application to a Judge of the District Court for the revocation or variation of a surveillance warrant under this paragraph may if made by a member of An Garda Síochána be made ex parte and, if so made, shall be heard and determined otherwise than in public.
- (c) A person shall not disclose or use information or material obtained by virtue of surveillance authorised by a surveillance warrant granted under this paragraph except for the purposes of the prevention or detection of crime including the lawful arrest or prosecution of any person in connection with the commission of crime, or for the purposes of carrying into effect the Criminal Assets Bureau Act, 1996, or where its disclosure or use is required for the purposes of compliance with an order of any court. These purposes also include compliance with any international convention, agreement or arrangement to which the State is a party having as its object any of the said purposes.
- (d) A person who discloses or uses such information or material for any purpose not authorised by subparagraph (c) of this paragraph shall be guilty of an offence.
- (3) (a) Subject to paragraph (4) a person shall not, whether overtly or covertly use for the purposes of surveillance of persons, activities, or things in a public place a fixed optical device designed, adapted or suitable for the purposes of filming or otherwise recording such persons, activities or things (including conversations between persons), unless he or she is a member of An Garda Síochána under and in accordance with an authorisation under this paragraph.
- (b) For the purposes of this paragraph a device is fixed if it is installed at a fixed position (including a vehicle, whether moving or not) at or from which it is capable of being used for surveillance, whether by manual operation or by remote control or other means.
- (c) A member of An Garda Síochána not below the rank of Chief Superintendent may grant (or refuse to grant) an authorisation on application by a member of An Garda Síochána for such authorisation under this paragraph and may if he sees fit

grant such authorisation subject to conditions. Such member may also revoke or amend such authorisation. Such an authorisation shall be granted for any period not exceeding three months and may be renewed for any similar period.

- (d) A person may not disclose or use information obtained as a result of surveillance authorised under subparagraph (c) of this paragraph except for the purposes of the prevention or detection of crime in the course of the discharge of the functions or duties of that person, including the lawful arrest or prosecution of any person in connection with the commission of crime, or for the purpose of carrying into effect the Criminal Assets Bureau Act, 1996, or where its disclosure or use is required for the purpose of compliance with an order of any court. These purposes include compliance with any international convention, agreement or arrangement to which the State is a party having as its object any of the said purposes.**
- (e) A person who contravenes subparagraph (a) or (d) of this paragraph shall be guilty of an offence.**
- (4) (a) A person who is not authorised in that behalf under paragraph (2) or paragraph (3) shall not use, for the purposes of surveillance of persons, activities or things in any public place or in any private place which is open to the public whether on payment of a fee, by invitation or otherwise, a fixed optical device designed, adapted or suitable for the purposes of filming or otherwise recording such persons, activities or things save in accordance with this paragraph.**
- (b) Surveillance of a public place may be carried out only by means of a device which is installed and fixed in premises owned or occupied by the person carrying out the surveillance, for the *bona fide* purpose of maintaining the security and protection of such premises, including the security and protection of persons (if any) and things (if any) therein, and provided that, in the case of surveillance of a public place (whether carried out along with surveillance of a private place or not) a notice clearly indicating the fact that such surveillance is being carried out is affixed to such premises at or in the immediate vicinity of the public place or each public place which is subject to such surveillance.**
- (c) In the case of surveillance of a private place to which the public have access, whether on payment of a fee, by invitation or otherwise, such notice shall be given at each entrance to**

such premises which is available for the purpose of such access to the public.

- (d) A person who carries out surveillance in contravention of this paragraph shall be guilty of an offence.
 - (e) A person shall not disclose or use information obtained by means of surveillance authorised under subparagraph (b) or (c) of this paragraph except *bona fide* for the purposes for which, in compliance with subparagraph (b) of this paragraph and any order of the Minister for Justice made under subparagraph (e) of the paragraph, such surveillance has been carried out, or where such disclosure or use is required by an order of any court. A person who contravenes this requirement shall be guilty of an offence.
 - (f) The Minister for Justice may by order lay down additional provisions for giving full effect to subparagraph (b) of this paragraph.
- (5) Without prejudice to any civil liability under these Heads or to any criminal liability under Head 9 or under paragraph (3) or (4) of this Head, a person who obtains information by means of surveillance of a kind mentioned in paragraphs (3) or (4) which has been carried out in breach the said paragraphs (3) or (4) as the case may be shall not disclose or use such information otherwise than by conveying it bona fide for the purposes of the detection or prevention of crime to a member of An Garda Síochána. A person who contravenes this provision shall be guilty of an offence.
- (6) A person carrying out surveillance under and in accordance with the terms of a surveillance warrant issued under paragraph (2), or of an authorisation issued under paragraph(3) or under and in accordance with paragraph (4), or lawfully disclosing or using information or material obtained by means of such surveillance shall have a full defence in respect of all civil or criminal liability as the case may be imposed by or under these Heads.
- (7) Overall judicial review of surveillance by An Garda Síochána to which this Head applies (as under the 1993 Act).

Explanatory Note:

The object of this Head is to secure for members of An Garda Síochána - engaged on behalf of the State in the prevention and detection of crime (which includes the prosecution or lawful arrest of any person for crime and general intelligence-gathering in relation to crime) suitable but nonetheless conditional powers of

surveillance notwithstanding the provisions concerning civil liability in Head 2 and those concerning criminal liability in Heads 9 and 10.

References to "crime" in this Head mean any crime for which under the relevant statutory provision in relation to that crime a search warrant may be obtained.

The provisions of this Head are therefore based on the assumption which follows from the provisions on civil liability and criminal provisions which we recommend that the State and its authorities, no less than private citizens, are subject to the restrictions and liabilities contained in these provisions.

The authorities also of course have the benefit of the defences contained in Head 10, in particular, the lawful exercise by a member of An Garda Síochána of powers granted by law (including the Heads) for the prevention or detection or prosecution of crime, and the existence of lawful authority by or under statute including these Heads.

Paragraph (2) of this Head recommends a special procedure for the authorisation of surveillance by An Garda Síochána of any private place by means of any optical or hearing device, whether used overtly or covertly, without the consent of the occupier or someone acting on his behalf. [Sub-paragraph (a)]. "Private place" means any place in private occupation including a dwelling, irrespective of whether or not the place is open to the public, whether on payment of a fee, by invitation or otherwise. This therefore applies to only some of the various forms of surveillance which would be prohibited under Head 9; prohibited forms of surveillance not covered by this Head 11 are, of course, in any event subject to the relevant defences contained in Head 10 where they are applicable to the facts of the case.

Sub-paragraph (b)(i) of paragraph (2) states the purposes for which the kind of surveillance to which paragraph 2 applies may be authorised by warrant. In short, these are the prevention or detection (including arrest, prosecution and general intelligence-gathering) of any crime in respect of which a search warrant may be obtained under existing legislation, and the obtaining of evidence as contemplated by Section 14 of the Criminal Assets Bureau Act, 1996. This Act primarily concerns the identification, freezing and seizure of assets which are the proceeds of crime, the due taxation of the proceeds of criminal activity and the investigation of social welfare claims by persons engaged in crime.

Under sub-paragraph (b)(iii) of paragraph (2) a surveillance warrant authorising surveillance of the kind envisaged by this paragraph may initially be granted by a Chief Superintendent for a period of not more than fourteen days.

In our recommendations we have proposed that the Garda officer to grant a surveillance warrant should be not less in rank than a Chief Superintendent. In the interests of operational efficiency however it might be thought more desirable to allow a Garda Superintendent to exercise such power. We have no view of principle as to whether the power should be granted to a Garda officer not less than the rank of Superintendent or not less than the rank of Chief Superintendent. We are of the

view, however, that the Garda officer who should have this power should at least be a Superintendent.

Under our proposals as they stand, a Chief Superintendent may not issue a surveillance warrant if there has at any time within the previous month been a surveillance warrant in force in respect of the same premises. (Sub-paragraph (b)(iii)). This provision is intended to remove any doubt or confusion as to what is to happen once the initial fourteen days' authorised surveillance has expired: if surveillance is continued it may only be authorised by a Judge unless there has been a break of at least a month in the authorised surveillance.

Subparagraph (b)(iv) of paragraph (2) introduces the recommended procedure for application to a Judge of the District Court for the grant of a surveillance warrant. This provision makes it clear that notwithstanding the procedure for obtaining a fourteen-day warrant from a Chief Superintendent, the application may be made to a District Judge ab initio: the applying member of An Garda Síochána need not go in the first instance to a Chief Superintendent if he does not wish to do so. Where application is made to a District Justice while a fourteen-day Chief Superintendent's warrant is still in force, the judge granting the application grants a fresh warrant in its place.

Sub-paragraph (b)(v) of paragraph (2) lays down the contents of a surveillance warrant, whether granted by a Chief Superintendent or a Judge of the District Court. Besides the place of surveillance, the person or persons or class of person who may carry it out, and the mode of surveillance authorised, the warrant may authorise the member of An Garda Síochána to whom it is granted, accompanied by such other persons as he or she considers necessary, to enter private property the surveillance of which is authorised by the warrant without the consent of the occupier for the purpose of initiating, maintaining or withdrawing the surveillance and may impose other conditions.

A surveillance warrant granted by a District Judge expires three months from the date of the grant thereof. It may be renewed from time to time for any period not exceeding three months. Any warrant granted under the paragraph may be revoked or varied by decision of the authority which granted it (sub-paragraph (b)(vi) and (vii) of paragraph (2)).

Sub-paragraph (b)(viii) and (ix) of paragraph (2) contain provisions of major importance: they lay down the basic conditions of substance to be satisfied where a surveillance warrant is granted either by a Chief Superintendent or by a Judge of the District Court. In either case the authority granting the warrant must be satisfied that there is substantial reason to believe that the information or material sought by means of the proposed surveillance is necessary for a purpose mentioned in subparagraph (b)(i) (see above) and furthermore that it is justified having regard to the likelihood (if any) that the information can be obtained either quickly enough or at all, by other lawful means, and furthermore, regard must be had in taking the decision to the likely impact of the surveillance on the rights of others and to all other relevant circumstances. This provision is intended to avoid a situation in

which surveillance warrants might be thought to be obtainable for the asking without any examination of substance of the reasons justifying the application. It is furthermore provided in subparagraph (b)(ix) that a warrant is not to be issued where it appears that the application is directed or is substantially directed to the surveillance of communications which are protected by privilege. The privilege which primarily arises here is the legal privilege of certain communications bona fide undertaken between a client and his lawyer (solicitor or barrister).

Sub-paragraphs (c) and (d) of paragraph (2) of this Head address the question of the use which may be made of information obtained by virtue of surveillance authorised by a surveillance warrant granted under paragraph (2). Notwithstanding Head 9(d) and (e) such information or material may be disclosed or used for the purposes of the prevention or detection of crime, the carrying into effect of the Criminal Assets Bureau Act, 1996, or compliance with an order of any court. These purposes also include compliance with any international convention, agreement or arrangement to which the State is a party and having as its object any of the said purposes. Otherwise, it is an offence to disclose or use information or material so obtained.

***Paragraph (3)** of this Head governs a different case: that in which An Garda Síochána uses fixed hearing or optical devices for surveillance of persons' activities or of things in public places. Subject to specific exceptions (paragraph (4)) we envisage that such surveillance may only be carried out by An Garda Síochána.*

The prevention and detection of crime can be assisted to an important extent by means of the surveillance of the public streets in particular by the Gardaí using cameras which are fixed in position and are designed or adapted to function automatically once activated or switched on without the need for continuous human operation or intervention. We include for this purpose such a device installed in a vehicle, whether moving or not.

Surveillance of public places under this paragraph requires authorisation, not from a court, but from a member of An Garda Síochána not below the rank of Chief Superintendent. Such authorisation may be granted subject to conditions. No requirement of public notice in respect of such authorisation is imposed. It is considered that to require such notice would be to risk depriving the surveillance of much of its effectiveness. Authorisations have a "life" of three months but they may be renewed.

In subparagraph (e) of this paragraph provisions concerning the disclosure or use of information or material obtained as a result of surveillance to which it applies, similar to those in paragraph (2) of this Head, are recommended.

***Paragraph (4)** governs certain kind of surveillance by private persons. The provisions of this paragraph lay down additional conditions, in addition to those recommended under the headings of civil and criminal liability in these Heads, for certain kinds of surveillance by private persons. This is surveillance by means of optical devices - in effect, video surveillance, whether accompanied by recording or*

not, where such devices are fixed to private premises and are used either for surveillance of private premises which are open to the public (whether on payment of a fee, by invitation or otherwise) or for surveillance of a public place in the vicinity of the private premises. Such surveillance is very often fully justified by the necessity for the occupier of the premises to protect his own rights in one way or another. However, we have reached the conclusion (which is supported by legislation in several other countries both in Europe and elsewhere) that where the surveillance is of private premises open to the public, notice of the surveillance should be given at each entrance to the premises which is so open to the public. Where the surveillance involves or includes surveillance of any public place there should be affixed to the premises a notice, visible to the public, of the fact that the public place is subject to such surveillance.

However, as legislation of this kind may be applicable to a wide variety of different situations which may not be foreseeable in advance, we propose (subparagraph (f) of paragraph (4)) that the Minister for Justice should have power by order to lay down supplementary rules to give effect to the proposals contained in paragraph (4). We also propose in sub-paragraph (d) provisions similar to those above concerning the disclosure or use of information obtained by private persons by means of such surveillance. A person who misused such information would, we propose, be guilty of an offence.

Paragraph (5) *addresses the question of the disclosure or use, by a person who has obtained information in contravention of paragraphs (3) or (4), of such information. Such information may only be conveyed to An Garda Síochána bona fide for the purposes of the prevention or detection of crime. Any other criminal or civil liability remains unaffected.*

These provisions are backed up by provisions for the creation of supplementary offences, where appropriate, of surveillance and of disclosure (paragraphs (2)(d), (3)(e), (4)(d), 4(e) and (5)).

Paragraph (6): *As a logical consequence of these provisions, we recommend that persons carrying out surveillance, or disclosing or using material or information obtained thereby, under and in accordance with the regulatory provisions (including any warrant or authorisation granted thereunder and any relevant ministerial order) should have a full defence in respect of all civil and criminal liability under the Heads.*

Paragraph (7): *Lastly, and in line with section 8 of the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993, we propose that there should be provision for overall judicial review of all forms of State surveillance covered by our proposed Heads. Such review would involve the following elements in line with the provisions of the 1993 Act:*

(a) A High Court Judge being designated to undertake (while serving as a Judge) the review duties envisaged in the Section, mutatis mutandis;

(b) the Judge in question having the duty of keeping the operation of State surveillance under review and of reporting (to the Taoiseach or the Minister for Justice as the case might be) at specified intervals in relation to the results of his review;

(c) the designated Judge having powers of investigation, access to and inspection of official documents relating to authorisations;

(d) all persons concerned in or having information relevant to surveillance warrants or authorisations or surveillance carried out thereunder being obliged to give the designated Judge such information as was in their possession relating thereto;

(e) the designated Judge having power where he thought fit to direct that a particular warrant or authorisation should not have been given and should be cancelled.

Head 12: Hearing of proceedings otherwise than in public and related matters

- (1) This Head is without prejudice to any power of any court under statute or otherwise in any civil or criminal proceedings to order that proceedings shall be heard otherwise than in public or providing for the anonymity of any person before the court or prohibiting the publication or broadcasting of information likely to lead members of the public to identify any person.**

- (2) Provide that at any stage of any civil proceedings in tort under these Heads or criminal prosecution under these Heads the court may on the application of any person who claims that his or her rights under these Heads have been or are about to be infringed, where the court considers it necessary for the purpose of either preventing such infringement or of protecting the rights of privacy of such person from the consequences of such infringement, and in light of all the circumstances including particularly the public interest in the administration of justice in public, make all or any of the following orders:-**
 - (a) an order that the proceedings or any part of the proceedings including any interlocutory application should be heard otherwise than in public;**

 - (b) an order that members of the public (excluding the parties to the proceedings and *bona fide* members of the press) should be excluded from attendance at the hearing;**

 - (c) an order providing for the anonymity of any person in connection with the proceedings;**

- (d) an order providing for the prohibition of the publication or broadcasting of matter likely to lead members of the public to identify any particular person in connection with the proceedings.

EXPLANATORY NOTE:

The purpose of this Head is to be distinguished from the purpose of Head 5 above which concerns privacy orders. A privacy order is one which restrains the commission of a tort contrary to these Heads, either by way of interlocutory or final order of the court. By contrast, the purpose of the present Head is to give the court jurisdiction, where this is necessary to protect the privacy rights of parties in a civil suit or persons (such as the complainant or other witnesses) involved in a criminal prosecution, to require that, in whole or in part, the proceedings should not be held in public, to exclude certain persons from the court, or to make orders protecting the anonymity of persons from outside reporting or disclosure or from publication or broadcasting of material likely to lead to the identification to the public of particular persons concerned.

These powers would be without prejudice to any powers of a similar nature vested in the court. The particular powers contained in the various paragraphs of this Head are drawn from various statutes. There are in fact numerous statutes that provide either for the holding of court hearings in camera or for restrictions on the publication of matter, including the names of one or more parties, arising from court proceedings.

For an elaboration of the justification for these provisions and a selection of relevant existing statutory sources, in the privacy context, see Annex IV to our Report.

Head 13: Amendments of Postal and Telecommunications Legislation

Technical amendments of the Postal and Telecommunications Services Act, 1983, and the Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.

See Recommendations 16 to 18 of our Consultation Paper on Privacy.

Head 14: Saver

These Heads are without prejudice to the constitutional rights of any person concerned.

EXPLANATORY NOTE:

Given the existence and likely further development of constitutional jurisprudence in the area of privacy it is necessary to safeguard the provisions of the proposed legislation from any accidental constitutional infirmity which is not foreseen at present by making provision that, in effect, where the constitutional rights of any person concerned so require, they take precedence over the legislation. In effect what this means is not only that the provisions of the legislation to be construed in accordance with the Constitution (which is already an existing constitutional rule for the construction of Acts of the Oireachtas) but also that were the necessity to arise, the express provisions of the legislation would be disappplied in favour of the Constitution.

Head 15: Penalties

Provide for penalties for criminal offences under Head 9 and Head 11.

SCHEDULE

List of acts referred to in paragraph (a)(i) of the Proviso to Head 3

(i) **Interception of the post or unlawful interception or monitoring of electronic communication contrary to the *Interception of Postal Packets and Telecommunications Messages (Regulation) Act, 1993.***

(ii) **Obtaining data by means of an act constituting illegal surveillance under Head 2 which act also constitutes a contravention of the *Data Protection Act, 1988.***

(iii) **Unlawfully accessing data by means of the operation of a computer contrary to Section 5, *Criminal Damage Act, 1991.***

(iv) **The infringement of Head 9(1)(a), (b) or (c) of these Heads.**

ANNEX I

THE RELATIONSHIP BETWEEN ARTICLES 8 AND 10 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS

1. Introduction

Part 1 - Article 8

2. Article 8

- i. The Basis and Ambit of "Private Life" under Article 8(1).
- ii. Factors that May Affect the Degree of "Reasonable Expectation" of Privacy.
- iii. Do States Parties have any Positive Obligations under Article 8 with respect to Regulating Private Behaviour?
- iv. The Adequacy of Existing Remedies as a Factor.
- v. The Existence of a Fair Balance between the General Interest and the Individual Interest as a Factor.
- vi. Does the Obligation to Take Positive Action Require or Allow for Legislation?
- vii. The Question Whether Covert Police Surveillance Using Electronic Means Requires a Basis in Positive Law and Related Matters.

Part 2 - Article 10

3. Article 10

- i. Is Freedom of Expression Intrinsicly Hostile to Privacy Legislation?
- ii. Does the "Public Interest" Defence Adequately Reconcile Privacy with Freedom of Expression?
- iii. Does the Latitude allowed for "Political Speech" have any Implications for the News-Gathering Process?
- iv. Are Prior Restraints on Expression Inherently Violative of Article 10?

1. Introduction

1.1 In this Chapter we highlight some of the more salient features of human rights law as it bears on the issues raised in this Report. Our Consultation Paper ranged quite broadly over a variety of international human rights instruments to which Ireland is a party including the European Convention on Human Rights (ECHR) and should be consulted for background material.

1.2 Here we focus more closely on certain aspects of the European Convention. We do so not merely to establish a clear legal basis for our recommendations but also in order to deal with some of the more important reservations made in written submissions and at the "listening exercise" concerning the compatibility of our provisional recommendations with the Convention. We also felt it necessary to deal more fully with certain matters that seemed important to us under the Convention and in the context of this Report. Since the reservations expressed in some submissions would go as much, if not more, to our final recommendations as they did to our provisional recommendations it is important that they are resolved satisfactorily.

1.3 This Chapter should be read in light of Chapter 3 outlining the inadequacy of domestic law and Chapter 4 which puts forward the positive case for a legislative response.

1.4 It is to be recalled that our core recommendation is for the enactment of a civil tort dealing with privacy-invasive surveillance and harassment as well as publication of any material that results from such actions. We also make recommendations with respect to the enactment of new criminal offences and other regulatory matters. Nothing in our recommendations precludes the establishment of self-regulating bodies dealing for example with the private investigators industry or the press. Indeed, such developments are to be encouraged since many strategies - not just legal ones - seem required to ensure "respect" for private life in the round.

1.5 Two core human rights under the Convention are implicated. The first is the right to privacy, or, more accurately, the right to respect for "private life", which is protected under Article 8 of the Convention. Our primary focus in addressing Article 8 is on how to enhance the protection of privacy; it should be borne in mind that this approach is somewhat unusual in that the normal form of analysis looks to the various legitimate restrictions on privacy and on the power of the Contracting States to impose such limitations. We identify five key issues concerning Article 8 arising from submissions and otherwise.

- First, there is the question concerning the breadth of the notion of "private life" and whether, for example, it has the potential to extend beyond the

territorial confines of the "home" and extend into public places. This is an important point for us since we are of the view that privacy is personal to the individual and not premised on, or bounded exclusively by, territorial considerations.

- Secondly, and related to the first question, the question arises how to identify the factors that may affect the degree of legitimate or reasonable expectation of privacy under Article 8. This is important since, if it is conceded that privacy follows the person, then some indication of these factors is necessary.
- Thirdly, there is the question whether Article 8 imposes on States positive obligations with respect to violations of privacy perpetrated by private parties.
- Fourthly, there is the question whether the obligation on States to "respect" privacy under Article 8(1) requires, implies or at least permits States to introduce legislation governing violations of privacy as between private parties. This is an important question since the enactment of such legislation (as least as it affects surveillance) forms our core recommendation. Obviously a principled and practical balance will have to be struck between all relevant competing rights including, in particular, freedom of expression.
- Fifthly, there is the question whether *covert* police surveillance (or such surveillance carried out by other state agencies) must have some basis in law and, if so, what kinds of safeguards are necessary.

1.6 Leaving aside altogether any consideration of Article 13 (right to an effective remedy) which was amply covered in our Consultation Paper, our general view on Article 8 is that it is at least permissive toward the kind of legislation we propose. We are of the view that an appropriate balance should be, and can be, struck between the people's right to know certain information and an individual's right to privacy and self-determination. We are also of the view that Article 8 requires, at the very least, the existence of some basis in positive law for covert police surveillance.

1.7 The second right implicated is freedom of expression which is protected by Article 10. It is relevant for the purposes of this Report at the secondary level of intrusion when publication occurs by means of, or as a result of, a prior invasion of privacy through surveillance. Article 10 has been used by the European Court to create space for the press to perform its "watchdog" role in democracy on political matters or other matters of public concern.

1.8 We identify four key questions under Article 10 arising from submissions and otherwise for our purposes.

- First, is freedom of expression an insurmountable barrier to the kind of legislation we recommend? The answer to this question is nuanced and not straightforward.
- Secondly, does our recommendation with respect to the "public interest" defence which we now propose adequately square the people's right to know with the person's right to respect for his/her privacy under Article 10?
- Thirdly, does an enhanced latitude to publish necessarily entail an enhanced latitude to gather information and news? If so, does this enhanced latitude to gather information operate to carve out implicit exceptions to either the extant positive law or to warrant or justify the insertion of relevant exceptions or relaxations into the new legislation which we now recommend? This is important since it goes to whether the media are to be held accountable to the same law in the same way as everyone else for their information gathering acts.
- Fourthly, are prior restraints inherently violative of Article 10? If so, our recommendation with respect to privacy orders cannot stand. If not, then under which conditions can a prior restraint stand and do our recommendations with respect to "privacy orders" meet these conditions?

1.9 Our general view on Article 10 is that the European Convention is at least permissive toward the kind of privacy legislation we recommend with respect to surveillance. Article 10 does not, we consider, place an obstacle in the way of such legislation but rather affects the way in which it should be drafted. We are of the view that the "public interest" defence and other defences which we now propose provide ample reconciliation of the essential interests served by both privacy and freedom of expression. Such a law would, we consider, respond appropriately and proportionately to a pressing social problem. Moreover, it is to be noted that, no matter how cogent, the Article 10 arguments go only to the question of intrusion on privacy at the secondary level (i.e. publication) and are not dispositive as to whether a privacy law governing particular *acts* of surveillance is permitted or even required under Article 8 which is in fact our core focus.

1.10 What follows is an assessment of the above issues under Articles 8 and 10 respectively. Two caveats require to be made. The first is that the case law under Article 8 and dealing especially with the interface between Articles 8 and 10 is not extensive. Secondly, the judgments are very much driven by the facts of individual cases. Due to their role as the providers of outer supervision the Commission and Court look more to the law in action than to the law in abstract terms. Nevertheless,

we believe that there is enough in the case law to support the broad outlines of our findings below.

Part 1 - Article 8

2. Article 8

1.11 The structure of Article 8 is twofold; first the right is announced and then limiting principles are provided. Article 8 reads as follows:

1. Everyone has the right to respect for his private and family life, his home and 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.

1.12 The general issues that arise under Article 8(1) concern the scope of the four protected interests (including "private life") and the nature of state obligations (whether negative or positive). The general issues that arise under Article 8(2) concern whether there has been an "interference" with the right, whether the interference was in "accordance with the law", whether it was for one or more of the legitimate aims listed and whether it was "necessary in a democratic society". These issues were addressed in general terms in our Consultation Paper.

1.13 In this section we shall focus more particularly on the five issues indicated in para. 1.5 above that go more directly to the recommendations of this Report.

(i) *The Basis and Ambit of "Private Life" under Article 8(1)*

1.14 Can "private life" as the term is used in Article 8 extend beyond the physical confines of a domicile or is it territorially bound? Can "private life" inhere in relationships formed by the person or is it confined to the person in his/her isolation? This depends on what are considered to be the basic values behind "private life" and whether the Convention organs read "private life" expansively in light of these values.

1.15 On its face, Article 8(1) has four denotations -

- private (and)
- family life

- home (and)
- correspondence.

1.16 The net question posed in this section is: What is meant by "private life" under Article 8(1)? It is clear that the term "private life" is treated as a term of art by the Commission and Court. While it is admittedly hard to discern a fully coherent conception of "private life" from the jurisprudence of the Commission and Court, it is nevertheless possible to highlight some of the more salient points to have emerged in the case law. Here we look at the provenance and ambit of "private life" under Article 8. In the next section we deal with the related question of the outer boundaries of "private life" and whether there are any clear criteria to indicate when a reasonable expectation of privacy arises and when it is lost (e.g., walking in a public place).

1.17 The European Court has eschewed the elaboration of a unified or unifying theory of "private life". Instead it has kept both the connotation and the denotation of the term fairly open. It has referred quite often in its case law on 'private life' to the notion of the human personality and to the need to keep space open for the expression of the human personality. This concept, long familiar in German constitutional law, can now be considered one of the anchor points of Article 8.¹ In an early case involving an Icelandic law that forbade the keeping of dogs except for agricultural purposes the Commission signalled a broad understanding of private life. It stated:

"For numerous Anglo-Saxon and French authorities the right to respect for 'private life' is the right to privacy, the right to live, as far as one wishes, protected from publicity...In the opinion of the Commission, however, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and to develop relationships with other human beings, especially in the emotional field, for the development and fulfillment of one's own personality²."

1.18 Unsurprisingly the keeping of dogs, though important, was held not to be vital to the development of the human personality and thus no 'interference' arose under Article 8.1. which called for justification under Article 8.2.

1.19 The Commission has also stated

1 See generally L.G. Loucaides, *Personality and Privacy under the European Convention on Human Rights*, (1990) B.Y.I.L. 175.

2 Application No. 6825/74 5 DR 86 at p. 87.

"The right to respect for private life is of such a scope as to *secure to the individual a sphere within which he can freely pursue the development and fulfillment of his personality.*"³

1.20 The language used by the Commission in the above passage is revealing. First, it supports the notion of a 'personal sphere' within which the human personality can be developed. That is significant because it indicates the existence of such a sphere in a way that is not directly connected to property and because it ties this space to normative ideas about personhood. Such a 'personal sphere' was subsequently found by the Commission to subsist even in (perhaps especially in) a prison environment⁴. Secondly, the related obligation on the part of States to *secure* that space is also significant.

1.21 This flexibility allows the European Court to develop and broaden its understanding of "private life" as social mores change and as new threats are posed. Thus the Court stated in *Niemitz v. Germany*⁵ that

"29. The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.

There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.⁶

1.22 It is therefore clear that, whatever else it is, "private life" extends beyond protecting the person in his/her isolation from others and encompasses a personal space within which to develop human relationships⁷. This idea of linking "private

3 Application No. 6959/75, 10 DR 100 at para. 55 [emphasis added].

4 *McCreeley v. U.K.*, 20 DR 44 at para 82.

5 (1993) 18 EHRR 97.

6 *ibid.* at 111.

7 One applicant has argued before the Commission that "the heart of the [private life] concept is that the individual should have the opportunity to establish and develop relationships with other human beings, an opportunity which is essential for the development of the personality": *Boffa v Italy* No. 21439/93, Decision on admissibility, 15 January 1998, 84B DR 34 at 45.

life" to human relationships was underlined by the Commission in *McFeeley v. UK*⁸. Thus the formation and development of human relationships, including, it seems, business relationships is considered to be within the term "private life". Private life is therefore interpreted purposively. Its ambit will depend, in part at least, on the purpose which it serves and the value to be placed on that purpose. This represents in a way, a move from a static conception of "privacy" to a more active and rounded conception of a "private life" and illustrates the fact that people require more than islands of protected calm in which to choose their own ends but also some space in which to pursue those ends and express themselves in common purpose with others.

1.23 In a parallel move and in the same case - *Niemitz* - the Court also extended its interpretation of the word "home". It stated

"30. As regards the word "home", appearing in the English text of Article 8, the Court observes that in certain Contracting States, notably Germany, it has been accepted as extending to business premises. Such an interpretation is, moreover, fully consonant with the French text, since the word "*domicile*" has a broader connotation than the word "home" and may extend, for example, to a professional person's office."⁹

1.24 Accordingly, to search a lawyer's office may amount to an "interference" with private life (including his home or his correspondence)¹⁰.

1.25 The purposive interpretation of the meaning of the word "home" fits in with the Court's overall approach to "private life". The home is protected not merely for its own sake but also because it advances certain broader human or personal goals including the development of relationships as an aspect of private life. In a sense the home is the shell within which such goals are normally pursued and advanced but the goals can transcend the shell and can be pursued outside it. Article 8 can therefore be pressed into the service of these broader privacy goals by either stretching the notion of "private life" to embrace intimate relationships or by stretching the notion of the "home" to embrace some activities that occur outside its strictly territorial or domiciliary bounds. As seen above, the European Court used both stratagems to good effect in *Niemitz*.

1.26 It is perhaps fair to say that, the less intimate the relationship, the less protection it attracts as an aspect of "private life" under Article 8. Indeed, the Court itself added in *Niemitz* that extending the scope of the terms "private life" and "home life"

8 No. 8317/78, 20 DR 44 (1980).

9 (1993) 16 EHRR 97 at 112.

10 See, e.g., *Botka v Austria*, No. 15882/89, 74 DR 48 at 58.

"...would not unduly hamper the Contracting States, for they would retain their entitlement to "interfere" to the extent permitted by Article 8(2); *that entitlement might well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case.*"¹¹

1.27 The Court has also used a purposive approach to interpret "private life" as encompassing and, to a certain extent, protecting the "physical and moral integrity of the person": *X & Y v. The Netherlands*¹². This view was recently reiterated in the judgment of the European Court in *Costello Roberts v. United Kingdom*¹³. This approach, which links physical integrity with private life makes considerable sense since both are crucial to maintaining an un-coerced space for the person. Physical integrity is, of course, already protected by Articles 2 (right to life) and 3 (freedom from torture, etc.). There is then an overlap of sorts between the zones protected by Article 8 and these other Articles. The European Court has stated in *Costello-Roberts* that "the protection afforded by Article 8 to an individual's physical integrity could be wider than that contemplated by Article 3"¹⁴. It must, however, be borne in mind that not all violations of physical integrity will amount to a violation of "private life".

1.28 An interesting if atypical case where an assault on physical integrity was taken to amount to an "interference" with "private life" (as well as to other overlapping interests protected under Article 8) was *Lopez Ostra v. Spain*¹⁵. In that case the applicant showed that a failure on the part of the state to control pollution emanating from private sources amounted to an "interference" with "private life". The *gravamen* of the claim was the alleged failure on the part of the state to control *physical* harm emanating from private sources, a harm that intruded on "private life". Noise pollution was also dealt with by the Commission as a potential interference with private life¹⁶. An arrest, as such, may affect physical integrity and therefore the private life of an individual¹⁷.

1.29 Parenthetically, the protection of "physical integrity" through the notion of "private life" would seem to provide a potentially strong basis for legislation dealing with harassment particularly where it accompanies physical harm (or the apprehension of physical harm) and is directly tied to invasions of privacy. Indeed

11 (1993) 16 EHRR 97 at para 31 [emphasis added].

12 (1985) 8 EHRR 235.

13 (1995) 19 EHRR 112.

14 *Ibid.* at para 34.

15 (1995) 20 EHRR 277.

16 *S. v. France* No. 13728/88 65 DR 250 at 263, Decision on admissibility, 17 May, 1990.

17 See e.g., *Chrysostomos v. Turkey* No. 15299/89 and 15300/89, 86A DR 4 at 32.

the Commission explicitly found on the facts of *Whiteside v. UK*¹⁸ that the harassment in that case (perpetrated by the ex-lover and father of two of the applicant's five children) was at a level that could arguably constitute an interference with private life (as well as with the enjoyment of the applicant's home)¹⁹.

1.30 The related notion of the "moral integrity" of the person as a basis for private life has yet to be fully explored by the European Court but seems fairly well settled under Article 8 caselaw. One commentator, Professor Feldman, draws a link between respect for "moral integrity" and pervasive surveillance²⁰ and opines that a failure on the part of the state to prevent or regulate the latter might be seen as a failure to "respect" private life. In this vein he writes that

"Watching people against their will...forces them to see themselves and their plans through the eyes of another, as object rather than subject, undermining their self-respect and evincing a lack of respect for their freedom to make choices without pressure from the outside."²¹

1.31 The influence of German law is, to a certain extent, apparent in this strand of the caselaw. Under German constitutional jurisprudence the term "moral integrity" is considered to flow from the protection of human dignity. From that reasoning the right to privacy sweeps beyond the familiar right to be left alone and encompasses the need to allow space (and a measure of protection) for personal development and for freedom of decision-making and action²².

1.32 The notion of "moral integrity" would also appear to support the enactment of legislation prohibiting harassment since harassment intrudes on the inner peace or ease of a person which is so necessary to enable persons to function normally. This would appear so quite apart from whether such harassment was accompanied by physical intimidation or harm or led to apprehension of harm or actual harm.

18 No. 20357/92, 76A DR 80 (1994).

19 *Ibid.* at 86.

20 D Feldman, *The Developing Scope of Article 8 of the European Convention on Human Rights*, [1997] EHRLR 265 at 270.

21 D Feldman, *Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty*, 47 *Current Legal Problems* (1994) 41 at 62.

22 See, for example, ruling by the Federal German Constitutional Court (BVerfG), *Neue Juristische Wochenschrift* (NJW) 1973, 1221; see also Feldman, *The Developing Scope of Article 8 of the European Convention on Human Rights*, [1997] EHRLR 265.

(ii) *Factors that May Affect the Degree of "Reasonable Expectation" of Privacy*

1.33 If "private life" can be uncoupled from territorial shackles then does it hold constant or does it vary in response to a multitude of external factors? If so, which factors help determine the level of reasonable expectation of privacy in any given case? This goes to whether an "interference" exists warranting a justification. It does not of course prejudge the existence or effect of a justification under Article 8(2).

1.34 Here we explore factors that may affect one's legitimate expectation of privacy arising from the case law under Article 8. Where no expectation - or a reduced expectation - is found the Commission/Court will find no "interference" and thus no need to move on to consider a justification for such interference under Article 8(2).

1.35 It may be, as some eminent commentators point out, that the Court is working toward some conception of personal space under the rubric of "private life"²³. At least that is one way of making sense of judgments that extend private and home life to encompass relationships, to cover physical locations that are not, strictly speaking within the home and to treat some aspects of physical harm as an interference with private life. As Harris *et al* point out:

"the expansion of the idea of private life to include the making and enjoyment of personal relations means that the idea of private space need not be confined to those areas in which the person has some exclusive rights of occupancy where secrecy or confidentiality can be maintained."²⁴

1.36 The authors go on to ponder whether "private life" would extend beyond personal territory to include semi-public places such as churches or restaurants. They state that

"Clear guidance on this question, and on the further question whether 'private life' extends to what a person does in public places, is lacking in the Strasbourg jurisprudence."

Nevertheless they tentatively conclude that

the expanding notion of private life set out in the *Niemitz* case indicates that a formal public/private division about the *nature of the location will not always be decisive*²⁵."

23 DJ Harris, M O'Boyle, C Warbrick, *Law of the European Convention on Human Rights* (Butterworths, 1995), pp308-309.

24 *Ibid.* at 309.

25 *Id* [emphasis added].

1.37 In other words, and in the view of the eminent authors, it is open to the Court to hold that the *locus* of the violation is not in itself dispositive as to whether the Article 8 protection of "private life" applies. The public or private nature of the locus is arguably one factor (albeit an important one) among many in determining a legitimate expectation of privacy.

1.38 If intrusion has been effectuated in a physical sense and touches on private life in a territorial sense then it appears that little hesitation will be felt in categorising such activity as an "interference": *Murray v. United Kingdom*²⁶. Conversely, it seems that participation in a high profile *event* taking place in a public place will take away from an expectation of privacy. The leading case on this point is *Friedl v. Austria*²⁷.

1.39 In *Friedl* the applicant was videotaped and photographed by the police while participating in a political demonstration against homelessness in Vienna. In order to determine whether an "interference" occurred the Commission had to decide first whether it was appropriate to hold that Friedl had a "private life" interest to protect in the circumstances of the case. One of the reasons why the Commission felt that the videotaping did not amount to an "interference" on his right to private life was because it was connected to an event that occurred in a public place. The event was, by definition, public. The Commission also took into account the fact that the intrusion did not reach Friedl's "inner circle" and that the authorities did not make any effort to identify the participants nor to store the information for later use.

1.40 What, however, of persons who appear in a public place but who do not participate in a public event? It would seem to overstate the Commission's decision in *Friedl* to assert that it completely forecloses the possibility that privacy or "private life" can subsist in public places.

1.41 First of all, most people would recognise that there is a qualitative difference between the various categories of *events* that are fated to take place in public but which may, nevertheless, attract varying degrees of privacy. There is, for example, a qualitative difference between attending a funeral in a place to which the public has a right of access and taking part in a public demonstration for a political or social cause.

1.42 Secondly, it is to be noted that Friedl voluntarily chose to participate in an event or demonstration which was, *perforce*, squarely in the public eye. There is arguably a world of difference between taking part in such demonstrations where the

26 Judgment of the Court, (1995) 19 EHRR 193.

27 (1996) 21 EHRR 83. See generally SH Naismith, *Photographs, Privacy and Freedom of Expression*, [1996] EHRLR 150 at 151.

whole purpose of the exercise is to draw attention to oneself and simply walking down a public street and minding one's own business.

1.43 Furthermore, the decision in *Friedl* hints that if the obvious or planned purpose for the intrusion was to collect and somehow process or disseminate information of a private nature then a qualitatively new element is added that may push the activity past the threshold. *Friedl* itself was settled before the Court on the basis that the photographs would be destroyed and compensation paid. Of course, *Friedl* spoke only to state "interference" but it could certainly be argued by analogy that States have positive obligations with respect to private violations (see section (iii) below).

1.44 One case involving the surveillance of a person in a public place unconnected with a public event arose before the Commission but was declared inadmissible for failure to exhaust domestic remedies²⁸. The applicant was in the process of suing a local authority for alleged personal injuries. The local authority hired a private investigator who proceeded to take photographs of her shopping and in her own home which tended to show that no injuries were manifest. The photographs were not in fact used in the relevant civil proceedings. She complained of a breach of "private life" to the Commission nonetheless. One commentator, Naismith, speculates that if the decision were declared admissible, then

"if the photographs disclose only that which anyone could have seen in public, application of the Commission's invasion of privacy criterion would seem to lead to the conclusion that no interference had taken place."²⁹

1.45 Naismith does concede that obtrusive or persistent surveillance verging on harassment might be sufficient to constitute an "interference"³⁰.

1.46 It does seem plausible to deduce, as Naismith suggests, that no "interference" will be found where people are merely observed casually as part of the ordinary and natural incidences of everyday living. But the real question then becomes whether exposure to covert surveillance in public places (or the deliberate targeting of people in public places) is considered a "normal" incident of everyday life. On the one hand, it can be argued that if one can be casually observed by strangers in public places then one can have no objection to a recording of that observation. However, it would appear to be entirely open to the Convention organs to draw a distinction between mere casual observation (unaided by technology) - which one takes for granted and is constrained to tolerate in society - and the

28 *EN v. Ireland* No. 18670/91, Decision of December 1, 1993.

29 SH Naismith, *Photographs, Privacy and Freedom of Expression*, [1996] EHRLR 150 at 153.

30 *Ibid.* at 152.

deliberate targeting of an individual using sophisticated sensory-enhancing technology in a public place. It might, in other words, be asserted that one's legitimate exposure to intrusion is limited to casual observation and incidental recording.

1.47 In one case the Court has effectively found a reduced expectation of privacy in circumstances where individuals are engaged in a criminal course of action which is inherently likely to attract the attention of the police: *Ludi v. Switzerland*³¹. In *Ludi* the German police informed the Swiss police about the suspected drug dealing of the applicant who had by then absconded from Germany to Switzerland. As a result Ludi was subjected to telephone tapping as well as undercover police operations. The undercover operation took the form of a plain clothes police officer who befriended Ludi. After gaining the confidence of Ludi at successive meetings the plain clothes officer was offered illegal drugs for sale. Ludi was subsequently convicted on drugs charges before the Swiss courts. The evidence of the undercover police officer was not in fact used at trial. Nevertheless, Ludi argued that the telephone tapping and the use of an undercover police officer violated Article 8.

1.48 The Court had no difficulty holding for Switzerland on the issue of telephone tapping since Swiss legislation was perfectly compatible with established case law under Article 8 and was not deviated from in its operation in the instant case. Importantly, the Court did not view the activities of the undercover agent (either alone or in combination with telephone tapping) as affecting "private life". The applicant, said the Court, must have been aware - *at least from the moment he handed over the drugs* - that he was engaged in criminal activity (drug dealing) and was therefore "running the risk of encountering an undercover police officer whose task would be in fact to expose him"³².

1.49 The defining task of the police is precisely to apprehend criminals; the Court's decision suggests that would-be criminals cannot be heard complain on the grounds of privacy if caught in the act. This, however, is not the same as saying that all persons suspected of criminal activity have no residual or reasonable expectation of privacy. Nor is it to say that general intelligence gathering with only a tangential connection to the detection of crime does not tread on a reasonable expectation of privacy. Nor indeed is it to say that electronic surveillance as distinct from normal police activities poses no threat to privacy, especially when one considers the

31 Judgment of the Court, (1992) 15 EHRR 173.

32 *Ibid.* at para 40.

collateral threat such surveillance poses to innocent third parties who happen to visit for *bona fide* purposes business premises or homes³³ which are under suspicion.

1.50 Significantly, state responsibility is also engaged for indirect attacks on rights:

"the Commission considers that Article 8 para. 1 of the Convention... cannot be interpreted so as to apply only with regard to direct measures taken by the authorities against the privacy and/or home of an individual. It may also cover indirect intrusions which are unavoidable consequences of measures not at all directed against private individuals."³⁴

1.51 Thus, surveillance that is targeted by the police on one individual or on one location but which nevertheless has collateral implications for other persons triggers state responsibility. Of course, to say a reasonable expectation of privacy arises is one thing; to provide a justification for "interferences" is quite another and will doubtless subsist in the majority of police operations.

1.52 There are, of course, risks of exposure inherent in all aspects of social intercourse (including risks attaching to the *means* of communication such as telephones) to which one may be assumed to consent. All artificial media of communication carry, in varying degrees, a risk of exposure. It would appear to be wrong, however, to simply assume that the use of any artificial medium automatically entails the loss of privacy. This easy assumption is forcefully challenged by Professor Feldman who writes:

"To hold that one loses privacy rights when using a telephone is analogous to saying that one loses rights of property in respect of one's baggage when one takes it on an airplane, because we all know that bags are sometimes lost or stolen in transit."³⁵

1.53 But a loss in reasonable expectations of privacy will occur when the level of exposure reaches the point where the means of communication themselves can more properly be described as public rather than private. Thus, the Commission held, for example, that the interception of a telephone conversation in circumstances where

33 The European Commission has had occasion to consider the impact on innocent third parties of surveillance of homes. Were the issue to be addressed by the Court, it is submitted that even if justification existed for the surveillance *per se*, this would not extend to all aspects of the recording of an innocent third party. While such recording may be acceptable as an unavoidable consequence of surveillance, its retention would call for close scrutiny. The danger arises that innocent third parties may be drawn into the net provided by the original (justifiable) surveillance.

34 *S v France* No. 13728/88, 65 DR 250 at 263. Decision on admissibility, 17 May 1990.

35 D Feldman, *Privacy as a Civil Liberty*, 47 *Current Legal Problems* (1994) 41 at 67.

the technology used was easily accessible to many persons did not amount to an "interference": *BC v. Switzerland*³⁶.

1.54 More recently the Court has begun to use the more nuanced language of "reasonable expectation of privacy" to find a right of privacy in the use of an office telephone: *Halford v. UK*³⁷. In that case the Court found a general "reasonable expectation of privacy" to exist in making calls from an office telephone. It found its conclusion fortified in this case by reference to a number of factors including the fact that Ms Halford had the sole use of her office and a particular phone was dedicated to her private use.

1.55 It therefore seems fair to say that if a suitable case were to arise (and surmount the admissibility hurdle) then it is certainly conceivable that the Commission might start making distinctions between, on the one hand, casual observation of the type one is constrained to tolerate as part of the price of living in civil society and the deliberate targeting of individuals through covert surveillance on the other. That approach would be consistent with the Court's view that private life is personal to the individual and creates a space that is independent of physical territory. This is, of course, without prejudice to the justifiability of such "interferences" under Article 8(2).

1.56 Perhaps the factor that might tip the scales in favour of a finding of an "interference" would be the purpose, or likely use (or perhaps even the actual use) of the information, photographs or material obtained. The focus here is not so much on the manner of obtaining the information (e.g., whether it was obtained in a public place or otherwise and the means used) but the use to which the resulting information is to be, or is, put. In support of this view it might be emphasised that the steady widening of the term "private life" has already allowed the Commission and Court to consider the information gathering activities of various parties³⁸. It has already been established by the Commission and Court that the taking of photographs and fingerprints by the police will amount to an "interference" with private life requiring justification³⁹ as will the collection and maintenance of medical records⁴⁰. Again, that is not to say that such activities cannot be justified under Article 8(2).

1.57 With respect to photographs the Commission has

36 No. 21353/93, partial decision of 27 February, 1995, 80A DR 101 at 105.

37 Judgment of the Court, (1997) 24 EHRR 523.

38 See, e.g., *Acmanne v. Belgium* No. 10435/83 40 DR 251 (1984) (x-ray tests); *Peters v. Netherlands* No. 21132/93 77A DR 75 (1994) (urine tests).

39 *Murray v. UK* (1995) 19 EHRR 193 and *McVeigh v. UK* No. 8022/77, 25 DR 15 at 49 (1981).

40 *Chave née Jullien v. France* No. 14461/88, 71 DR 141 at 155 (1991).

"taken into account the fact that the use made of them was legitimate and limited, and has placed particular emphasis on whether the photographs were made available to the general public."⁴¹

1.58 Where the information gathering activities are closely connected with a legitimate purpose such as the prevention or detection of crime then, as Naismith points out,

"the use by the authorities of photographs which were validly obtained...will normally fall outside the scope of private life altogether and there will consequently be no interference with the right to respect for private life."⁴²

1.59 This would be all the more so where the controls on the flow or dissemination of the information to third parties was sufficiently tight. In an application involving the display of police photographs (taken on the occasion of a previous arrest) to third parties (potential witnesses) in connection with a criminal investigation the Commission took into account the following extenuating circumstances:

"firstly...the photographs were not taken in a way which constitutes an intrusion upon the applicant's privacy [photograph on arrest]; secondly...the photographs were kept in police or other official archives since they had been taken by the police in connection with a previous arrest; and thirdly...*they were used solely for the purpose of the identification of drug dealers during an action initiated by the public prosecutor to relieve a certain area of Amsterdam from the nuisance caused by drug trafficking and there is no suggestion that they have been made available to the general public or used for any other purpose.*"⁴³

1.60 Taking all the above into consideration the Commission found that the particular use of the photograph in question did not amount to an interference with private life.

1.61 Security checks on prospective (and existing) employees may also give rise to an "interference". Normally such a person will be unable to say with exactitude whether the relevant file actually explored aspects of his/her private life. However,

41 Naismith, *op. cit.*, at 154.

42 *Ibid.* at 154-5.

43 *Doorson v. The Netherlands* No. 20524/92, 75 DR 231 at 238 (1993). See also *TV v. Finland* No. 21780/93, 76A DR 140 (1994) ('interference' justified in a democratic society where disclosure of a prisoner's HIV-positive status to staff directly involved in his care in circumstances where a strict obligation of confidence applies and where there was no evidence of any wider disclosure) [emphasis added].

"an individual may, under certain circumstances, claim to be the victim of a violation occasioned by *the mere existence of secret measures...without having to allege that such measures were in fact applied to him.*"⁴⁴

1.62 Thus the very existence of laws and practices permitting and establishing a system for effecting secret surveillance amounts in itself to an interference with an individual's right to respect for private life calling for justification under Article 8(2). Again, this is without prejudice to the existence of such justification under Article 8(2).

1.63 Not everyone can claim that the mere existence of a system entails an interference with private life. It is only in circumstances where there exists a reasonable likelihood that the security services involved had compiled (and continues to retain) personal information about particular individuals that an applicant may be allowed to proceed in the absence of definitive proof of an interference⁴⁵. Usually this is not difficult to establish from the circumstantial evidence⁴⁶.

1.64 However, where the purpose for the collection of the information is less obviously valid then the level of intrusion required to constitute an interference may be lower. It is to be noted that one of the factors mentioned by the Commission in *Friedl*⁴⁷ was that the information was not rigorously processed and disseminated. Naismith concludes on this point that

"the authorities are not at liberty to engage in general intelligence-gathering, even in public, without any immediate link to investigations concerning a specific individual. Such conduct might well be regarded as an interference requiring justification in the same way as a straightforward invasion of privacy."⁴⁸

1.65 It is therefore plausible to assume that even if a particular act of surveillance cannot on its own be fairly labelled an "interference" (e.g., photographing a person in a public place) it might nevertheless be deemed an "interference" (requiring justification under Article 8(2)) if its purpose is to gather and disseminate personal information. As Harris *et al* point out,

44 *Klass v. Germany* (1978) 2 EHRR 214 at para 34 [emphasis added].

45 See, for example, *Hilton v. UK* No. 12015/86, 57 DR 108 at 119 (1988).

46 See, for example, *Hewitt and Harman v. UK* No. 12175/86, 67 DR 88 (1989).

47 (1996) 21 EHRR 83.

48 Naismith, *op. cit.*, at 155.

"[t]he mere fact that the collection of information might [itself] be justified does not inevitably mean that its retention or *use* will be equally defensible."⁴⁹

1.66 This would seem to apply, *a fortiori*, where the information is disseminated in circumstances where the controls against abuse are found non-existent or wanting under domestic law.

1.67 In sum, the extent to which the Commission and Court have embraced nearly all the values and functions of privacy mentioned in chapter 1 of this Report (1.7) is striking. They have certainly shown solicitude to privacy in a territorial sense and are quick to label intrusion at this level as an "interference". But they have gone beyond that to a more purposeful and dynamic view of "private life". They have grasped the point that privacy serves human dignity ("moral integrity") and have begun making tentative connections between certain aspects of physical harm and respect for private life. This raises the possibility of linking ideas about harassment to notions of private life.

1.68 Moreover, it is entirely plausible to suggest that the Commission and Court tend to view, and value, private life from the perspective of human autonomy. As evidence of this, human relationships are now embraced within the concept of private life. The notion of personal space described by Harris *et al* - a space or aura that follows the person - seems to fit well with the caselaw. It is certainly arguable that the deliberate targeting of a person in a public place through covert surveillance amounts to an "interference" requiring justification. What would appear to count most is whether a 'reasonable expectation' of privacy exists given all the circumstances of the case. This would be all the more so where that person's presence in a public place is unconnected with a public event. It would also be so where the actual or likely purpose behind obtaining the material was to disseminate it or otherwise publish it. In much the same vein it may be argued that to subject persons in general (e.g., pedestrians) to surveillance may "interfere" with their ease of mind. Adequate notification (if appropriate) and safeguards against abuse would seem warranted. The key would seem to be the notion of "reasonable expectation of privacy" which as a term is now openly used by the Court.

1.69 Lastly, the informational aspect of privacy also receives due attention and, as strongly suggested by Naismith, may even tip the scales in labelling certain behaviour as an "interference" when it might not otherwise be so considered.

1.70 Nothing in the above analysis prejudices the availability of a justification under Article 8(2). What it does show, however, is that "interferences" requiring

49 [emphasis added].

justification can be found by the Strasbourg authorities in a variety of circumstances thus placing an onus on those who would intrude on private life to come forward with a satisfactory justification.

(iii) *Do State Parties have any Affirmative Obligations under Article 8 with respect to Regulating Private Behaviour?*

1.71 Our core recommendation - the enactment of a tort of privacy-invasive surveillance - does not entail a restriction on privacy. Rather it entails taking some positive action to enhance the protection of privacy in the context of the behaviour of private parties. The question arises whether Ireland is permitted or even required to do so under the Convention. This question can be subdivided into two.

1.72 First, do States have any obligation to take positive action under Article 8 with respect to the regulation of private parties in the context of privacy-invasive surveillance? If they do not, a further question is whether States may act as if a positive obligation existed, so that while Article 8 may not impose any such obligation, it places no obstacles in the way of States voluntarily assuming such an obligation. We believe that such a positive obligation does arise under Article 8 and that, in any event, the assumption of such an obligation would not encounter insurmountable obstacles under the Convention.

1.73 Secondly, would Ireland be acting within its margin of appreciation by choosing to legislate in order to discharge its positive obligation under Article 8 (whether imposed or voluntarily assumed). We are of the view that appropriate legislation (of the type we recommend) is within Ireland's margin of appreciation in this regard since the public interest defence we now recommend provides an adequate balance between privacy and the main right in competition - freedom of expression. This is most assuredly not to decry the role of other methods of ensuring respect for private life including the active encouragement and support of self-regulation. The deployment of a range of means including self-regulation may well be appropriate but, in our view, legislation is the linchpin in any overall strategy.

1.74 As was rightly pointed out in submissions, state responsibility under Article 8(2) is only engaged where there has been an "interference" with private life by a "public authority". It follows that the only obvious obligation on States is to abstain from interfering except on certain narrow and tightly controlled grounds under Article 8(2). This, at any rate, is the classic view of a "negative right" - i.e., a right that simply negates state power but does not animate it or reach private power.

1.75 One superficially attractive solution to the conundrum of state responsibility concerns an expansive interpretation of what is meant by "public authority" to include private actors in some sufficiently close relationship with the public sphere. A

sufficiently close nexus was found, for example, in *A v. France*⁵⁰ where an individual recorded a telephone conversation with a third party in the presence of (and with the consent and active assistance of) a police officer using the officer's official telephone - a form of participant monitoring. Even though the police officer in question had not sought official sanction the Court nevertheless found that "the public authorities were involved to such an extent that the State's responsibility under the Convention was engaged"⁵¹. This approach - linking private acts with public power and authority - works well up to a point as demonstrated in *A v. France* but becomes patently artificial at a certain elusive point and so has very discrete limits. Sooner or later one is left with private behaviour that has no colourable connection to public authority and consequently with the need to find an alternative basis for engaging state responsibility.

1.76 There is a continuum of approaches to this question of state responsibility. At one end of the continuum a strict construction of the term "interference by a public authority" would entail only protecting people against public power and effectively turning a blind eye to violations perpetrated by the strong on the weak in civil society. On this view, however harsh, the state bears no responsibility for the private violation of rights - nor even for countenancing a legal regime or vacuum that allows (or even tacitly encourages) such violations to take place. At the other end of the continuum a more liberal interpretation would hold that the state must assume full and ultimate responsibility for all infractions of rights no matter the identity of the perpetrator (whether public or private). The truth lies somewhere between these two extremes.

1.77 The arguments against the literal and narrow view are quite persuasive. There does come a point where, by simply allowing losses to lie where they fall, human rights could be seen as a mere *apologia* for an unjust status quo where the results of gross imbalances of power in civil society are ratified by law⁵². It might therefore be argued that the classical approach is valuable in its own right but needs to be supplemented with some sense of a state's affirmative responsibilities in regulating private relations at least in circumstances where there is a gross disparity of power as between private parties. Such a broader approach would seem to fit better with the spirit of the European Convention and with the "social state" principle accepted in many European countries⁵³. The essence of the "social state" principle is that states bear some affirmative responsibilities to intervene to regulate private

50 Judgment of the Court, (1993) 17 EHRR 462.

51 *Ibid.* at para 36.

52 See, for example, A Clapham, *Opinion: The Privatisation of Human Rights*, [1995] EHRLR 20. See also, by the same author, *Human Rights in the Private Sphere*, (Oxford University Press, 1993), especially Chapter 7, *The Application of the European Convention on Human Rights to the Acts of Non-State Actors: The Case-Law of the European Commission and Court of Human Rights*.

53 See, for example, N Foster, *German Legal System and Laws* (Blackstone Press, 1993), p.151.

relations especially in circumstances where, if left unregulated, stronger parties will predictably prevail and thus set fundamental rights effectively at naught.

1.78 On the other hand, the second or more liberal approach which holds the state accountable for all private wrongs would subvert the very line between things public and private which is, after all, what human rights are primarily designed to preserve. Such an approach, in any event, is plainly at odds with the text of the Convention which is addressed in the main at States.

1.79 The "solution" which has been adopted by the European Court takes a middle course. It has not meant to make States responsible for all third party behaviour. That would plainly be at odds with the spirit of the Convention which was designed chiefly to deal with curtailing state power and would stretch the text of Article 8 to breaking point. But, in order to do full justice to the rights at stake, it has developed a theory of where the imposition of affirmative obligations is appropriate - and perhaps even necessary.

1.80 At a very general level it must be borne in mind that Article 1 - which contains the overall obligation on States to secure the rights contained in the Convention - sets an important tone that informs the rest of the text as well as this particular debate concerning state responsibility. It states:

"The High Contracting Parties *shall secure to everyone within their jurisdiction* the rights and freedoms defined in Section I of the Convention."⁵⁴

1.81 This general obligation is referred to from time to time to fortify a holding that some Convention right or other entails a modicum of positive state responsibility to reach private behaviour. The case of *Costello-Roberts v. UK*,⁵⁵ for example, involved claims under Articles 3 and 8 arising out of the infliction of corporal punishment in a private fee-paying school. The British Government's initial objection was that it could not be held answerable for this since it did not amount to a direct "interference" by a "public authority". The Court stated:

"The Court has consistently held that the responsibility of a State is engaged if a violation of one of the rights and freedoms defined in the Convention is the result of non-observance by that State of its obligations under Article 1 to secure those rights and freedoms in its domestic law *to everyone within its jurisdiction...*"⁵⁶

54 [emphasis added].

55 (1995) 19 EHRR 112.

56 *Ibid.* at 132 [emphasis added].

1.82 Education is, of course, one of the rights protected under the First Protocol to the Convention.

1.83 Also at a general level the right to an effective remedy under Article 13 must be taken into account. This aspect of the Convention was explored in our Consultation Paper. In itself, Article 13 does not require the transposition of the Convention into domestic law. In essence, it requires the existence of an effective remedy where arguable claims can be made regarding violations of the rights secured by the Convention. Failure to so provide amounts to an autonomous violation of the Convention. According to the case law an "effective" remedy need not necessarily be a legal one although States do enjoy a margin of appreciation (under both Articles 8 and 10) in choosing means that would seem to them appropriate. However, to repeat a point made by the Court and stated earlier in our Consultation Paper, an "effective" remedy for the purposes of Article 13 means a remedy that is "as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance"⁵⁷.

1.84 The Court also emphasised in *Costello-Roberts v. UK* that with respect to Convention obligations a state

"cannot absolve itself from responsibility by delegating its obligations to private bodies or individuals."⁵⁸

1.85 This does not appear to mean that States cannot delegate certain responsibilities with respect to the rights protected under the Convention to private actors if that is judged to be an effective way of securing a right. Indeed, the optimal situation might well entail a creative mix of reliance on properly primed self-regulatory bodies and positive law. Self-regulation and the provision of legally binding parameters are not mutually exclusive but can be mutually reinforcing. What the above passage does indicate is that States cannot avoid answering for the behaviour of private regulatory bodies if they choose to rely on them. Thus, even if a State deliberately opts for (or merely acquiesces in) self-regulation in, say, the media, then it cannot avoid having to answer for the effectiveness (or otherwise) of the apparatus of self-regulation in meeting its overall Convention responsibilities.

1.86 Assuming *arguendo* that state responsibility does arise with respect to private behaviour under Article 8 then it would, of course, be in a State's own self-interest to ensure that any mechanism of self-regulation was well structured and adequately tasked to take due account of all rights at stake. In our view, the best way to do this is to provide framework legislation providing effective preventative as well as

57 *Klass v. Federal Republic of Germany*, Judgment of the Court, (1978) 2 EHRR 214 at para 69.

58 Judgment of the Court, (1995) 19 EHRR 112 at para 27.

compensatory legal remedies, within which provision is made for self-regulation. This view assumes that States do have positive obligations with respect to private parties under Article 8 and are therefore answerable for intermediary bodies where relied upon to help them discharge their obligations. In our view the case law bears this assumption out.

1.87 Leaving such general considerations to one side, there arises an interesting tension between two different ways of rendering state responsibility under Article 8 with respect to the interests protected thereunder. On the one hand, the notion of "respect" for private life etc. contained in Article 8(1) seems even on its face quite broad and to embrace some consideration of an obligation to take positive action⁵⁹. Secondly, the notion of non-interference by a public authority under Article 8(2) seems on its face quite narrow and to implicate state responsibility only in the classic negative sense. The net question is: Which aspect of the Article takes precedence in determining the extent of a State's positive responsibilities, if any, in the context of private behaviour? Normally it would appear that the narrow view prevails but there is a long and authoritative line of Court judgments that sometimes point in the other direction. This strand in the case law did not originate in Article 8 but has begun to make its influence felt under that Article.

1.88 The seminal case of *Airey v. Ireland*⁶⁰ involved state responsibility for failing to act positively to secure respect for an "effective" right of access to a court under Article 6. The European Court in *Airey* stated that

"fulfilment of a duty under the Convention on occasion necessitates some positive action on the part of the State; in such circumstances, the State cannot simply remain passive and [quoting from the decision in *Marckx v. Belgium*] "there is... no room to distinguish between acts and omissions"⁶¹.

... The Convention is intended to guarantee not rights that are theoretical or illusory but rights that are *practical and effective*.⁶²

1.89 The obligation found in the *Airey* case and its progeny is one to take sufficient action to ensure *effective* enjoyment of a right. It is an acknowledgement of sorts that failure on the part of the state to redress inequality of resources in as much as they bear on the effective enjoyment of a right engages state responsibility. It goes to distributive issues in as much as they directly impact on the effective

59 On this issue generally, and on the drafting of Article 8, see T Opsahl, *The Convention and the Right to Respect for Family Life*, in AH Robertson (Ed.) *Privacy and Human Rights* (Manchester University Press, 1973), p182.

60 (1979) 2 EHRR 305.

61 *Ibid.* at para 25.

62 *Ibid.* at para 24 [emphasis added].

enjoyment of a right secured by the Convention. The outer boundaries of the obligation are left quite fluid and States are entitled to a wide margin of appreciation in deciding which methods or policy tools to use⁶³.

1.90 Inequality of resources and other vulnerabilities may also leave the individual exposed to the depredations of third parties. Material inequality is not, of course, the only or exclusive cause of vulnerability. The absence of an appropriate legal regime can also expose very wealthy people to violations of rights by private parties. The real point is that respect for private life applies to all persons regardless of material wealth and the vulnerabilities can arise in many ways.

1.91 On occasion the Court has found that States have an obligation to take positive action in the form of regulating private behaviour. In the early and celebrated case of *Young, James and Webster v. United Kingdom*⁶⁴ the European Court held that state responsibility is engaged for permitting certain private actions to occur which in fact violated Article 11 (freedom of association). The UK was held answerable by the Court not for the acts themselves but for a legal regime that allowed such acts to occur.

1.92 Such strains in the case law are also having an effect on the way the Court approaches the issue of state responsibility under Article 8. In *X & Y v. The Netherlands*⁶⁵ the Court had to deal with Dutch legislation that allowed the minor victims of rape to instigate criminal proceedings but which denied a similar standing to a parent in circumstances where the minor in question was incapable through mental disability of so doing. In an important passage the Court stated

"23. The Court recalls that although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an *effective respect* for private or family life. *These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves.*

...

24. The Court ... observes that the *choice* of the means calculated to secure compliance with Article 8 in the sphere of the relations between themselves

63 See, for example, *Andersson & Kullman v. Sweden* No. 11776/85, 46 DR 251 (1986), where the argument that states had a positive obligation arising under Article 8 to provide the financial means whereby one or both parents could remain at home to look after children was rejected.

64 (1982) 4 EHRR 38.

65 (1985) 8 EHRR 235.

is in principle a matter that falls within the Contracting States' margin of appreciation. In this connection, there are different ways of ensuring "respect for private life", and the nature of the State's obligation will depend on the particular aspect of private life that is at issue. Recourse to the criminal law is not necessarily the only answer.

...

27. The Court finds that the protection afforded by the [Dutch] civil law in the case of wrongdoing of [this] kind [rape] ... is insufficient. *This is a case where fundamental values and essential aspects of private life are at stake. Effective deterrence is indispensable in this area and it can be achieved only by criminal law provisions...*⁶⁶."

1.93 The notion of "effective respect" which arose in *Airey* in the context of distributional issues was extended by the Court in *X & Y* to embrace a concern for regulation as between private parties. Unfortunately, the Court did not put forward a coherent theory of when and under what circumstances the imposition of this kind of obligation to regulate private relations is warranted. Indeed the Court in *Abdulaziz, Cabales and Balkandali v. UK* (a case which dealt with the comparable notion of family life) said:

"especially as far as those 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."⁶⁷

1.94 The diversity of practices among the Contracting States dealing with the right of admission, if any, of the relatives of settled immigrants, was uppermost in the minds of the members of the Court in *Abdulaziz*⁶⁸. Arguably, however, European States are converging on a consensus about the importance of protecting privacy and very many of them do have legislation dealing with the matter as indicated in Chapter 6 of this Report. Of some relevance in this regard is the Resolution on Privacy adopted by the Parliamentary Assembly on 26 Jun, 1998 which is analysed in Chapter 1 (see Annex V for full text). The Resolution rejects the call for the drafting of a full privacy convention on the basis that Article 8 of the Convention is adequate as it stands and on the assumption that national privacy-specific legislation already exists and is equal to the task. With respect to those Member States that do not already have such legislation (this would include Ireland), the Resolution calls for its introduction along certain detailed guidelines provided.

66 *Ibid.* at 239 et seq [emphasis added].

67 (1985) 7 EHRR 471 at para 67.

68 See also, *Tanko v. Finland* No. 23634/94, 77A DR 133 (1994).

(iv) *The Adequacy of Existing Remedies as a Factor*

1.95 It seems from the case law that one factor in determining whether such positive obligations arise is the adequacy of existing remedies. The Commission appears not to treat the question whether a tailor-made remedy lies for a particular grievance as controlling. Instead, it tends to look to the cumulative adequacy and effectiveness of all remedies that may lie whether directly or indirectly relevant. It therefore sweeps into the equation many remedies that may have been fashioned to meet other ends but which may nevertheless play a role (in isolation or in combination with other remedies) in protecting private life.

1.96 In *Whiteside v. UK*, for example, the Commission conceded that harassment at a particular level of intensity might amount to an interference with private life. The problem was that no tort of harassment existed under English law at the time. The Commission nevertheless went on to decide that there were well-established remedies under domestic law which could have provided adequate relief (including particularly the possibility of taking an action in respect of conduct calculated to impair health)⁶⁹. This approach, in a sense, drove the applicant back to her remedies in domestic law which did not in fact directly address the grievance in question.

1.97 Similarly, in *Winer v. UK*⁷⁰ the applicant complained of the absence of a remedy in English law, including a right of reply, for gross invasions of privacy arising from matters published in book form and which were not necessarily defamatory or untrue. Winer submitted that the concept of privacy has no satisfactory definition in English law. Significantly, the Commission

" [did not] accept that the remedy of breach of confidence, taken alone or in conjunction with an action for defamation, may constitute an adequate or effective remedy within the meaning of Article 26. In particular, the Commission notes the uncertainty as to the precise scope of the remedy... and also the disquiet expressed by the Law Commission... as to the extent of the remedy."⁷¹

1.98 This at least signaled the Commission's unhappiness with the adequacy of the British law of confidence even as a way of indirectly protecting privacy interests. Nevertheless, the Commission did not view the very absence of an actionable right to privacy as such under UK law as evincing a lack of respect for private life. This was so because privacy was not wholly unprotected as shown by defamation law and

69 *Whiteside v. United Kingdom* No. 20357/92, 76A DR 80 at 86-87 (1994).

70 No. 10871/84, 48 DR 154 (1986).

71 *Ibid.* at 170.

settlement and the liberty to publish. Again, this approach drives the applicant back on his or her remedies under domestic law.

1.99 More recently the Commission had to consider the application of Earl and Lady Spencer against the UK⁷². The applicants had, like *Winer*, similarly argued that the absence of a specific remedy for breaches of privacy violated Britain's obligations under Article 8. The Commission found the application inadmissible on the basis that the applicants had failed to exhaust their domestic remedies. In essence, the Commission acknowledged that recent developments since *Winer* in the British law of confidence were making some of the claims of the applicants more *arguable* than hitherto before the British courts.

1.100 From this perspective it might well be argued that the existing law on defamation, trespass law, nuisance, confidence, etc., adequately discharge any positive obligation arising under Article 8 in the context of privacy-invasive surveillance. The reason why it is possible for the Commission to take this approach is because although the concept of privacy *per se* is relatively new it has been embraced to a certain degree by a myriad of remedies in most legal systems. Focusing on the importance of harnessing all possible remedies to their full potential is no doubt wise since it provides an incentive for creative argumentation and organic growth in the law and relieves the Commission from the onerous task of suggesting that tailor-made remedies are needed.

1.101 However, the Commission and Court cannot postpone hard questions indefinitely. There is a limit to the ability of the civil law for self-regeneration. Remedies which are currently relied upon to protect privacy are often inappropriate for this purpose. For example, defamation law is sometimes stated to protect privacy interests. This is so because a plaintiff can effectively force a defendant to prove the truth of published matter to avail of the chief defence of truth. This is not always easy to do and therefore the threat of a libel action be enough to act as a powerful deterrent against publishing true matter in the first place. This function is not, of course, what defamation law is primarily designed to do. One should not be forced to torture the form of defamation to suit the substance of a claim in privacy. Even if the Commission persists in its approach a State could well take the view that existing remedies should be supplemented with a general remedy that more directly protects privacy. Although it may not be required to do so, the Commission would be entitled to form the view - compatible with the Convention - that such action is necessary.

1.102 The Convention organs have yet to be confronted with a stark case where the accumulated body of such laws proves utterly incapable of adequately protecting

72 Nos. 18851/95 and 28852/95. Decision on admissibility, 16 January, 1998.

private life in the context of surveillance and resulting publication. As demonstrated in Chapter 3 such cases come about in part because our inherited law was not primarily designed to protect privacy interests and because developments in technology have outstripped the capacity of the law to respond. Many such cases have failed to reach the Court as a result of the Commission's finding of a failure to exhaust domestic remedies. This illustrates the difficulties encountered by plaintiffs who may often find themselves engaged in a guessing game as to the most appropriate remedy to pursue.

(v) *The Existence of a Fair Balance between the General Interest and the Interests of the Individual as a Factor*

1.103 Another factor used by the Commission and Court in determining whether positive obligations under Article 8 exist is that

"regard must be had to *the fair balance that has to be struck between the general interest and the interests of the individual.*"⁷³

1.104 The Court recently emphasised the boundaries to the notion of positive obligations in *Stjerna v. Finland* where it stated

"The boundaries between the State's positive and negative obligations under Article 8 do not lend themselves to precise definition. The applicable principles are nonetheless similar. In both contexts regard should be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole."⁷⁴

1.105 Since the boundary between negative and positive obligations is inherently nebulous and depends on many different factors the resulting jurisprudence is somewhat less stable than normal. This relative instability, which is probably an inescapable feature of such a novel domain, has not been universally approved⁷⁵. Nevertheless, the domain itself seems here to stay.

1.106 Whether the general obligation to "respect" private life will be rendered into an obligation to regulate private relations depends on many factors. In the context of this Report that means an evaluation of how Article 8 relates to Article 10. In this context it will be recalled that the Commission has stated in *N v. Sweden* that where

73 *B v. France* Judgment of the Court, (1992) 16 EHRR 1 at para 44 [emphasis added].

74 Series A, No. 299-B (1994).

75 For a review of the case law and the attitude of some of the judges on the Court see Colin Warbrick, *The Structure of Article 8*, [1998] E.H.R.L.R. 32.

"a question arises of interference with private life through publication in the mass media, the State must find a proper balance between the two Convention rights involved, namely the right to respect for private life guaranteed by Article 8 and the right to freedom of expression guaranteed by Article 10 of the Convention⁷⁶."

1.107 The published matter in that case had to do with allegations of criminal acts concerning large-scale fraud. Consequently, in the view of the Commission, they concerned a matter of some public interest. Without saying as much, the Commission is clearly of the view that the closer the expression comes to matters of public interest the more controlling are the Article 10 concerns. It is to be noted that the "public interest" defence we recommend explicitly includes cases where there are allegations of criminal activity and is therefore quite in keeping with the attitude of the Commission on this matter.

1.108 Another case involving the balance between Articles 8 and 10 arose before the Commission in *Ijspeerd v. The Netherlands*⁷⁷. The applicant, who was a student and who received free passes to public transport, objected to the practice of sending out unsolicited advertising brochures to the recipients of such passes. The Government responded by claiming that it was the inclusion of such material that helped ensure subsidised public transport and could, in any event, be easily ignored. The Commission looked at the facts of the case to see whether they disclosed a lack of respect by the respondent Government on the basis of a positive obligation. The Commission weighed, on the one hand, the freedom to impart information of a commercial nature (protected under Article 10) and the need to adopt innovative methods for financing public transport. On the other, it looked to the fact that the information in question could easily be ignored. Unsurprisingly, the Commission held, in effect, that the annoyance experienced by the applicant was more than outweighed by the other socially beneficial factors indicated.

1.109 These two applications, *N v. Sweden* and *Ijspeerd v. The Netherlands*, do not go to the core of private life. They balance private life with freedom of expression in situations where the privacy interest is weak, such as where there are well grounded allegations of criminality or where there is a need to balance mere annoyance to certain members of the public with the social need to subsidise public transport. Consequently, they do not lend strong authority to the proposition that freedom of expression must always outrank the right to respect for private life.⁷⁸

76 No. 11366/85, 50 DR 173 at 175 (1986).

77 No. 24967/94, 80A DR 175 (1995).

78 See Part 2 of this Chapter, *infra*.

1.110 Based on the case law to date, the key criterion in determining whether any positive obligations arise under Article 8 with respect to the regulation of private behaviour is what is needed to ensure "*effective respect*" for private life. From the case law so far it is plausible to assume that the Court will take into account the following

- the fundamentality (or otherwise) of the right (or aspect of the right) at stake,
- the nature of the threat/s posed by third party behaviour,
- the adequacy of existing legal remedies in the round,
- the consequences for the individual of leaving such behaviour unregulated or inadequately regulated,
- prevailing views and practices across the spread of Contracting States and
- an appropriate balance between this and other competing rights (if applicable).

1.111 On all of the above counts a very convincing case can be made for the regulation of private relations with respect to privacy-invasive surveillance. The case law to date does not suggest that Article 10 interests always outrank Article 8 concerns.

(vi) *Does the Obligation to Take Positive Action Require or Allow for Legislation?*

1.112 If an obligation to take positive action in the form of regulating third party behaviour arises in the context of privacy-invasive surveillance then the next question is what form should this regulation take.

1.113 States enjoy a wide margin of appreciation in determining the best means to discharge a positive obligation. It is to be noted that this "margin of appreciation" doctrine is somewhat different from the one that normally applies under Article 8. The normal "margin of appreciation" doctrine applies where States resolve to interfere directly with a protected right like private life through, for example, telephone tapping legislation. In doing so they are entitled to a wide "margin of appreciation" in determining whether their measures are "necessary in a democratic society" as required under Article 8(2). Here, however, the matter is somewhat different because the affirmative nature of the obligation actually *requires* direct state intervention in order to advance the right to private life in the context of regulating private behaviour. The rights implicated are third party rights such as freedom of expression. Therefore, the limiting grounds listed in Article 8(2) - which are really

addressed to the State in the exercise of its police power to protect and balance rights - are not directly relevant but may be indirectly so.

1.114 We now arrive at the heart of the matter. If an affirmative obligation is acknowledged to arise with respect to regulating private behaviour consisting of privacy-invasive surveillance then the real question becomes whether legislation is required or at least permitted. The key question for our purposes is not so much the debate about the necessity for legislation but whether the Convention would place any insurmountable obstacle to legislation if that were judged necessary and viable by a State.

1.115 As indicated above in *X & Y v. The Netherlands*⁷⁹ the Court will normally defer to a State's choice of means and apply a variant of the "margin of appreciation" doctrine. The Court certainly reserves the right to pronounce on the adequacy of the means (or mix of means) employed, for example administrative, reliance on self-regulation, civil law, criminal law, etc.

1.116 It is noteworthy that the Court's key concern in *X & Y v. The Netherlands* was not that the law enacted was inadequate but that it did not in fact go far enough bearing in mind the fundamental values and essential aspect of private life at stake. It might be said that this case was an easy case for the Court since it focused on a glaring *procedural* gap in Dutch law. However, it is certainly plausible to suggest, given the fundamentality of the values at stake and the fact that surveillance touches an essential aspect of private life, that legislation regulating private parties is permitted if not actually required. It is interesting to note that neither French nor German privacy legislation dealing with surveillance has been challenged to date before the Strasbourg authorities although obviously one should be careful about inferring too much from this factor alone.

1.117 The general point in *X & Y v. The Netherlands* concerning the occasional necessity to assume positive obligations under Article 8 was strongly reiterated recently by the Court in *Stubbings and Others v. UK*.⁸⁰ In that case the Court stated:

"61. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is in issue. *It follows that the choice of means calculated to secure compliance with this positive obligation in principle falls within the Contracting States' margin of appreciation.*

79 (1985) 8 EHRR 235.

80 (1997) 23 EHRR 213.

62. Sexual abuse is unquestionably an abhorrent type of wrongdoing, with debilitating effects on its victims. Children and other vulnerable individuals are entitled to State protection, in the form of effective deterrence, from such grave types of interference with essential aspects of their private lives.

...

64. ...Article 8 does not necessarily require that States fulfil their positive obligation to secure respect for private life by the provision of unlimited civil remedies in circumstances where criminal law sanctions are in operation."⁸¹

1.118 It is noteworthy that in the above case a full panoply of civil sanctions was deemed unnecessary where effective criminal sanctions are in place. The very permissibility of establishing criminal sanctions was not seriously in question in light of the fundamentality of the right (or aspect of the right) at issue as well as the nature of the threat posed by private behaviour. At the very least, this creates space for the enactment of criminal sanctions. Obviously such sanctions should be reserved for the most egregious of violations.

1.119 The *X & Y* and *Stubbings* judgments stand as authority for the following related propositions. First, the requirement on the State to "respect" the rights secured by Article 8 may extend beyond merely abstaining from "interfering" if this is necessary to secure "effective respect" for private life; secondly, the choice of means, including legislation, is within the State's "margin of appreciation" to decide; and thirdly, the appropriateness of particular means will be reviewed by the European Court in light of whether "fundamental values" and "essential aspects of private life" are at stake.

1.120 In circumstances where sufficiently important values and aspects of privacy were implicated the Court has shown little hesitation in demanding effective legislative responses. Arguably, privacy-invasive surveillance is one such area.

1.121 In short the Court is not averse to imposing a requirement to take positive action in the form of regulating private behaviour if this is needed to effectively secure a right. For a variety of reckonable reasons, including the fundamentality of private life, the nature of the threat posed by modern technology and the inadequacy of existing legal remedies, a strong case can be made for such an obligation in the context of privacy-invasive surveillance carried on by private parties. While States are entitled to a wide margin of appreciation in selecting the means for the regulation of private parties, the Court reserves the right to review the adequacy of the means selected.

81 [emphasis added].

1.122 On occasion the Court seems to require legislation as a means and has even endorsed criminal sanctions in a suitable case. A strong case exists for the view that civil legislation is at least permitted under Ireland's "margin of appreciation" and that criminal sanctions can be tolerated provided they are narrowly tailored and do not intrude unduly on other protected rights. Self-regulation is an option but with the *caveat* that States may not thereby absolve themselves of their Convention responsibilities (assuming that such responsibilities do arise with respect to regulating private behaviour).

(vii) *The Question Whether Covert Police Surveillance Using Electronic Means Requires a Basis in Positive Law and Related Matters*

1.123 In the preceding sections we looked at the ambit of private life and at the question whether States have any positive obligations to regulate private parties with respect to protecting privacy. Another way of looking at this is to ask whether States would be acting within their margin of appreciation to enact legislation regulating such private relations. As already mentioned, the margin of appreciation that applies in this context is very different from that which normally applies. With respect to the former one looks to the reasonableness of the impact (adverse or otherwise) on *other* protected rights and interests in determining how far States can go in protecting rights such as private life. One such *other* right is freedom of expression and we take a closer look at this right - and the degree to which it can legitimately be curtailed - later in this Chapter.

1.124 In this section we revert to the more classical situation where States opt to limit privacy. As mentioned at the outset of this Report, Ireland has a well developed statutory regime dealing with the interception of communications by the State and its agents. Parenthetically, it should be noted that the Court in *Malone v. UK* brought the practice of telephone metering within the protective embrace of Article 8. It stated

"The records of metering contain information, in particular the numbers dialled, *which is an integral element in the communications made by telephone*. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8⁶²."

1.125 No similar regime to the one established under interception legislation exists with respect to other forms of covert state surveillance. The issue addressed in this section is whether the Convention requires such action to be based on positive law

and, if so, what kinds of minimum attributes (substantive and procedural) such law should have.

1.126 To say that some basis in positive law is required is one thing. There is an argument to be made that to demand the full rigour of due process is quite another issue and would perhaps be out of place considering the exigencies under which the police are constrained to work under in the context of covert surveillance.

1.127 The normal checklist for the Court in evaluating the compatibility of state action with the Convention is:

1. whether there has been an "interference"
2. whether the "interference" was "in accordance with law"
3. whether the "interference" was "necessary in a democratic society"
4. whether the "interference" was grounded on one or other of the legitimate indicators contained in Article 8(2).

1.128 Does covert police surveillance using aural and video devices amount to an "interference" with private life? This issue is likely to be resolved by looking at whether a "reasonable expectation" of privacy exists in any given situation. It is presumably fair to infer from *Ludi v Switzerland*⁸³ that the closer one is to pure criminal activity then the less is the reasonable expectation of privacy. In *Ludi* the object of the police at the outset had been to arrest and not merely observe or gather evidence. However, it is also fair to assume that some sort of continuum exists ranging from outright participation in crime to fringe and perhaps unwitting involvement. More often than not, police surveillance with respect to the latter end of the continuum will be concentrated on general intelligence gathering rather than detecting the commission of a specific crime. Intelligence gathering is, of course, absolutely vital to the work of the police but it is probably fair to say that the further away it gets from specific crime the greater is the risk of unjustifiable intrusions on privacy. Furthermore *Ludi* did not directly address electronic means of covert surveillance which is the subject matter of this Report. It is certainly plausible to maintain that covert police surveillance (using aural and video devices) amounts to an "interference".

1.129 Should such activities be provided for by positive law? This reflects the underlying requirements of the rule of law which animates the entire Convention. The basic value at stake is the insistence that all limits imposed by States on rights must not rest merely on a substantive justification but must also be based on law. Any limit to a right that is not so based - even one that is substantively justified in the abstract - is likely to prove a threat to a right because of the extent of the

discretion afforded to the authorities. This insistence that limits be channeled through law is not just procedural but takes in substantive considerations also. Broken into its component parts this demands the prior existence of law (common law can count as law) and that the law possess certain qualitative attributes such as "accessibility" and "foreseeability". In the established case law of the Court, "accessibility" refers to the degree to which the law can be comprehended (via legal advice if necessary) and "foreseeability" refers to the precision with which it is cast. A high degree of precision enables individuals to plan their actions rationally so as to avoid entanglement with the law. Foreseeability is therefore at a premium where fundamental rights are at stake. Conferring discretion on officials is not, as such, inherently violative of Article 8. What matters is how adequately that discretion is bounded by law and the adequacy of the remedies available in the event of its misuse.

1.130 On occasion the Court has had to deal with the complete absence of any legislation governing covert surveillance. In *A v. France*,⁸⁴ for example, no legal regime existed to cover the interception in question (private interception with the connivance of a public official) and a violation of Article 8 was found. Similarly, in *Halford v. UK*⁸⁵ there was a complete absence of a regulatory regime dealing with the interception of telephone communications from a private office which was held violative of Article 8. The Commission recently admitted a case dealing with police surveillance in the form of drilling a hole through a boundary which enabled listening and optical devices to be installed: *Govell v. UK*⁸⁶. No specific legal regime existed at the time covering such activity. It was governed merely by UK Home Office Guidelines⁸⁷.

1.131 The problem in *Malone v. UK*⁸⁸ had to do with an insufficiently precise legal base for telephone tapping (as well as telephone metering) in UK law at that time.

1.132 If an "interference" with private life exists in the context of covert police surveillance (using electronic means) and if there is therefore a requirement for some legal basis to exist governing such activities then the next question that arises relates to the quality of the law to be enacted.

84 (1993) 17 EHRR 462.

85 (1997) 24 EHRR 523.

86 (1996) 23 EHRR CD 101, Decision on admissibility.

87 The complete absence of a legislative base was also held to violate the Convention in two other Article 8 cases: *N v. UK* No. 12327/86, 67 DR 123 at 133 (1989), and *Hewitt & Harman v. UK* No. 12175/86 67 DR 88 at 101 (1989).

88 (1984) 7 EHRR 14.

1.133 The Court in *Malone v. UK* isolated several factors of relevance in determining whether the law in question had provided adequate and effective guarantees against abuse. These factors went to

- the scope of the "interference" allowed,
- the duration allowed,
- the grounds specified in the legislation,
- the quality of the procedure involved in obtaining permission, in supervising the execution of the permitted action and in affording a remedy.

1.134 It was imprecision as to scope and manner of telephone tapping that led to a finding of a violation of Article 8 in *Kruslin v. France*⁸⁹.

1.135 Police surveillance is, of course, rather peculiar in that its very effectiveness depends in large measure on it remaining secret. This point was conceded by the Court in the first important case in the field, *Klass v. Germany*⁹⁰. There, the Court stated that

"...the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with [Article 8], since it is this very fact which ensures the efficacy of the 'interference'⁹¹."

1.136 Since this form of activity is (and generally must remain) secret to ensure its efficacy the focus of concern of the Court is not so much on *ex post facto* remedies but on the existence and quality of supervisory mechanisms. Remedies *ex post facto* are important but are unlikely to be availing given the absence of any general requirement of notification of the fact of surveillance.

1.137 It does not appear to be absolutely essential that there should be judicial involvement at the level of sanctioning action but that the independent element (which judicial involvement can best provide) is highly desirable in the supervisory mechanism.

1.138 In sum, it is certainly arguable that covert police surveillance (using electronic means) amounts to an "interference" with private life, especially the more remote it is from a specific crime. If so, some sort of legal basis is necessary to allow it to occur in a manner compatible with Article 8. This is not to say that the

89 Judgment of the Court, (1990) 12 EHRR 547.

90 (1978) 2 EHRR 214.

91 *Ibid.* at para 58. For illustrations see, for example, *Slip-on v. Switzerland* No. 11811/85, 55 DR 182 (1988) and *L v. Norway* No. 13564/88 65 DR 210 (1990).

procedure according to which it should occur must be exactly akin to that obtaining under telephone interception. What is important is that adequate guidance should be given in the law as to the scope of covert surveillance, its duration, the grounds on which an application may be made, the nature of the competent authorities permitting, executing and supervising the acts and the remedies available. What seems particularly important is the presence of some independent element in the process of supervising the implementation of such regime.

Part 2 - Freedom of Expression

3. Article 10

1.139 In addition to our core recommendation which is for the enactment of a statutory tort attaching to privacy-invasive surveillance we make an important ancillary recommendation that civil liability should attach also to the publication of material obtained through such acts. We do not recommend a general privacy statute as such since that is beyond the scope of this paper. Our ancillary recommendation dealing with publication addresses only the publication of matter that is the *result* of a prior act of privacy-invasive surveillance.

1.140 We feel it is necessary to prohibit publication in order to remove an incentive for privacy-invasive acts. In doing so we are seeking to protect privacy in two ways; first, by preserving the shield that protects private or personal space by denying actors the fruits of the poison tree and, secondly, by protecting information of a private nature at least to the extent that it has been obtained by piercing the privacy shield through surveillance. As has been seen above, both aspects of private life (personal space and personal information) are encompassed within Article 8.

1.141 Liability with respect to publication is subject to the defences of taking due care as to sources and to a public interest defence (see Chapter 9). It makes no difference that the information itself is private in its nature although it usually will be. What matters is that the publication of the full result of privacy-invasive surveillance is prohibited.

1.142 Undoubtedly, our ancillary recommendation would amount to an "interference" with freedom of expression under Article 10(1) and thus require justification under Article 10(2). Strong reservations were made in submissions and at the listening exercise as to whether the legislation we recommend can be reconciled with Article 10. While these reservations go mainly to the ancillary recommendation and not to the core recommendation they are crucial nonetheless.

1.143 Article 10 reads as follows:

"1. Everyone has the right of freedom of expression. That right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

1.144 It is our view that the legislation which we envisage is well within a State's margin of appreciation under Article 10.

1.145 The public interest defence which we now recommend provides, in our view, a principled and practical way of balancing the peoples' right to know under Article 10 with an individual's right to respect for private life under Article 8. Every person, including public figures, has a right to respect for his or her private life. It is only where an aspect of one's private life is closely and demonstrably connected to one's public function that the right of the public to know takes exceptional precedence over the right to private life. We do not view our recommendations as giving rise to a smoke-screen to be used by the wealthy and powerful. On the contrary, we open up considerable space through the public interest defence to publish material about such figures that is clearly of relevance in the public domain.

1.146 It should be noted that the reservations expressed in submissions and at the "listening exercise" go essentially to the proposed imposition of civil liability as to publication and leave largely unaffected our recommendation as to the imposition of civil liability - and indeed criminal liability - for particular *acts* of privacy-invasive surveillance. We do not consider that the case-law under Article 10 creates any entitlement to disregard existing positive law dealing with particular information-gathering acts. In our view, the information gathering acts are distinct from the publication process and we see nothing firm in the case-law under Article 10 to suggest the European Court thinks otherwise. We are of the view that a countervailing public interest in the "rule of law" takes precedence where violations of the criminal law are in issue.

1.147 Taking all things into consideration, including especially the "public interest" defence to publication which we now recommend, we believe that Ireland would be acting within its margin of appreciation in introducing legislation of the sort we recommend.

1.148 This whole question brings into sharp focus the interplay between Articles 8 and 10. Specifically, it calls for a consideration of how, or whether, legislation that is motivated by a desire to discharge a positive obligation arising under Article 8 can

be reconciled with the margin of appreciation doctrine under Article 10. Even if no positive obligation arises under Article 8 it remains to be seen whether legislation that affects interests protected under Article 10 can be independently justified under Article 10(2) as an exercise of a States' margin of appreciation to protect or advance the "rights of others".

1.149 As is clear from the text of Article 10, freedom of expression embraces not merely the right to impart information and ideas but also the right to receive it. The role of the media is particularly important in this regard since it enables the widest possible dissemination of information and ideas. Article 10 does not preclude a licensing system for certain organisations of the media⁹². The freedom is stated to carry with it duties and responsibilities and can therefore be subjected to formalities, conditions, restrictions (before the fact) or penalties (after the fact). Moreover any limitations must be prescribed through law (the principle of legality) and must be "necessary" in a "democratic society" for the advancement of a number of stated grounds including the protection of the "rights of others".

1.150 To evaluate the submissions more closely and, in particular, to assess the role to be played by the "public interest" defence we believe it is necessary to briefly review the ambit of Article 10 and to consider the special regard it has for "political expression" since this aspect of Article 10 was perceived to be the principle obstacle to our provisional recommendation with respect to publication. It is also necessary to canvass the nature of a State's margin of appreciation both generally under Article 10(2) and as it relates to measures motivated by Article 8. In the context of this paper the limiting ground at issue is that of "the rights of others" listed under Article 10(2) which provides the link with the interests protected under Article 8.

(i) *Is Freedom of Expression Intrinsicly Hostile to Privacy Legislation ?*

1.151 There is relatively little debate or dispute about what amounts to protected expression under Article 10(1).⁹³ This is no doubt due, in part, to the fact that unlike many constitutions the Convention is very explicit as to the limiting grounds at stake. Attention and disputation is therefore deflected away from Article 10(1) to Article 10(2). In the result, the publication of information, pictures and images of a purely private nature, indeed of any nature, is *ex facie* protected expression for the purposes of Article 10.

92 A relic from the time of resource scarcity - not a subterfuge for content-based restrictions.

93 Expression is taken to include pictures and images: see *Muller v. Switzerland* (1991) 13 EHRR 212 and *Chorea v. Austria* (1993) 17 EHRR 358.

1.152 Nor does much litigation turn on the question whether a given limitation was "prescribed by law". Obviously, the relevant law must possess certain liberty-enhancing technical attributes such as clarity, accessibility and foreseeability. However, the real threshold issue raised in submissions is whether privacy legislation of the type we recommend is compatible in principle under any conditions with Article 10.

1.153 While there may be little dispute over whether certain categories of expression are protected, the Court has effectively distinguished between differing levels of protection depending on the category of expression at stake with implications for the ambit of a State's margin of appreciation. This general solicitude seems to cut right across the various limiting grounds that can be relied upon under Article 10(2) (e.g., protecting the reputation of others, protecting the rights of others, maintaining the authority of the judiciary⁹⁴). It is clear that the Court treats limitations on "political" expression with the utmost seriousness and will closely scrutinise the alleged justification particularly where the most coercive means are involved such as criminal sanctions. In effect, when it comes to political speech, the Court is disinclined to view restrictions as being "necessary in a democratic society". That is why it is important to review the relevant case law and to establish whether any space is left for the kind of legislation we recommend.

1.154 This solicitude toward "political speech" is no surprise. Freedom of expression is different - and is universally viewed as different - in the sense that it is not merely targeted at the negation of state power but also plays a vital role in opening up and maintaining a healthy marketplace of political ideas⁹⁵. While it serves the interests of the person in self-expression it also serves much broader social and political interests. The enhanced status of freedom of expression as a human right flows therefore from a recognition that the democratic accountability of incumbents is enhanced wherever the flow of *relevant* information is at its optimum⁹⁶. History, especially European history, is replete with examples where

94 On the compatibility with Article 10 of laws protecting the judiciary from criticism see e.g., *Barfod v. Denmark* (1991) 13 EHRR 493 (criticism of judiciary found to be within acceptable bounds); *Prager and Oberschlick v. Austria* (1996) 21 EHRR 1 (criticism found to exceed acceptable limits); and *De Haes and Gijssels v. Belgium* (1998) 25 EHRR 1 (criticism found to be within acceptable limits). On the compatibility of laws restricting speech in the interests of justice generally see *Sunday Times v. UK* (1979) 2 EHRR 245 and *Weber v. Switzerland* (1990) 12 EHRR 508.

95 The metaphor of the market has one crucial implication. In any pure market it is the laws of supply and demand that determine price and value. Conceptualising news and information in market terms means that the only rational limitation to the market is that dictated by market forces - i.e., by the consuming public. This places an extremely heavy onus on those who would argue for content-based restrictions to square their views with a market perspective. On the market place metaphor see generally, Melville Nimmer, *Nimmer on Freedom of Speech: A Treatise on the Theory of the First Amendment*, (Mathew Bender, 1984 with 1989 supplement); Stanley Ingber, *The Marketplace of Ideas: A Legitimizing Myth*, (1984) *Duke L.J.* 1; and for a critique see Paul Brietzke, *How and Why the Marketplace of Ideas Fails*, 31 *Val. U.L.Rev.* (1997) 951.

96 See, e.g., Kent Greenawalt, *Free Speech Justifications*, 89 *Columbia L.Rev.* (1989) 119; Frederick Schauer, *Free Speech: A Philosophical Enquiry*, (Cambridge Univ. Press, ch.3, *The Argument From Democracy*; Thomas Emerson, *The System of Freedom of Expression*, (Random House, 1970).

the manipulation of information can be used as a tool to help consolidate elites in power. It is important that those who have most to gain (or hide) by manipulating what is meant by *relevant* information should not be allowed to control its meaning and ambit. If the Convention organs sometimes seem to give undue prominence to the democratic function of expression relative to domestic constitutions it is due, in part, the fact that the very purpose of the Convention was to maintain open democratic systems.

1.155 Power and the exigency of holding on to power creates temptations. Among other things, freedom of expression is said to have a "checking value" on any such tendencies⁹⁷. Furthermore, opening up the political economy of information and ideas serves not merely to hold incumbents to account but also helps to ensure that people have a realistic opportunity to adjudge the merits of competing political platforms. The freedom provides a space for fruitful encounters between those who espouse different visions of the future of the polity and who compete for control of the helm of the state.

1.156 The leading statement of the Court on why expression is considered so worthy of protection is contained in *Handyside v. UK*⁹⁸, where the Court stated that:

"Freedom of expression constitutes one of the essential foundations of a [democratic] society, one of the basic conditions for its progress and for the development of every man. Subject to Article 10(2), it is applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive ... but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of ... pluralism, tolerance and broadmindedness without which there is no 'democratic society'. This means, amongst other things, that every 'formality', 'condition', 'restriction' or 'penalty' imposed in this sphere must be proportionate to the legitimate aim pursued⁹⁹."

1.157 This democratic theme recurs throughout the case law. Moreover the Court is conscious of the vital role of the press in bridging the gap between the supply of relevant information and the legitimate demand for such from the public. For example, the Court stated in *Observer and Guardian v. UK*¹⁰⁰:

97 See generally Victor Blasi, *The Checking Value in First Amendment Theory*, (1977) American Bar Assoc. Res. J. (1977) 523.

98 (1978) 1 EHRR 737.

99 *Ibid.* at para 49.

100 (1992) 14 EHRR 153.

"Freedom of expression constitutes one of the essential foundations of a democratic society, in particular freedom of political and public debate. This is of special importance for the free press which has a legitimate interest in reporting on and drawing the public's attention to deficiencies in the operation of Government services, including possible illegal activities. It is incumbent on the press to impart information and ideas about such matters and the public has a right to receive them.¹⁰¹"

1.158 *Handyside* (and numerous cases like it) makes it plain that the democratic rationale is powerfully present in Article 10 and that its ambit stretches to expression that is uncomfortable not merely for the person who is the focus of critical comment but also for the audience as well.

1.159 The logic of *Handyside* is such that the political economy of ideas and information of relevance to the public sphere is considered of primary importance. As a result, any justification proffered by Governments for the limiting of such expression will be closely scrutinised.

1.160 In keeping with this line of reasoning the Court has held that persons who hold a status close to, or squarely within, the apparatus of state are constrained to tolerate a greater than normal forbearance toward expression that is hurtful. The leading case is *Lingens v. Austria*¹⁰². The net question for our purposes is whether this extra latitude to publish hurtful comment reaches into (and renders disclosable) information pertaining to a person's purely private life. If so, are there any limits or preconditions for such publication - are all aspects of a person's private life equally disclosable or is it only those aspects that bear directly on a person's public function?

1.161 The applicant in *Lingens*, who was a publisher/journalist, was fined for the criminal defamation of Chancellor Kreisky in two journal articles. The articles in question had criticised Mr Kreisky for having allegedly protected a former SS member and for his general sympathy toward ex-Nazis involved in politics. The impugned passages were in the form of critical comment for which there was no defence of "fair comment" under Austrian law as it then stood. In ruling that the "interference" in question was not "necessary" in a democratic society for the protection of the "reputation of others" the Court first emphasised the positive role of the press in democracy. It said:

"[I]t is ... incumbent on [the press] to impart information and ideas on *political issues just as on those in other areas of public interest*. Not only does

101 *Ibid.* at para 75.

102 (1986) 8 EHRR 407.

the press have the task of imparting such information and ideas: the public also has a right to receive them¹⁰³."

1.162 It is to be noted that the term "political issues" is conjoined with "other areas of the public interest" in the passage quoted. This evidences the rejection of a narrow interpretation of what is meant by a "political issue". Thus, political issues are not confined to matters of high politics but might include, for example, controversial topics such as attitudes toward racism.

1.163 An attempt was made in *Thorgeir Thorgeirson v Iceland*¹⁰⁴ to separate "political" issues from matters of "public interest" in the hope that the Court might hold that a State's margin of appreciation was wider with respect to the latter. The Court rejected this argument. It stated:

"the Court observes that there is no warrant in its case law for distinguishing...between political discussion and discussion of other matters of public concern¹⁰⁵."

1.164 The issue in contention in *Thorgeirson* was an allegation of police brutality which was clearly a matter of public concern. It is to be regretted that nowhere does the Court enunciate a general theory of what constitutes a matter a public concern. Potentially, nearly every subject is a matter of public concern; for example, an outrageous case of domestic violence could raise issues concerning the adequacy or enforcement of legislation. Nor did the Court address the question whether the test is an objective one - in which case "public concern" has autonomous meaning capable of being apprehended in legislation and grasped by a court. If the test is subjective then a related question arises whether the subjective opinion of, for example, an organ of the media concerning newsworthiness is sufficient. Indeed, does newsworthiness itself equate with "public concern"? Tentatively, it would appear that the notion of "public concern" does have some autonomous meaning and that it does not simply equate with newsworthiness. Other factors besides "public concern" can generate newsworthiness.

1.165 The Court does seem to treat critical comment from particular professions as being somewhat different to critical comment directed at public or political officials. Judge Rysdall summarises the overall approach of the Court as follows:

"Whilst recognising the importance of professional people contributing to public debate on matters of public concern linked to their professions, it has

103 *Ibid.* at para 41 [emphasis added].

104 (1992) 14 EHRR 843.

105 *Ibid.* at para 64.

given special emphasis to the "margin of appreciation" doctrine which it considers essential in areas as complex and fluctuating as professional ethics and unfair competition. The Court has attached particular weight not only to whether the criticism was substantiated but also whether it was *primarily aimed at contributing to discussions of matters of public interest or was rather intended to promote competitive interests*¹⁰⁶."

1.166 This seems to accept that professional life is not without implications for public life and that on occasion matters of public interest are at stake. However, no clear indication as to the guiding principles in cases such as this are given.

1.167 The Court in *Lingens* went on to widen the space permitted for critical comment on persons whose status brings them close to political or public affairs. It said:

"The limits of acceptable criticism are ... wider as regards a politician as such than as regards a private individual. Unlike the latter, the former inevitably and knowingly lays himself open to close scrutiny of his every word and deed by both journalists and the public at large, and he must consequently display a greater degree of tolerance¹⁰⁷."

1.168 The Court applied and amplified this aspect of its *Lingens* ruling in the case of *Castells v Spain*¹⁰⁸. In *Castells* the Court found that the greatest possible tolerance (with a correspondingly reduced margin of appreciation for States) applied to criticisms levelled at members of Governments in power. The Court said

"The limits of permissible criticism are wider with regard to the Government than in relation to a private citizen, or even a politician. In the democratic system the actions or omissions of the Government must be subject to the close scrutiny not only of the legislative and judicial authorities but also of the press and public opinion. Furthermore, the dominant position which the Government occupies makes it necessary for it to display restraint in resorting to criminal proceedings, particularly where other means are available for replying to the unjustified attacks and criticisms of its adversaries or the media¹⁰⁹."

106 Report by R Rysdall, *The Case Law of the European Court of Human Rights on the Freedom of Expression Guaranteed Under the European Convention on Human Rights*, delivered at the XIth Conference of the European Constitutional Courts, Budapest, 6-10 May, 1996, p11.

107 (1986) 8 EHRR 407 at para 42.

108 (1992) 14 EHRR 445.

109 *Ibid.* at para 46.

1.169 The speech in question was in fact uttered by an opposition member of Parliament without the benefit of parliamentary privilege. Restrictions on such speech was said to call for the "closest scrutiny" by the Court,¹¹⁰ which stated that

"Freedom of the press affords the public one of the best means of discovering and forming an opinion of the ideas and attitudes of their political leaders. In particular, it gives politicians the opportunity to reflect and comment on the preoccupations of public opinion; it thus enables everyone to participate in the free political debate which is at the very core of the concept of a democratic society¹¹¹."

1.170 This seems to contemplate a sliding scale depending on the status of the person and how close he/she is to the centre of political power.

1.171 The late President of the Court, Rolv Ryssdal, explained the result in *Lingens* as follows:

"The Court found that the Austrian law was excessively strict and liable to deter journalists from contributing to public discussion and to hamper fair comment in good faith on political issues¹¹²."

1.172 The ruling in *Lingens* brings out the presence and power of the democratic rationale. This is entirely fitting since the European Convention was itself designed largely to try to ensure the maintenance and stability of democratic regimes in Europe. The emphasis on democratic speech does not mean that other kinds of expression are unprotected. But it does mark out *restrictions* on political expression as deserving the closest of scrutiny. In fact the Court developed three *de facto* categories of expression ranging from political through cultural and commercial expression. Whereas political expression has the widest protection, cultural expression is less extensively protected, but ranges above expressions of a purely commercial nature.¹¹³

1.173 The net result of *Lingens* and its progeny is that States have a reduced margin of appreciation when it comes to regulating critical speech of a particular kind (i.e., on political issues or on issues in the public interest) and with respect to persons of a particular status (members of Government, members of parliament).

110 *Ibid.* at para 42.

111 *Ibid.* at para 43.

112 Ryssdal, *op. cit.* In *Thorgeirson v Iceland* (1992) 14 EHRR 843, the Court inveighed directly against the unavailability of any defence of fair comment under Icelandic law.

113 See, for example, *Mueller v. Switzerland* (1991) 13 EHRR 212 on artistic expression and *Barthold v. Germany* (1991) 13 EHRR 431 on commercial expression.

This is not the same as saying that all private matter relating to the personal lives of public figures is disclosable. Implicit in the Court's holdings is a certain view of the public sphere and of the critical importance of ensuring an uninhibited flow of relevant information about that sphere and the personages in it to the public at large. More often than not, information dealing with the private life of a public figure will have nothing clearly to do with his/her capacity to perform a public function. Sometimes, however, there will be circumstances where purely private information may be relevant to political issues or matters that are squarely in the public interest. Freedom of expression is not intrinsically hostile to privacy legislation. The real question is whether the opening created by the public interest defence which we propose adequately reconciles the people's legitimate democratic right to know with a person's right to privacy.

(ii) *Does The "Public Interest" Defence Adequately Reconcile Privacy with Freedom of Expression?*

1.174 The "public interest" defence creates an opening to publish what would otherwise be unpublishable under our recommendations. Is it good enough to satisfy the people's right to know under Article 10?

1.175 *Lingens* itself dealt with critical comment on the attitude of a politician concerning a topic of pressing public importance (dealing with the Nazi past). It did not directly address the question of reconciling private life with political expression as that term is broadly interpreted by the Court. Indeed, the Court expressly reserved judgment on this point in *Lingens*¹¹⁴.

1.176 The Court in *Lingens* looked to two separate but related matters. First, it had regard to the *nature* of the information at issue (political or related to public affairs). Secondly, it looked to the *status* of the person involved to determine the scope of a State's margin of appreciation in regulating expression.

1.177 By analogy with *Lingens* the argument can certainly be made that the publication of information which is of a private nature but which also has some connection to the public sphere enjoys a similarly enhanced latitude with respect to publication. In addition, or in the alternative, it may be asserted that persons having a certain status in (or who are sufficiently close to) the political/public sphere must forebear a greater than normal level of criticism which might include disclosure of information dealing with aspects of their private lives. How valid are these assertions?

114

(1986) 8 EHRR 407 at para 38.

1.178 Take the "information" issue first. The ruling in *Lingens* seems to postulate an elusive line between matters that are colourably political (including matters that are not political in the conventional sense but may be otherwise in the public interest) as against all other matters. Only the former gets the benefit of the ruling. This begs the question whether information about purely private and personal matters is, or can ever be, in the political domain or of relevance to the political domain. There is a continuum of possible views on this.

1.179 At one end of the continuum it is possible to hold that purely private information relating to an individual's personal life is just that. That is, it has no natural or logical relationship to the public sphere. German law, by way of example, reflects this view, in part at least, by insisting on the absolute inviolability (and non-disclosure) of the person's "intimate sphere" (see Chapter 6).

1.180 At the other end of the continuum it might be asserted that there is no such thing as a hermetically-sealed private sphere. Everything private has some broader social or political implication. People do not come pre-packaged into public and private. It might be maintained, by way of example, that marital infidelity goes to one's trustworthiness in general which has obvious implications regarding a capacity to hold position of trust or public office.

1.181 The motivation behind the first approach ("what's private is private") is certainly consistent with the thrust of Article 8. Taking privacy seriously must mean starting with a strong working assumption that private matter is only of purely private concern. That does not necessarily mean, however, that the working assumption cannot be departed from for just cause. It follows that although the public/private divide holds solid, an opening should arguably be allowed for isolated occasions when purely private information might also be of direct relevance in the public sphere. Such an eventuality might appear quite rare but it would seem entirely right in principle to make allowances for it nonetheless. Once the semi-permeability of the public/private line is acknowledged then the focus of attention shifts to the nature of the *nexus* needed to be established in order to bring "private" matter over the line into the public realm. Emphasis might also shift to safeguards and limiting principles such as ensuring proportionality in the degree and depth of private information disclosed. This is so since the disclosure of private information is an exception to the right of privacy and must therefore be construed narrowly. Proportionality would seem to point strongly against the publication of excessive detail that goes above and beyond what is reasonably necessary to respond to a genuine public interest.

1.182 As a matter of principle and consistent with both Articles 8 and 10 (especially as the latter is interpreted in *Lingens*) it would appear defensible to insist on a hard public/private divide but to carve out some space in which to allow for arguments that information of a private nature has some close nexus to the public sphere. It would also appear consistent with Article 8 to place an onus on those who

would make this claim to come forward with convincing proof. We believe that the "public interest" defence we now recommend would create this space and thus satisfy the *Lingens* ruling in as much as its rationale could be applied, by way of analogy, to information of a private kind.

1.183 The second approach ("everything private is public") is much less plausible. To claim that everything private is public is to break down the very public/private divide that human rights are designed to preserve. While it may be superficially attractive to assume that everything private is public or always has disclosable implications for the public sphere, to do so is to deny one of the basic rationales of privacy which is to carve out a space for self-reflection and for the possibility for self-transformation. Treating people as ends in themselves must have some implications for how we draw the public/private divide. Personal space - which is vital to personal ease, emotional release, and the dynamics of personal growth and autonomy - is gone if the assumption that whatever is private is public is made.

1.184 With respect to the question of "status" a number of important questions arise. What status counts? Does a person having the requisite status automatically lose all privacy rights? Must the information disclosed bear some demonstrable connection to that person's function in public life or is all private information disclosable simply on account of status? Is there some point at which the disclosure of excessive detail brings the publication over the line where the benefit of the public interest is lost?

1.185 It would appear wrong in principle to make the existence and applicability of the right to private life dependent entirely upon status. That would seem to usher in a new Feudalism that is at odds with the notion of equal human rights. The better view is that status functions not to deny rights but to qualify them. Furthermore, it seems reasonable to deduce that it is not status *simpliciter* but the *presumed* connection between the status of a person and political or public affairs that counts. If it is the presumed *connection* that counts then it follows that not all aspects of private life are equally qualified by status but only those that have a *direct or colourable bearing* on a persons' function in public life. If a person voluntarily assumes a certain status in public life then it is fair to deduce that he has laid aspects of his private life that are relevant to his public life open to more scrutiny than normal. But this is quite different to the assertion that public status equates with a *carte blanche*.

1.186 In sum, *Lingens* does not appear to create a *carte blanche* with respect to all aspects of a public figure's private life. Article 8 acts as a constraint on Article 10 except where information of a private nature has some provable connection to a person's public function. If the information in question bears directly on his or her fitness for public office or performance in public office then it would appear fully in

keeping with the democratic rationale in cases like *Lingens* to allow for greater disclosure than normal.

1.187 We believe that the "public interest" defence which we recommend and which specifically embraces the exposure of criminality and other private matters that go directly to a person's capacity to perform the functions of public office represents a principled and practical way of marrying the legitimate concerns of Articles 8 and 10.

1.188 It must always be borne in mind that our aim is to protect aspects of private life from public scrutiny. We do not see private life as a subterfuge with which to hide information that is of relevance to public office or competence. Such information would be fully disclosable under our "public interest" defence.

(iii) *Does the Latitude allowed for "Political Speech" have any Implications for the News-Gathering Process ?*

1.189 The question next arises whether, in addition to creating an enhanced latitude for publication, Article 10 also creates an enhanced latitude for news-gathering activities, particularly where these activities are governed by the extant positive law dealing, for example, with the interception of telecommunications. Put another way, is there a limit derivable from Article 10 on whether or how States can regulate news-gathering activities? Is there something special about news-gathering that justifies applying the extant law differently in this sector? If so, should any new law governing, for example, surveillance, carve out appropriate exceptions (or otherwise relax its strict application) when it comes to news-gathering activities?

1.190 Here, in a sense, we are working backward from the secondary level of intrusion (publication) to the primary level of intrusion (privacy-intrusive acts of surveillance). The argument is that an enhanced latitude to publish private matter under, for example, the "public interest" defence, generates a knock-on effect with respect to liability for particular acts of intrusion.

1.191 There are two general views on this. On the one hand, opening up latitude to publish on a theory that the information supplied helps to enhance democratic life calls for a holistic appraisal of the environment in which the media work. It follows that a like solicitude should be shown for the process by which information is obtained and processed. Otherwise, information might not come into the possession of the media and, through publication, to the attention of the public to the detriment of all in democratic society. On this view, and as a matter of strict logic, any enhanced latitude to publish must have at least some implications for enhancing the latitude to gather information.

1.192 On the other hand, it could be maintained that Article 10 is *sui generis* to expression. Since it deals only with expression it has no necessary implications for particular acts of news-gathering. To allow it to do so, no matter how logical, is to place undue strain on the notion of one law applicable to all without any special dispensations and thus bring the rule of law itself into disrepute. It might even be asserted that a countervailing "public interest" comes into play at this point which concerns the necessity for upholding and maintaining respect for the "rule of law".

1.193 The Court appears to be steering a difficult and uneasy middle course between the above options. One case of relevance is *Jersild v Denmark*¹¹⁵. This case concerned the imposition of criminal sanctions under Danish law against a journalist for having commissioned, produced and broadcast a television talk show in which several members of the panel engaged in racist speech - speech that violated the "rights of others" bearing in mind particularly the relevant terms of the UN Convention on the Elimination of all forms of Racial Discrimination (CERD). The Court found against Denmark on the basis that it was inappropriate and disproportionate to effectively target the messenger rather than the message. The Court reiterated its view that the duties and responsibilities (and therefore the latitude to regulate) depended in part on the impact of the media in question (e.g., press, TV)¹¹⁶ and that very careful scrutiny was called for in cases of restrictions on the media given its watchdog role in democratic society¹¹⁷. The Court was particularly keen to protect the prerogative of journalists to choose their methods of reportage and to engage in interviews. It stated:

"It is not for this Court, nor for the national courts for that matter, to substitute their own views for those of the press as to what *technique of reporting* should be adopted by journalists. In this context the Court recalls that Article 10 protects not only the substance of the ideas and information expressed, but also the form in which they are conveyed."¹¹⁸

It continued:

"The punishment of a journalist for assisting in the dissemination of statements made by another person in an interview would seriously hamper the contribution of the press to *discussion of matters of public interest and should not be envisaged unless there are particularly strong reasons for doing so*."¹¹⁹

115 (1995) 19 EHRR 1.

116 *Ibid.* at para 31.

117 *Ibid.* at para 34.

118 *Ibid.* at para 31.

119 *Ibid.* at para 35 [emphasis added].

1.194 It is noteworthy that the speech in question related unquestionably to a matter of public concern or importance - namely, immigration and race. The *Jersild* decision is fully in keeping with the *Lingens*¹²⁰ approach which values toleration toward even critical speech on a matter of political or public concern. It does not, however, extend the *Lingens* rationale to embrace (and curtail) privacy. To do that one would have to draw a link between private material and public issues - which is largely (though not totally) a contradiction in terms. More importantly, although the Court emphasised that the *methods of reporting* are for the journalist alone to decide, it did not address the question of whether a journalist has a right to break the extant positive law in gathering information. There is, in other words, a difference between choosing a method of reporting on the one hand and engaging in a series of acts to gather information on the other. Although the spirit of the judgment is itself quite broad the actual ruling in *Jersild* does not colourably reach the latter issue.

1.195 Another important case of relevance under this heading is *Goodwin v UK*¹²¹. This case concerned the imposition of potential penalties against a journalist for refusing to name the source of damaging leaks from a company. In holding against the UK the Commission stated in an important passage that it

*"considers that protection of the sources from which journalists derive information is an essential means of enabling the press to perform its important function of "public watchdog" in a democratic society. If journalists could be compelled to reveal their sources, this would make it more difficult for them to obtain information and, as a consequence, to inform the public about matters of public interest. The right to freedom of expression ... requires that any such compulsion [to disclose sources] must be limited to exceptional circumstances where vital public or individual interests are at stake*¹²²."

1.196 In a sense, the Commission opted to view freedom of expression holistically. It had its eye on ancillary supports or rights to *enable* the press to perform its primary task as watchdog in democratic society. Though the Commission enunciated a very strong assumption that the privilege serves an undifferentiated public interest it did not completely rule out compulsion to disclose.

1.197 The Commission's Opinion was not unanimous. In his dissenting opinion, Commissioner Trechsel (with whom five Commissioners agreed) stated:

120 (1986) 8 EHRR 407.

121 (1998) 22 EHRR 123. On the subsequent handling of similar cases in the British courts see S Foster, English Judges and the Spirit of the Convention, *New Law Journal*, September 12, 1997, pp1306-7.

122 Opinion of the Commission, 22 EHRR 123 at para 64 [emphasis added].

"[t]his legitimate interest [in protecting journalistic sources] may enter into conflict with other legitimate interests *such as the protection of private life*...In my view the majority of the Commission has given too much weight to the interest of a journalist in protecting his sources as an element of freedom of expression. I am of the opinion, having regard to the duties and responsibilities referred to in Article 10, that the protection of a journalist's sources is only justified in cases where the disclosure of confidential information clearly serves a public interest. *In cases where, for example, an abuse of office, corruption or any other perversion of private or public power is in issue, the journalist should not be compelled to disclose his sources*¹²³."

1.198 In Trechsel's view the privilege did have a place which should be more carefully tied to instances where the public interest was clearly at stake. In other words, he would not allow for the assumption that the public interest rationale was engaged without more. Due account had to be taken on this view of competing rights such as private life. Space, in his view, should only be left for the protection of sources where a public interest could clearly be served.

1.199 The Commission and applicant argued before the Court that the information was newsworthy even though it did not reveal matters of vital public interest. They thus sought to widen the notion of "political expression" or matters of "public interest" to include mere newsworthy items. The Court gave no express ruling on this point and it seems at least plausible to assume that there is no simple, easy or unquestioning equation of newsworthiness with "public interest" under Article 10. The fact that an item is newsworthy might, of course, count as weighty evidence that the public interest is in fact engaged.

1.200 In its judgment the Court recalled its case law on the importance of freedom of expression in democratic society. It stated that the protection of journalistic sources was "one of the *basic conditions* for press freedom":

"Without such protection, sources may be deterred from assisting the press in informing the public *on matters of public interest*. As a result the vital public watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10...unless it is justified by an overriding requirement in the public interest¹²⁴."

123 (1996) 22 EHRR 123 at 138-9 [emphasis added].

124 *Ibid.* at para 39 [emphasis added].

1.201 The Court closely scrutinised the averred justification (protecting the "rights of others" - in this case, the economic interests of a company) and found the compulsory disclosure involved in this case to be disproportionate to the end sought to be achieved. In the Court's view, the chief interests of the company had already been adequately catered for by the issuance of a prior injunction against disclosure and no additional justification could be found for compulsory disclosure as a means of reinforcing the injunction. On its face, the argument that an order for disclosure was necessary to protect the company against future damaging disclosures seemed strong although it was ultimately rejected by the Court. Interestingly, the question of the compatibility of the grant of the previous injunction (which is a form of prior restraint) was not in itself an issue and did not draw adverse comment.

1.202 The joint dissenting opinion of Judge Rysdal (President of the Court) *et al*, evaluated favourably the adequacy of the presumption against disclosure already present in British law. That law provided for compulsory disclosure only in cases where its necessity was clearly established on the basis of four indicators that went to matters of public concern. He found the test of "necessity" under British law to be broadly similar to that required or implicit under Article 10(2). Furthermore, he did not view the order for disclosure as merely "reinforcing" the interim injunction but as a necessary additional measure to plug the gaps left by the injunction which, if left unplugged, could result in serious economic harm to the interests of the company. He stated:

"No detailed assessment of these interests [of the company in obtaining comprehensive protection through an order for disclosure] is however, undertaken [in the majority judgment] and in the absence of it there is no satisfactory basis for the balancing exercise which the Court is required to undertake¹²⁵."

1.203 In a separate dissenting opinion Judge Walsh dissented on the basis that the new "privilege" announced by the Court effectively placed the press in a different category compared to the rest of society. This, he noted, was despite the initial observation of counsel for the applicant that his client was "claiming no special privilege by virtue of his profession because journalists are not above the law"¹²⁶. Furthermore, the majority judgment in Judge Walsh's view seemed to give the press, in virtue of its status, the right effectively to determine when the "public interest" is best served. In Judge Walsh's view:

125 *ibid.* at p151 para 10.

126 *ibid.* at p151, para 1.

"There is thus a breach of a primary rule of natural justice - no man is to be the judge of his own cause¹²⁷."

1.204 What are the implications of *Goodwin* for the kind of legislation we recommend? Even on its face the judgment does not create an absolute right to refuse to disclose sources. The formula used by the Court does not foreclose a reasoned balancing exercise of the privilege against other competing rights. What it does achieve is to inflate the value of expression in any inevitable balancing equation out of deference to the democratic rationale for speech. This does not completely preclude the possibility that at some point the legitimate public interest in freedom from disclosure may be overborne by a countervailing public interest in protecting or advancing other Convention rights at least under certain circumstances. The judgment says nothing directly about the value to be placed on privacy as such and whether (or under what circumstances) it might be considered important enough to cancel or qualify the new privilege. Furthermore, the new privilege itself does not carry forward to liability for particular acts of news gathering that may infringe the extant law.

1.205 It would therefore appear reasonable to assume that the Court in *Goodwin* did not intend to open up a plenary or broad privilege that is wholly insensitive to competing rights and interests. *Goodwin* did not involve balancing freedom of expression with vital aspects of a person's private life. It furthermore seems reasonable to assume that the Court will revert to a more traditional form of balancing analysis in a suitable case. That is not to say that weighty reasons for forcing disclosure of sources will not be required. They clearly will. The true force of *Goodwin* will be to place a very heavy onus on States to justify laws forcing disclosure. We believe that the law which we recommend would be justifiable given the extremely perishable nature of privacy, the fact that disclosure need not take place in open court and that the defendants have the right to publish if there has been no complicity in obtaining the material illegally and it is otherwise in the "public interest" to do so.

1.206 The full implications of the *Goodwin* ruling will doubtless require further litigation. However, it seems to us that the argument from strict logic for an extension of the latitude to publish to encompass a broad latitude to gather information cannot be carried to its own logical conclusion. It will sooner or later bump up against the rule of law as well as the fact that Article 10 is itself focused on expression with inherently limited radiation effect on all acts preparatory to publication.

127 *Ibid.* at p26, para 3.

(iv) *Are Prior Restraints on Expression Inherently Violative of Article 10?*

1.207 Interestingly, and despite its solicitude toward political speech and the press, the Court has not taken the step of denouncing "prior restraints" as an inherent violation of Article 10. Its approach is somewhat more permissive and nuanced. It stated in *Observer & Guardian v. UK*¹²⁸ that

"For the avoidance of doubt... the Court... [finds] that Article 10 of the Convention does not in terms prohibit the imposition of prior restraints on publication. This is evidenced not only by the words "conditions", "restrictions", "preventing" and "prevention" which appear in that provision, but also by the [Court's] *Sunday Times* judgment...."¹²⁹

The Court did add that

"the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the Court. This is especially so as far as the press is concerned, for news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest"¹³⁰.

1.208 In short, States are not debarred from using prior restraints but will be subject to very close scrutiny if they do so.

1.209 Three factors fortify us in our view that the privacy orders which we recommend (and which do constitute a form of prior restraint) would pass muster under the Convention.

1.210 First of all, it would appear that States have a positive obligation under Article 8 to regulate private behavior in cases where it potentially threatens private life. It is our view that the emphasis on prevention rather than compensation makes the injunctive remedy an integral aspect of an effective legal regime protecting privacy.

1.211 Secondly, private life is an equally, if not more, perishable commodity as expression. An invasion of privacy cannot easily be undone. A temporary ban on publication can always be lifted if found unjustified in the fullness of legal proceedings where adequate space is provided to debate the application of the public

128 Judgment of the Court, (1992) 14 EHRR 153.

129 *Ibid.* at para 60. See the partly dissenting opinion of Judge De Meyer *et al* who, quoting Justice Black of the US Supreme Court, viewed prior restraints as an inherent violation of Article 10: (1992) 14 EHRR 153 at 206n.

130 *Ibid.* at para 60.

interest defence. No one outlet need suffer a competitive disadvantage if the law is applied evenhandedly to all. Even if States do not bear a positive obligation under Article 8 it can still be strongly argued that Ireland would be acting within its margin of appreciation under Article 10 in providing for limited prior restraints for the sake of protecting private life.

1.212 Thirdly, we expressly provide that even a temporary injunction may be refused if the defendant claims a good arguable defence in the public interest. This should tip the balance favourably toward freedom of expression and allow injunctions to latch onto serious invasions of privacy (arising out of surveillance) where no good arguable defence related to the public interest arises.

Annex II

EVOLUTION OF THE PRIVACY DEBATE IN THE UNITED KINGDOM

1. Introduction

Part 1 - Reports, Private Members' Bills and the Opinion of the Lord Chancellor.

2. The Privacy Issue from 1948-1972
3. The Younger Report, 1972
4. Report of Calcutt I, 1990
5. Report of Calcutt II, 1993
6. Report of National Heritage Committee, 1993
7. The Lord Chancellors' Consultation Paper on the need for a Statutory Tort of Privacy, 1993

Part 2 - Government Responses

8. Conservative Government Response, 1995
9. The Issue under the New Labour Government, 1997-
10. Conclusions

1. Introduction

2.1 The general surveillance issue has seldom been viewed in isolation in the UK. Apart altogether from the specialised topics of police surveillance, CCTV codes of practice and the interception of telecommunications,¹ the general issue of surveillance has always been approached in the much broader context of media intrusions. It was in this peculiar context that there developed a consciousness of the problem posed by surveillance. Perhaps, it is because of this context that the arguments for privacy legislation against the general threats posed by surveillance have become subsumed in separate but related arguments about the role of the media in democratic society.

2.2 It follows that in order to understand the debate about surveillance it is necessary to briefly outline the contours of the more general privacy debate in the UK.

Part 1 - Reports, Private Members' Bills and the Opinion of the Lord Chancellor

2. The Privacy Issue from 1948-1972

2.3 The general privacy issue as it pertains to the media has received extensive official attention in the UK. There have been three Royal Commissions dealing with various aspects of the media including privacy;

Royal Commission on the Press, 1949 (Ross Report);²

Royal Commission on the Press, 1962 (Shawcross Report);³

Royal Commission on the Press, 1977 (McGregor Report).⁴

2.4 These Royal Commissions did not dwell specifically on the threat posed by surveillance. The Ross Report of 1948 recommended self-regulation for the media, the establishment of a Press Council and the promulgation of code dealing with the highest journalistic standards. Inaccuracy and sensationalisation figured prominently in that report but not privacy.⁵ The Shawcross Report looked more to the economic

1 These issues were broached in our Consultation Paper and touched on in chapter 6 of this Report.

2 Cmnd. 7700 (June 1949).

3 Cmnd. 1811 (September 1962).

4 Cmnd. 6810 (July 1977).

5 Ch. XIII, *The Performance of the Press* (2).

and financial environment within which the press functioned. Likewise the McGregor Report looked to economic issues in the main.

2.5 A Press Council was eventually established in 1952-53 partly as a result of a Private Member's Bill introduced in 1952. The objects of the original Press Council were fourfold (as originally recommended by the Ross Commission);

- i. To preserve the established freedom of the British Press.
- ii. To maintain the character of the British Press in accordance with the highest professional and commercial standards.
- iii. To consider complaints about the conduct of the Press or the conduct of organisations towards the Press; to deal with these complaints in whatever manner might seem practical and appropriate and record resultant action.
- iv. To keep under review developments likely to restrict the supply of information of public interest and importance.

2.6 As is plain from the above the remit of the Press Council was quite broad. However, the Press Council was largely perceived as ineffective in handling complaints and was eventually replaced in 1992 by a Press Complaints Commission (PCC).

3. The Younger Report, 1972

2.7 In 1967 the Nordic section of the International Commission of Jurists (ICJ) held a major conference on the subject of privacy and the media in Stockholm. The Conference Conclusions defined privacy as follows:

The right of the individual to lead his own life protected against: (a) interferences with his private, family and home life; (b) interference with his physical or mental integrity or his moral and intellectual freedom; (c) attacks on his honour and reputation; (d) being placed in a false light; (e) the disclosure of irrelevant or embarrassing facts relating to his private life; (f) the use of his name, identify or likeness; (g) spying, prying, watching and besetting; (h) interference with his correspondence; (i) misuse of his private communications, written or oral; (j) disclosure of information given or received by him in circumstances of professional confidence⁶.

6 Conference Conclusions, para. 2.

The general definition was stated to include

- ...
- (iv) untrue or irrelevant embarrassing statements about a person;
- ...
- (vii) use of electronic surveillance or other "bugging" devices;
- ...
- (viii) recording, photographing or filming;
- ...
- (x) public disclosures of private facts;
- ...
- (xii) harassing a person (e.g., watching and besetting him or subjecting him to nuisance calls on the telephone)⁷.

2.8 The Report of the Nordic Conference prompted an influential report by JUSTICE (which is the British section of the ICJ) in 1970⁸. The 1970 JUSTICE report contained a draft Right of Privacy Bill⁹ which, in turn, inspired the introduction of a Private Members' Bill.

2.9 The official response by the Home Secretary of the day was to set up a committee of enquiry chaired by Kenneth Younger. Its report was the first notable official report in recent times on the subject: *Report of the Committee on Privacy, 1972* (commonly referred to as the "Younger Report")¹⁰.

2.10 Among the many notable features of the Younger Report were the following. First, Younger was quite unsure whether there was a privacy problem at least with respect to media intrusion¹¹. Secondly, Younger rejected the introduction a general tort of privacy as being incapable of sufficiently exact and clear expression (paras. 33-44). Such a tort was also rejected as it went against the grain of English tort law which was to target the unsocial behaviour of the defendant (something that was discrete and relatively easy to define) rather than announce and protect general rights of the plaintiff. Thirdly, Younger focused on many different "sources" of the privacy problem and purported to tackle each of them individually. The threat posed by surveillance devices was a major focus of the Report (Chapter 19) and Younger went on to recommend discrete criminal offences directed at socially unacceptable uses of such devices where the expectation of privacy was at its highest (i.e., on private property). Fourthly, Younger did make an ancillary recommendation that the publication of material obtained by the unlawful use of such devices should itself be

7 Conference Conclusions, para. 3.

8 A Report by JUSTICE: *Privacy and the Law* (1970).

9 For text see Appendix J of the 1970 Report.

10 Cmnd. 5012, July 1970.

11 A survey of public opinion was in fact commissioned by Younger.

tortious (para. 565). Lastly, Younger recommended that the respective Law Commissions of England/Wales and Scotland should be asked by the Government to take a closer look at the law of confidence.

2.11 The Younger Report was not unanimous. Two trenchant, short and well reasoned minority reports were issued by A W Lyon and D M Ross¹². These two minority reports dissented from the majority view that a civil tort was unnecessary and impracticable. On the contrary, the dissenters felt that privacy is quite capable of sufficiently exact definition for the purposes of civil law. Ross went on to point out that, in his view, the absence of such a law would render the UK's international human rights commitments a "sham"¹³.

2.12 The debate about the adequacy of the law of confidence was duly taken up by the Law Commission and by the Scottish Law Commission as suggested by Younger. The English Law Commission reported on this topic in 1981¹⁴ and the Scottish Law Commission in 1984¹⁵. Younger's main recommendations were not, however, acted on by the Government.

4. The Calcutt I Report, 1990

2.13 Several Private Member's Bills were presented to Parliament throughout the 1980s. The most prominent of these were the *Right of Privacy Bill* (William Cash, MP, 1987-1988) and the *Protection of Privacy Bill* (John Browne, 1988-1989). John Browne's Bill made great progress through Parliament and was only dropped when the Government announced the establishment of a committee of enquiry: *Committee on Privacy and Related Matters*. This committee was established in July 1989 under the chair of David Calcutt and reported to the Home Secretary in June 1990¹⁶ (the report of which is commonly referred to as Calcutt I).

2.14 Unlike Younger, Calcutt's report was unanimous. The Calcutt I committee did not confine itself to intrusion by publication. It also covered intrusion by certain news-gathering methods deemed highly objectionable. Indeed, the regulation of these specific acts through criminal law became the dominant focus of Calcutt I until self-regulation in the media was given one final chance to prove itself.

2.15 Among the many notable features of Calcutt I are the following.

12 At p. 208-215.

13 *Ibid.* at 213

14 The Law Commission, *Breach of Confidence*, Law. Com. No. 110, October, 1981 (Cmnd. 8388).

15 Scottish Law Commission, *Breach of Confidence*, December 1984 (Cmnd. 9385).

16 Home Office: *Report of the Committee on Privacy and Related Matters*, June 1990 (Cmnd. 1102).

2.16 First, unlike Younger, Calcutt felt that a general privacy tort could be enacted with sufficient clarity and with appropriate sensitivity to the legitimate concerns of the media (para. 12.17). On the other hand, Calcutt simply wasn't convinced that there was a need for such a general law at that point in time. The issue was treated as (temporarily) moot. As will be seen, Calcutt changed his mind on this issue later and in light of subsequent events.

2.17 Secondly, Calcutt rejected a tort of harassment not out of principle but because he wasn't sure of its practicability in the context of group harassment and much preferred criminal sanctions since it afforded greater immediate relief (para. 6.25).

2.18 Thirdly, Calcutt focused on particular forms of information-gathering activities. Like Younger, Calcutt proposed a series of criminal offences all aimed at aspects of privacy whilst on private property (territorial privacy) such as

- (a) entering private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to 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.

[para. 6.33].

He proposed three defences as follows:

- (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 authority¹⁷.

2.19 Calcutt did not recommend that publication achieved as a result of the commission of these offences should itself be an offence¹⁸. Instead he

17 Para. 6.35.

18 Para 6.37.

recommended that publication obtained in such a manner as to violate the criminal law (as broadened) should be a statutory right of action¹⁹.

2.20 Fourthly, Calcutt recommended that the press be given one last chance to show that it could regulate the behaviour of its members and provide adequate remedies for breaches of privacy. He recommended the disbandment of the Press Council and the establishment of an independent Press Complaints Commission (PCC). If, after an appropriate period of probation, the PCC was shown not to work, Calcutt recommended that it be replaced with a statutory Press Complaints Tribunal. Two triggers were identified as justifying the move from a Commission to a Tribunal; (1) failure to establish the Press Complaints Commission on the terms recommended, and (2) that the system itself proved incapable of halting abuses (para. 16.10-12). The replacement Tribunal was to have powers to award compensation (para. 16.16) and to restrain publication (para. 16.17). In order to "avoid possible abuse of this provision" Calcutt recommended that no injunction should issue where the publisher (or intending publisher) could show that he had a good arguable case corresponding to the suggested defences including a public interest defence (par. 16.17). Calcutt was aware of the overlap between the powers of the Tribunal and those normally reserved to courts. To try to handle this he recommended that applicants to the Tribunal would have to waive their legal rights before taking a complaint to the new body.

2.21 Calcutt I was warmly welcomed by both Government and Opposition. The Press Council was duly disbanded. The proposed Press Complaints Commission (PCC) came into being in January 1991. Its terms of reference, in contrast to those of the original Press Council, gave prominence to the expeditious handling of complaints. Its first chair was Mr McGregor. A "last chance" before the enactment of a civil tort of privacy was famously and officially given to the press by David Mellor MP (then Home Secretary) who promised to review the workings of a non-statutory Commission after 18 months of its existence. The new PCC quickly established its Code of Practice. The following provisions of its original Code relate directly to privacy.

4. Privacy

- (i) Intrusions and enquiries into an individual's private life without his or her consent, including the use of long-range photography to take pictures of people on private property, without their consent, are only acceptable when it can be shown that these are, or are reasonable believed to be, in the public interest.

- (ii) Publication of material obtained under (i) above is only justified when the facts show that the public interest is served.

Note - Private property is defined as (i) any private residence, together with its garden and outbuildings, but excluding any adjacent fields or parkland and the surrounding parts of the property within the unaided view of passers-by, (ii) hotel bedrooms (but not other areas in a hotel) and (iii) those parts of a hospital or nursing home where patients are treated or accommodated.

5. Listening Devices

Unless justified by the public interest, journalists should not obtain or publish material obtained by using clandestine listening devices or by intercepting private telephone conversations.

...

8. Harassment

- (i) Journalists should neither obtain nor seek to obtain information or pictures through intimidation or harassment.
- (ii) Unless their enquiries are in the public interest, journalists should not photograph individuals on private property (as defined in the note to Clause 4) without their consent; should not persist in telephoning or questioning them after having been asked to desist; should not remain on property after having been asked to leave and should not follow them.
- (iii) It is the responsibility of editors to ensure that these requirements are carried out.

...

18. The Public Interest

Clauses 4, 5, 7, 8, and 9 create exceptions which may be covered by invoking the public interest. For the purpose of this Code that is most easily defined as -

- (i) Detecting or exposing crime or a serious misdemeanour.
- (ii) Protecting public health and safety.
- (iii) Preventing the public from being misled by some statement or action of an individual or organisation. In any cases raising issues beyond these three definitions the Press Complaints Commission will require a full explanation by the editor of the publication involved, seeking to demonstrate how the public interest was served.

2.22 The following observations on the above provisions are noteworthy. First of all, territorial privacy is accentuated in Clause 4. Property is defined narrowly and

in a way that is dispositive of the entire privacy claim. Secondly, intrusions can be justified in the public interest. A reasonable belief that publication is in the public interest is enough. Clause 18 was not clear as to whether some notion of proportionality tempers the public interest. Thirdly, Clause 5 which deals with listening devices seems to imply an exception to the existing law on the interception of communications. Fourthly, the ban against persistent telephoning and questioning under Clause 8 (ii) is phrased in such a way as to place an onus on the plaintiff to call a halt to these activities before the ban becomes effective.

5. The Calcutt II Report, 1993

2.23 Yet another Private Member's Bill was introduced in 1992 with the aim of setting up the Statutory Tribunal mooted by Calcutt I (Clive Soley MP, 1992: *Freedom and Responsibility of the Press Bill*). It failed at its Third Reading.

2.24 At the end of the probation period for the Press Complaints Commission Sir David Calcutt was invited back by the then Secretary of State for National Heritage to review the adequacy of press self-regulation. This entailed an evaluation of how well the Press Complaints Commission had performed and led to the report commonly known as Calcutt II which was issued in January 1993 (*Review of Press Self-Regulation*²⁰). For a variety of reasons, Calcutt II found the Commission system wholly inadequate²¹. He specifically recommended the following.

2.25 First, he recommended that the Statutory Press Complaints Tribunal, which had been outlined in Calcutt I as a fall-back option, should be set up immediately with the power to award compensation, issue fines and restrain publication (chapter 6).

2.26 Secondly he reiterated the recommendations made in Calcutt I (at para. 6.33) with respect to the enactment of criminal offences and added certain modifications (para. 7.4). Perhaps the most important modification was that the suggested offence relating to the taking of a photograph should be extended to cover situations where the person taking the photograph is not himself placed on private property (7.14). This would capture long-range photography taken from a public place onto a private place. Calcutt II added two new defences. First, on the basis of the provisions of a draft Code of Practice for the Press already set out in an annex to Calcutt I (Appendix Q) he proposed a new defence

20 Department of National Heritage: *Review of Press Self-Regulation*, Sir David Calcutt, January 1993 (Cmd. 2135).

21 See generally Calcutt II, chapter 5, 'Assessment of Self-Regulation'. See also Louis Bloom-Cooper & Lisa R. Prout, *Privacy Jurisprudence of the Press Complaints Commission*, [1994] *Anglo American Law Rev.* 133.

for the purposes of preventing the public from being misled by some public statement or action of the individual concerned²².

2.27 Thirdly, and in order not to impede the work of responsible investigative journalism, he recommended a new defence

for the purpose of informing the public about matters directly affecting the discharge of any public function of the individual concerned²³.

2.28 Fourthly, he reiterated the recommendation made in Calcutt I (at para. 6.36) that an injunction may be sought in the High Court, or damages awarded where the information had been obtained as a result of the criminal offences (para. 7.4).

2.29 Fifthly, he recommended that that the Government must now give active thought to enacting a general privacy tort (something his committee had earlier - and unanimously - found practicable but premature) (paras. 7.33-7.44). He felt that, although his terms of reference were confined to the press, the new tort should sweep more broadly.

2.30 In reaction the Government accepted in principle the need for new criminal offences to deal with physical intrusion and covert surveillance and agreed to give the matter further and serious consideration. The Government reserved its position as to a Statutory Press Complaints Tribunal until the National Heritage Committee had issued its report on the whole matter.

6. Report of the National Heritage Committee, 1993

2.31 The National Heritage Committee of the House of Commons (chaired by Gerald Kaufman MP) issued its own report on the matter in March 1993: *Privacy and Media Intrusion*²⁴. It had two overriding concerns; securing privacy for every citizen regardless of status and curtailing the use of invasive technology. Its remit was wider than Calcutt II - it embraced many different media outlets including the press.

2.32 The Committee received many written submissions and heard extensive oral evidence²⁵. It proclaimed itself unconvinced that the low number of complaints concerning privacy registered with the Press Complaints Commission was an accurate reflection of the number of breaches of the CPC's Code (para. 35). It felt that some

22 Para. 7.18.

23 Para. 7.20.

24 National Heritage Committee, Fourth Report, Vol. 1: *Privacy and Media Intrusions*, March 1993 (294-1).

25 For submissions see Vol. 2, Minutes of Evidence.

people may well feel inhibited to make a complaint in writing and that the absence of a telephone hot-line may make it difficult for private citizens to make their complaints at the most effective moment. It stated

"In addition, many people, as our witnesses made clear, will feel reluctant to prolong their trauma by making a complaint and they may also consider that as the PCC has no power to award compensation, however heinous the offence, there is no point in adding to their stress by pursuing a complaint."

[para. 35].

2.33 The Committee agreed with Calcutt II that the existing PCC was ineffective. However, it disagreed with Calcutt II as to the remedy. Specifically, the Committee did not view the idea of a statutory Press Complaints Tribunal with any favour. It stated

"Unless future events show such a tribunal to be utterly unavoidable, the Committee believes that it would be far preferable to rely initially on voluntary regulation by the press."

[para. 39].

2.34 Instead, the Committee recommended strengthening self-regulation. It wished to see the PCC replaced by a non-statutory Press Commission. It took issue with Calcutt who had argued that the PCC should concentrate on maintaining standards and not on broader issues dealing with press freedom. The Committee disagreed. It recommended that the Press Commission (as it preferred it to be called) should be charged specifically with the task of upholding press freedom. This would mark a reversion, of sorts, to the tasks set out for the Press Council in 1952.

2.35 Among the varied and technical recommendations with respect to the revamped Press Commission the Committee recommended that it should have the power to require compensation to be paid and fines to be imposed in cases of blatant violation of the Code (paras. 76-77).

2.36 Specific recommendations were also made with respect to strengthening the PCC Code.

2.37 The Committee also recommended the establishment of a statutory Press Ombudsman to handle complaints from people dissatisfied with the outcome of a Press Commission enquiry concerning alleged breaches of the Code (paras 94-107). This office was seen as an outer and independent layer of protection.

2.38 The thrust of the recommendations of the National Heritage Committee was to try to ensure that self-regulation works. However, and in a somewhat contradictory manner, the Committee went on to recommend the enactment of a *Protection of Privacy Bill* dealing with a tort of the infringement of privacy and specified criminal offences dealing with unauthorised use of surveillance and harassment (paras. 47-59). This is perhaps explained by the fact that the Committee viewed privacy broadly as embracing many more actors than the media. If so, then complaints regarding the media could be handled by the Press Commission and other complaints could be handled by the courts. The Report is not, however, clear on whether such a dual system was intended.

2.39 The main elements of the new tort were stated to include

- obtaining and/or publishing harmful or embarrassing personal material or photographs; or
- obtaining and/or publishing private information (e.g., medical records) or photographs without the permission of the person concerned or, where that person is not in a position to give permission, by his next of kin; or
- publishing inaccurate or misleading personal information; or
- violating the peace of another by intruding upon him, or persistently communicating with him²⁶.

2.40 The Committee mentioned a public interest defence to the above and did not specify whether the defence was confined to intrusion through publication or applied more broadly to all intrusions of privacy.

2.41 The Committee's recommendations with respect to the proposed criminal offences were as follows;

- placing a surveillance device on private property without the consent of the lawful occupant, with intent to obtain personal information;
- 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;
- taking a photograph, or recording the voice, of an individual who is on private property, without his consent to the taking or recording, with intent that the individual shall be identifiable;

26 Para. 48.

- publishing of a recording or an intimate photograph of an individual taken without consent;
- entering private property without the consent of the lawful occupant with intent to obtain personal information;
- the buying, selling or retention of any recording without the permission of the person on the tape; or of any material obtained through eavesdropping or use of long-range cameras where any of the parties was aware that the material was procured through illegal means or suspected it to be so obtained; and publication of any recording or material so obtained even where no financial transaction was involved.
- the deliberate interception of calls made on mobile phones.
- the enactment of a criminal offence of harassment or besetting²⁷.

The defences to the above were stated as follows:

- for the purpose of preventing, detecting or exposing the commission of any crime, or
- for the purpose of preventing the public from being harmfully misled by some public statement or action of the individual concerned; or
- for the purpose of informing the public about matters directly affecting the discharge of any public functions of the individual concerned; or
- for the protection of health or safety; or
- under any lawful authority²⁸.

2.42 The Committee recommended that prosecutions should be brought only with the consent of the DPP²⁹.

2.43 Significantly, recommendation no. viii made it explicitly clear that the "public interest" defence was to apply to acts (i.e., not merely publication) contrary to the new criminal offences.

2.44 Interestingly, the Committee was of the view that an expanded right to know - through freedom of information legislation - would take considerable pressure off journalists to produce reports using privacy-invasive means³⁰.

27 Para. 52.
 28 Para. 55.
 29 *Id.*
 30 Para. 44.

2.45 The Committee recommended that the Government should draw up a definition to cover the most potentially intrusive surveillance devices and should give urgent consideration to the desirability of either licensing or registering such devices (para. 57 & recommendation x). It also recommended that certain devices be limited to the use of the law enforcement agencies (recommendation xi).

2.46 The Committee recommended extending legal aid to cover actions under its proposed privacy legislation (recommendation xii). Ancillary recommendations had to do with editors' contracts of employment (to incorporate the PCC Code - recommendation xiv) and that greater use should be made of "readers representatives" (recommendation xv).

7. The Lord Chancellors' Consultation Paper on the need for a Statutory Tort of Privacy, 1993

2.47 In response to Calcutt II the Home Secretary charged the Lord Chancellors' Department (together with the Scottish Office) with the task of producing a consultation paper on the possible outline of a new general statutory tort of privacy. A Consultation Paper on that subject was duly issued in July 1993 (interestingly, with the acknowledged assistance of one of the Law Commissioners): *Infringement of Privacy - Consultation Paper*. In a remarkable paragraph the Consultation Paper states:

"[The Lord Chancellor's Office and the Scottish Office suggest]...that the time has now come, as a matter of principle, to recognise in law another such interest (besides those already protected by tort law) which...(belongs to the person)..., that aspect of personal integrity which we call privacy. The right of privacy should now be seen as sufficiently important to justify its recognition *per se* rather than leaving it to be dealt with piecemeal. The number of cases which will thereby arise is irrelevant to this issue: there are comparatively few actions for trespass to land and nuisance, but that does not mean that the interests which they protected should not be protected. On the other hand, it would not be the object of a new right to encourage litigation. Its presence on the statute book should have a deterrent effect."

[para. 3.13].

2.48 The Consultation Paper suggested a new tort along the following lines:

A natural person shall have a cause of action, in tort or delict, in respect of conduct which constitutes an infringement of his privacy, causing him substantial distress, provided such distress would also

have been suffered by a person of ordinary sensibilities in the circumstances of the complainant.

A natural person's privacy shall be taken to include matters appertaining to his health, personal communications, and family and personal relationships, and a right to be free from harassment and molestation.

The following defences, at least, shall be available in such proceedings: consent, lawful authority, absolute or qualified privilege, and a public interest defence.

[para. 5.22].

2.49 Submissions were invited as to a range of issues including; whether, as a matter of principle, privacy should receive protection under the law; whether the law should be allowed to develop in its own pace or whether legislation was necessary; whether the right, as such, should be enunciated, or whether particular breaches of it should be singled out in the legislation; whether harm must be established³¹; how privacy should be defined and how the types of infringement should be organized and defined; whether harassment and molestation should be incorporated (as was suggested); whether "false light" should be covered; whether appropriation of a person's identify should be covered; whether the basis for liability should be "intention", "recklessness" or "negligence" ("intention" was suggested).

2.50 With respect to the defences the Paper supported the idea of a public interest defence and stated that the problems of definition in this regard are not insuperable. Submissions were requested on how to phrase the "public interest" defence; as to the relationship between remedies for privacy and other civil remedies; whether an Ombudsman for press complaints should be established (as recommended by the Heritage Select Committee) and, if so, what relationship should exist between legal remedies and the "remedies" afforded by such an office. Regarding preventative injunctions submissions were invited as to the principle and also to the test that should apply; should it, e.g., be the same as in defamation where no injunction is awarded if the defendant can show a good arguable defence. The relevant part of the Lord Chancellor's Consultation Paper is worth quoting in this regard.

6.6. The JUSTICE report described the injunction as a valuable weapon and recommended that it should be available "particularly where there has been an infringement of privacy in obtaining information

31 The Paper suggested that cases should be limited to where persons have suffered harm in circumstances where a person of ordinary sensibilities would have suffered substantial distress (para. 5.9).

and there is a threat to publish". Indeed it may be said that unless a plaintiff can prevent an infringement by way of publication from taking place, the value of the [privacy] remedy is greatly reduced. As the Calcutt report said, such an injunction would be far more valuable than an apology or compensation after the infringement. It is suggested that it would be wholly unjust to plaintiffs if they were denied the possibility of preventing a potentially harmful publication.

6.7 However, representations were also made to the Calcutt committee to the effect that permitting such a restraint on the press would amount to an excessive restriction on the freedom of the press. It was suggested that the situation under a new law should be similar to that in defamation, where an interlocutory injunction will only be granted in the clearest circumstances; *if the defendant can show he has a good arguable defence he should not be prevented from publishing*. In *Bonard v. Perryman* the case which established this rule, reference was made to "the importance of leaving free speech unfettered".

[emphasis added].

2.51 The Consultation Paper was not sympathetic to extending legal aid to privacy cases. One year was suggested as the relevant period of limitation.

Part 2 - Government Responses

8. Conservative Government Response, 1995

2.52 The Government of the day issued a paper in July 1995 which rejected the proposals of the Heritage Select Committee and analysed the responses to the Lord Chancellors' Consultation Paper³². The Government did not contest the existence of a problem. This in itself was indicative of how far matters had developed since the earlier hesitation of the Younger committee on this point. However, the Government was simply not convinced that legislation was the answer. The Governments' response dealt in the main with three things;

1. the question of self-regulation or statutory regulation for the press,

³² *The Government's Response to the House of Commons National Heritage Select Committee: Privacy and Media Intrusion*, July 1995 (Cmnd. 2918).

2. the question of criminal law reforms,
3. the question of a new civil tort of privacy.

2.53 It dealt with the recommendations of Calcutt II and the National Heritage committee in separate chapters. Its overall attitude was contained in three early chapters dealing with the above issues. This effectively sealed the fate of Calcutt II and the National Heritage Committee.

2.54 As to the first issue the Government did not find that

the case for statutory measures in this area compelling. It believes that, in principle, industry self-regulation is much to be preferred. That conclusion applies equally to (Calcutt II as well as the National Heritage Committees's reports).

[para. 2.5.]

2.55 It went on to outline improvements already made to the PCC and encouraged more to take place (chapter 2).

2.26 As to criminal law the Government accepted the principle that certain forms of intrusion should be subject to the criminal law. Its ostensible problem was, however, in coming up with an acceptable legislative formula that adequately addressed the mischiefs in question and yet combined clarity with sufficient sensitivity to the legitimate pursuit of investigative journalism. It proceeded to point out particular difficulties in the formulae suggested by Calcutt and it concluded that the appropriate balance was not present in the formulae presented thus far. For its part, it did not expressly commit itself to the search for an appropriate formula (chapter 3).

2.57 As to the proposed civil tort the Government evaluated the submissions made to the Lord Chancellors' Consultation Paper. It noted that a large majority (including the judges) were against the idea of the judicial creation of such a tort. If it were to come into being it must be created under statute law. Most of the submissions that were given prominence in the Government's paper were negative as to the central question of legislation. The Government stated

"First, it does not believe there is sufficient public consensus on which to base statutory intervention in this area. Secondly, it strongly prefers the idea of self-regulation."

[para. 4.13].

2.58 The publication of the Government's response in 1995 marked a stalemate of sorts in the debate until the general election of May 1997.

9. The Issue Under the New Labour Government, 1997-.

2.59 The issue had been simmering away in academic journals and in the newspapers themselves. Distinguished judges and jurists such as Lord Bingham and David Eady Q.C. wrote eloquently about the need for a privacy law³³. Lord, Bingham, it will be recalled, was one of the judges sitting in *Kaye v Robertson*³⁴. Indeed, David Eady was a member of the first Calcutt committee.

2.60 The whole issue was given added impetus with the death of Diana, Princess of Wales, in late August 1997. Allegations, so far unfounded, have been made that the actions of some elements of the media (or at least connected with the media) led to, or contributed to, the circumstances leading to her death and the deaths of two others. Whether true or not, the whole episode seemed to galvanise public opinion against media intrusion and in favour of stricter controls. Eminent academics and media law practitioners joined the chorus for privacy-specific legislation including Professor Eric Barendt and Geoffrey Robertson Q.C.³⁵.

2.61 The Press Complaints Commission lost no time in promising to respond to the public outcry. It published general proposals for changes in its Code of Practice in late September 1997³⁶. The enhanced privacy provisions in the Code was ratified by the Commission on 26 November 1997 and came into effect on 1 January 1998. Among the more directly relevant provisions of the revised Code of are the following.

3. Privacy*

- (i) Everyone is entitled to respect for his or her private and family life, home, health, and correspondence. A publication will be expected to justify any intrusion into any individual's private life without consent.
- (ii) The use of long-lens photography to take pictures of people in private places without their consent is unacceptable.
Note: Private places are public or private property where there is a reasonable expectation of privacy.

33 Lord Bingham of Cornhill, *Opinion: Should There Be a Law to Protect Rights of Personal Privacy*, [1996] EHRLR Issue 5, 450; David Eady Q.C., *Opinion: A Statutory Right to Privacy*, 3 EHLR [1996] 243.

34 [1991] F.S.R. 62.

35 Eric Barendt, *End this Intrusion Now*, The Guardian September 24, 1997, at p.19; Geoffrey Robertson, *Press for a Legal Right to Inquire - but not to Intrude*, The Guardian, September 2, 1997 at p. 18.

36 Editorial, *Some Modest Proposals*, The Guardian, September 26, 1997 at p. 18. See also, *Pressing for Privacy: Paper Tiger Leaves Editors Purring*, The Guardian, September 26 1997 at p. 2.

4. Harassment*

- (i) Journalists and photographers must neither obtain nor seek to obtain information or pictures through intimidation, harassment or persistent pursuit.
- (ii) They must not photograph individuals in private places (as defined in clause 3 note) without their consent; must not persist in telephoning, questioning, pursuing or photographing individuals after having been asked to desist; must not remain on their property after having been asked to leave and must not follow them.
- (iii) Editors must ensure that those working for them comply with these requirements and must not publish material from other sources which does not meet these requirements.

5. Intrusion into Grief

- (i) In cases involving grief or shock, enquiries must be carried out and approaches made with sympathy and discretion. Publication must be handled sensitively, but this should not be interpreted as restricting the right to report judicial proceedings.

8. Listening Devices*

- (i) Journalists must not obtain or publish material obtained by clandestine listening devices or by intercepting private telephone conversations.

The Public Interest

There may be exceptions to clauses marked * where they can be demonstrated to be in the public interest.

1. The public interest includes:
 - (i) Detecting or exposing crime or a serious misdemeanour.
 - (ii) Protecting public health or safety.
 - (iii) Preventing the Public from being misled by some statement or action of an individual or organisation.
2. In any case where the public interest is invoked, the Press Complaints Commission will require a full explanation by the editor demonstrating how the public interest was served.
3. In cases involving children, editors must demonstrate an exceptional public interest to over-ride the normally paramount interests of the child.

2.62 The following changes from the original Code are noteworthy. First of all, property is no longer dispositive. What matters is not whether one is one private or

public property but whether one is in a private place which is defined as place where one has a "reasonable expectation" of privacy. Secondly, the responsibility of editors under Clause 4 (harassment) extends to encompass publication obtained through outside sources in circumstances where the Code has been violated. Thirdly, an onus is placed on the publisher to demonstrate how the public interest was served by publication. Lastly, it is to be noted that the interception of private telephone conversations still seems permissible under the Code if the public interest is served. This is cast in much broader terms that the defence of consent laid down under section 1(2)(b) of the *Interception of Communications Act 1995* and presumably must be read in light of it.

2.63 The revised Code was generally welcomed³⁷ but its publication did not still the debate for legislation.

2.64 Expectations for legislation were raised in particular by the campaign pledge made by the Labour Party before the May 1997 election to incorporate the European Convention on Human Rights into British Law. The new Government published its long awaited White Paper on this topic in October 1997³⁸. As of March 1998 the resulting Human Rights Bill is still going through Parliament. Even though by its own terms the Bill will not enable the courts to strike down legislation³⁹, the Lord Chancellor, Lord Irvine, and the Lord Chief Justice, Lord Bingham, are both of the view that the enactment of the Bill will potentially enable the British courts to fashion a right to privacy⁴⁰ with application as between private parties. Clause 6 of the Bill makes the its terms effective against "public authorities". The view is taken by some that this embraces the activities of the Press Complaints Commission and that therefore opens up an opportunity for the courts to review its operations and jurisprudence in light of Article 8. Lord Bingham's view is that since the courts are an arm of the state there would arise a "clear duty on the courts to protect privacy"⁴¹.

2.65 It is disputed whether the Press Complaints Commission was a public authority for the purposes of the Human Rights Bill. In any event, Lord Wakeham, the chair of the Press Complaints Commission moved an amendment to the Bill in the Lords to the effect that the PCC should not be considered a "public authority" and that its actions should therefore be unreviewable by the courts under the terms

37 See, however, *The Cook Affair: Roy Greenlade on the press ratting on their promises*, *The Guardian*, 13 January, 1998, at p. 15.

38 Home Office White Paper, *Human Rights Brought Home: The Human Rights Bill*, October 1997 (CM 3782).

39 See Clause 4 of the Bill which enables a court to make a declaration of incompatibility.

40 See Clare Dyer, *Top Judge Sees Courts as Arbiter of Privacy Rights*, *The Guardian*, 9 October 1997 at p.2.

41 *Id.*

of the Bill⁴². The Prime Minister was pressed in the Commons on 11 February 1998 by the Leader of the Opposition whether he accepted the judgment of the Lord Chancellor that the Human Rights Bill would lead to a privacy law. He replied:

No, it will not lead to a privacy law. The incorporation of the European Convention on Human Rights allows us to claim in this country what we would otherwise have to claim in Europe⁴³.

2.66 An arrangement was announced in the Commons by the Home Secretary, Jack Straw MP, on 16 February last⁴⁴. In debate the Home Secretary stated:

"We have repeatedly stated our support for the freedom of the media and our opposition to a statutory law of privacy. We do not believe that the Bill is contrary to that position. We do not believe that it will lead to the courts developing the common law in a way that will inhibit legitimate press investigations into matters of public interest. Nor do we believe that it will lead the courts to issue injunctions in respect of stories in which there is a public interest in publication⁴⁵."

2.67 Nevertheless he recognized that the press may well have fears that their freedom might be eroded unwittingly or gratuitously by the legislation. He revealed that he had been in consultation with Lord Wakeham about an appropriate way of copperfastening freedom of expression. He did not propose to meet this fear by amending Clause 6. Instead he proposed a framework of amendments comprising three elements.

2.68 The first element concerned an effective (though not a *de jure*) ban on *ex parte* injunctions. This would be done by insisting that no injunctive relief would be granted unless the respondent is either present or represented or unless the applicant has taken all practicable steps to alert the newspaper against which the application is brought. Secondly, he announced that a formula would be found to the effect that whenever a person applies for relief or a remedy on Article 8 grounds that relate to a claim for respect for private life and where the granting of that remedy would raise issues under Article 10 ECHR, the court must have *particular regard* to freedom of expression⁴⁶. This, it was said, would provide a useful signal and reminder to the

42 Speech of Lord Wakeham moving an amendment to the Human Rights Bill, House of Lords, Hansard, 24 November, 1997, col. 772.

43 Reply of Prime Minister, House of Commons, Hansard, 11 February, 1998, Col. 362.

44 Human Rights Bill, House of Lords, Hansard, 16 February 1997, col. 777.

45 House of Commons, Hansard, 16 February, 1998, Col. 776.

46 Even in the absence of this Clause the courts are under a general requirement to take into account the case law established under the Convention by the European Commission and Court on human Rights (Clause 2).

courts. Thirdly, a formula would be found to require the courts to take into account the public interest in publication, whether the newspaper had acted fairly and reasonably and whether it had complied with the provisions of the Press Complaints Commission's Code.

2.69 All of the above seems to implicitly concede that the British courts will now be able for the first time to treat claims of breaches of privacy by the media⁴⁷. The cumulative effect of the proposed changes by the Home Secretary might be to tilt the balance decisively or slightly (depending on how one reads the eventual statutory language) in favour of freedom of expression.

2.70 The Home Secretary was asked whether the amendments in question would amount to an alteration or attempted derogation from the Convention. In reply he pointed out that the tilt given to Article 10 in the Bill was fully consistent with the case law established by the European Court of Human Rights under the Convention. Interestingly, he cited the *Sunday Times* case as well as the case related to the publication of *Spycatcher* as authority for the proposition that the Strasbourg Court have afforded precedence to Article 10 over Article 8 when freedom of the press and of other is involved⁴⁸. This assertion is curious since neither of these two cases had anything to do specifically with the interrelationship between Article 10 and the right to respect for private life under Article 8. Indeed, as pointed out in Annex I, the European Court has yet to rule expressly and definitively on the interrelationship between Articles 8 and 10.

2.71 The approach taken by the Government under the Human Rights Bill mirrors that taken under proposed legislation to transpose the 1995 Data Protection Directive into British law. It will be recalled from chapter 3 of this Report that Article 9 of the Directive requires Member States to carve out exceptions for legitimate journalistic activity as appropriate. In fact clause 31 of the *Data Protection Bill, 1997* states that personal data which are processed only for special purposes are exempt from much of the principles secured by the Bill. These special purposes are stated to be

- (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material,
- (b) the data controller reasonably believes that, having regard in particular to the special importance of freedom of expression, publication would be in the public interest, and

47 See editorial, *Free at Last...But Now Read the Fine Print*, *The Guardian*, 18 February, 1998.

48 Speech of Home Secretary, House of Commons, Hansard, 16 February, 1998, Col.778. See *The Sunday Times v. United Kingdom*, 2 EHRR [1979] 245; *Observer and Guardian v. United Kingdom*, 14 EHRR [1992] 153.

- (c) the data controller reasonably believes that, in all the circumstances, compliance with the provision in question is incompatible with the special purposes.

2.72 Ireland must also consider this issue since the Directive must be transposed into Irish law by October 1998.

10. Conclusions

2.73 Most official reports since Younger - Calcutt I, Calcutt II, National Heritage Committee, Lord Chancellors' Consultation Paper and even the Government response in 1995 - accept the existence of a privacy problem in the context of the media. The issue of privacy-invasive surveillance has nearly always been approached in the UK from the perspective of the media.

2.74 All official reports since Younger accept the need for new criminal offences targeted on methods of information or news-gathering deemed repulsive. The view of the outgoing Government was sympathetic in principle but skeptical about the possibility of finding appropriate statutory language. The view of the present Government on criminal offences is not yet clear.

2.75 Most official reports since Younger - Calcutt I, Calcutt II, National Heritage Committee, Lord Chancellors' Consultation Paper -believe that it is technically possible to produce a workable civil tort protecting privacy. The Conservative Government was opposed to this as is apparently the present Government. Time will tell whether the formula settled on by the Home Secretary in amending the Human Rights Bill will effectively obviate the development of a privacy tort through the courts.

2.76 Most official reports since Younger, etc., draw a link between the concepts of harassment/molestation with the protection of privacy.

2.77 The possibility of a statutory Press Complaints Tribunal has been mooted but has not yet found favour.

ANNEX III

DATA PROTECTION LAW AND THE USE OF CCTV

1. The Application of Existing Data Protection Legislation to CCTV.
2. Implications of Directive 95/46/EC for the Coverage of Existing Legislation.
3. The Need to Develop CCTV Codes of Practice Whether Under the Data Protection Legislation or More Generally.

1. The Application of Existing Data Protection Legislation to CCTV

3.1 As the Data Protection Commissioner has pointed out¹, the use of advanced CCTV systems for surveillance purposes may already fall under the coverage of the *Data Protection Act, 1988*.

3.2 For the purposes of the Act, "data" means information in a form which can be processed [S.1(1)]. On the face of it this definition is not limited to information processed by computer. It has the potential to extend to other kinds of equipment which respond to instructions. *Processing* means performing automatically logical or arithmetical operations on data and includes extracting any information constituting the data [S.1(1)]. Personal data means 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 [S. 1(1)].

3.3 Depending therefore on the technical sophistication of the equipment used and on the ability or otherwise of the data controller to match the data with other information relating to identity, the data captured and recorded by CCTV may well fall under the scope of the 1988 Act. If so, and this issue can only be addressed on a case by case basis, then the data protection principals contained in S. 2 of the Act would apply.

3.4 The application of the data protection principles in the particular context of CCTV (in as much as CCTV falls under the Act) are usefully summarised by the Data Protection Commissioner as follows:

"Firstly and most importantly, every user should specify the precise purpose for which the system is used [section 2 (1)(c)(i)]. Secondly the user should ensure that he is obtaining personal data fairly [section 2(1)(a)]. People should be made aware that a CCTV system is in operation, the purposes for which it is used and who is responsible for it. Thirdly, there should be clear guidelines to ensure that the information collected is adequate, relevant and not excessive in relation to the specified purpose [section 2(1)(c)(iii)]. For example, a system that scanned private gardens - where the specified purpose was to monitor a particular street in the interests of public safety - would contravene this requirement."²

1 Data Protection Commissioner, *Annual Report 1996*, 'Case Study 14: use of closed circuit television (CCTV) - privacy implications - does the Data Protection Act apply?', at p. 26.

2 Data Protection Commissioner - *Annual Report, 1996* at 26.

3.5 Point 4.4. of the Garda Síochána *Code of Practice for the use of Closed Circuit T.V. Monitoring Systems in Temple Bar* (July 1995) concedes the potential application of the 1988 Act:

"The provisions of the *Data Protection Act 1989 [sic]* will apply to video recordings which related to an identified or identifiable individual."

3.6 It is to be noted that the *Data Protection Act* applies regardless of Point 4.4 of the Code if the criteria of the Act are met. In other words, its operation is independent of the terms of the Code. The Garda Commissioner has in fact registered the Temple Bar CCTV system under the 1988 Act³.

2. Implications of Directive 95/46/EC for the Coverage of Existing Legislation

3.7 It is noteworthy that, while the 1988 Act is less forthcoming on the technical question whether CCTV is covered, it does not allow for any general exception for the sake of detecting or preventing crime. This is so because it was modelled on, and intended to give effect to, a Council of Europe Convention on Data Protection of 1981. However, a complicating element in the analysis arises due to the need to transpose EC Directive 95/46/EC on data protection into Irish law before the Autumn of 1998.

3.8 On a positive note, it is fairly clear from the wide technical definitions accorded to 'personal data' and to the 'processing of personal data' under Article 2 of the directive that many forms of CCTV are now more clearly covered. On the negative side, the Directive appears to give Member States the option to carve out new exceptions in their data protection legislation - exceptions that could make a difference in the way (or even whether) such legislation is applied in the context of CCTV. To understand why it is important to appreciate that the breadth of competence of the Community is much narrower than that of the Council of Europe.

3.9 An EC Directive cannot by definition operate in any sphere outside the legal competence of the Community. Crime and matters relating to policing are, of course, outside the competence of the Community (Pillar I of the EU) as such. Logically therefore, Article 3(2) goes on to state that the Directive

"shall not apply to the processing of personal data

3 The registration entry on behalf of the Garda Commissioner, which is renewable annually, was last updated in October 1997 and must be renewed by 24 October, 1998. Such renewal would presumably have to take account of the other locations to where CCTV systems have been extended.

- in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union *and in any case* to processing operations concerning public security...the activities of the State in areas of criminal law."

3.10 Similarly, recital 16 states:

"Whereas the processing of sound and image data, such as in the cases of video surveillance, does not come within the scope of this Directive 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."

3.11 Article 3(2) essentially reiterates that matters lying outside the scope of Community law are not included within the scope of the Directive and that some matters that in fact lie within the scope of Community law are explicitly excluded in any event.

3.12 Nevertheless, as pointed out in the Department of Justice, Equality and Law Reform Consultation Paper on the transposition of the Directive into Irish law,

"there is nothing to stop individual Member States from applying the principles in the Directive in a uniform way to all processing activities be they inside or outside the scope of Community law."⁴

3.13 It follows that Member States need not view the transposition of the directive as an occasion in which to revisit and curtail the scope of existing legislation. Likewise, Member States need not operationalise the exceptions permitted them under the directive.

3.14 In our view it would be highly desirable that the implementing legislation should leave the coverage of the 1988 Act intact particularly as it may reach State activity connected with sophisticated CCTV systems. Given that the 1988 Act already operates in the sphere of crime and crime prevention and that the data protection principles established under the Act are especially useful in the context of CCTV activity it would appear wrong in principle to exclude coverage just as the point where the technology is developing in its sophistication.

⁴ *Consultation Paper on Transposition into Irish Law: Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* - Department of Justice, Equality and Law Reform, November 1997 at p. 11.

3. The Need to Develop CCTV Codes of Practice Whether Under the Data Protection Legislation or More Generally

3.15 Codes of practice are extremely useful tools with which to educate users and the public at large about the use of CCTV. Such codes provide a regulatory framework within which more careful consideration can be given such matters of detail including the form, etc., of notices to the public.

3.16 So far, only one area-specific code of practice exists with respect to the public sector: the Temple Bar Code of 1995 (see chapter 3 of this Report). As its title suggests, this Code is confined to the Temple Bar CCTV programme and thus has no formal (as against informal) authority for the rest of the country. Although good in itself the Temple Bar Code appears under-developed at least relative to the *Code of Practice for CCTV* prepared by the British Local Government Information Unit in March 1996. Nor does it take detailed account of the operation of the Data Protection Act.

3.17 It is for these reasons that we consider that the Government should now actively consider developing a comprehensive and country-wide code governing the use of fixed CCTV systems in public places by the Gardaí (in cooperation with local authorities) [see para. 9.37 of this Report]. Such a code should have a firm foundation in legislation. It should could take account of more sophisticated norms developed subsequently, for example, in the British Code and also take more explicit account of data protection principles where appropriate. Among other things the new Code would be the ideal place to deal with such matters of detail such as the size, shape and form of notices to alert members of the public that upon entering a certain area their activities are being monitored and recorded.

3.18 It is to be noted that section 13 of the *Data Protection Act* allows for the development of sectoral codes or practice which, if approved by the Data Protection Commissioner, assume the force of law upon a resolution of both Houses of the Oireachtas to that effect. Although this Code would obviously have to take account of the data protection principles there would appear to be nothing stopping the Gardaí from embracing more general safeguards in the code.

3.19 It would therefore appear that there is a choice whether to place a code of practice under general surveillance legislation of the type we recommend in this Report or under the existing data protection legislation. The advantage of developing a code under the rubric of the data protection legislation is that it would engage the active contribution of the Office of the Data Protection Commissioner which has built up a wealth of experience on privacy issues and which can readily draw on the wisdom and experience of similar bodies worldwide. This option would therefore appear preferable particularly, as noted before, there seems to be no obstacle to

including matter in such a code that went beyond pure data protection principles if felt necessary.

3.20 Likewise, we consider that active consideration should also be given to the development of codes of practice in various private sectors which use CCTV technology [see para. 9.38 of this Report]. Such sectors include industry, banking, commercial shopping centres, etc. Again this can be done either under the existing data protection legislation or more generally under enabling legislation.

Annex IV

THE POWER OF THE COURTS TO HOLD PROCEEDINGS *IN CAMERA* OR TO MAKE ORDERS RESTRICTING PUBLICATION OR BROADCASTING RELATING TO SUCH PROCEEDINGS

4.1 As explained in the Heads of Bill (Head 12) and in Chapter 9 (para. 9.34) of this Report, we recommend that any legislation providing for the remedies suggested should confer discretion on the relevant court to order that proceedings be held otherwise than in public and/or to place tailored restrictions on publication where, on balance, privacy so warrants.

4.2 We looked at the issue whether there is a need for additional protections of privacy in the *manner* by which the judicial proceedings entailed by or recommendations (civil and criminal) should be conducted and/or reported. Are there, in other words, good and sufficient grounds for provisions which would permit or even require the hearing of privacy cases (whether civil or criminal) arising from our proposals otherwise than in public or the imposition of other restrictions on the disclosure or reporting of evidence or other material arising before the courts in such cases? We believe that there are such grounds.

4.3 We also looked at the constitutional parameters surrounding this issue. We have come to the conclusion that the proposed power constitutes, where the court sees fit, a necessary and legitimate exception to the general constitutional requirement that legal proceedings in court are to be conducted in public.

4.4 We consider the argument for such an ancillary power (or rather judicial discretion) to be sound. Civil and criminal proceedings on the basis of the Heads which we propose will invariably be based on claims concerning the privacy rights of individuals and therefore will not infrequently involve private information concerning such individuals which they will claim should not be disclosed or published either directly by the offending party or through the medium of court proceedings. We have concluded the privacy rights which we proposed should be created would in at least some cases be unjustly circumvented and set at nought, and proceedings to

enforce those rights, whether civil or criminal in nature, would fail in their object of securing the due administration of justice, if the court had no jurisdiction to order that proceedings arising from our proposals be heard otherwise than in public or to make orders of an appropriate nature prohibiting or restricting publication of information, including the identities of parties, the subject of such proceedings.

4.5 We believe sufficient flexibility exists under the Constitution to allow for such restrictions. At play is a tension between different constitutional provisions. On the one hand various constitutional provisions require openness in judicial proceedings and the freedom to publish contemporaneous and accurate accounts of the same. On the other hand, different constitutional imperatives and rights can pull in the opposite direction. These include the overriding necessity of ensuring the integrity of the trial process (Article 38), the need to afford the accused a right to fair trial (Article 40.3) and the need to secure other constitutional rights which may rank higher on a hierarchy of constitutional rights. All of this calls for a delicate balancing act - one that presumptively favours openness over secrecy in democratic society and that does not advance one right to the complete detriment of the other.

4.6 The constitutional imperative for openness in judicial proceedings is rightly very strong. It is grounded principally on Article 34 but also receives powerful impetus from Article 40.6.i. dealing with freedom of expression and of the press. Article 34.1 provides that

"justice shall be administered in courts established by law... and, save in such special and limited cases which may be prescribed by law, shall be administered in public."

4.7 Quite obviously, public access to proceedings is critically important in assuring the public of regularity and due process in judicial proceedings. As indicated by Keane J. in his judgment in the seminal Supreme Court decision of *The Irish Times et al v. Ireland, the Attorney General and His Honour Judge Anthony G Murphy, etc*¹ the right of public access provides a checking mechanism against the potential of corruption and irregularity. That case, which arose out of a drugs prosecution against several foreign nationals, concerning an order of a trial Judge to the effect that reporting on most matters beyond the rudimentary should be delayed pending the outcome of the trial. The order was issued in to try forestall what the trial Judge perceived to be a threat to the accused's right to a fair trial. The trial Judge was moved to do so on the basis of previous experience as well as apprehended mis-reporting. The order of the trial Judge was affirmed in the High Court (Morris J) but unanimously overturned on appeal to the Supreme Court.

1 Unreported judgment of the Supreme Court, 2 April, 1998.

4.8 The Supreme Court's judgment in the *Irish Times* case is now the leading authority on the whole issue of public rights of access to, and associated publicity about, ongoing judicial proceedings. It is an important judgment generally (see the general treatment of the judgment in chapter 3 of this Report) and also in the specific context of the instant issue for the following reasons.

4.9 First of all, Article 34 would appear on a literal reading merely to grant a public right of physical access to judicial proceedings. It does not, in other words, appear to grant any corollary right to publish. If so, the order given by the trial Judge in the instant case could not be impugned under Article 34. However, the Supreme Court in the *Irish Times* ruling significantly expanded its understanding of Article 34 to include a right on the part of the press to impart information concerning ongoing trials and a corollary right of the public to receive such information. In effect, the Supreme Court subsumed a general right of publicity concerning ongoing judicial proceedings under Article 34. In support of this view it was pointed out by many members of the Supreme Court that the press are the eyes and ears of the public and that it would defeat the broader democratic purpose of Article 34 if the right to publish were not subsumed thereunder. It followed that a temporary ban on publication - which was at issue on the facts of this case - amounted to a denial of a right of public access under Article 34 and was analysed accordingly.

4.10 Some members of the Supreme Court fortified their reasoning by reference to Article 40.6.1 of the Constitution (freedom of expression). This had the effect of bringing Article 40.6.1 into the overall balancing equation - a factor absent in the trial Judge's order. In the process, the decision also expands the Supreme Court's understanding of the role and content of Article 40.6.1. A majority felt that freedom of expression, as guaranteed by Article 40.6.1, was reckonable in the context of the instant case and that it conferred certain rights on the press. At least two judges (Barrington and O'Flaherty JJ.) were expressly of the view that its protective coverage included the reportage of facts as well as covering the expression of convictions and opinions. That point seems to be accepted by all. Barrington J. further bolstered freedom of expression by linking it to the dynamics of political change. The chief flaw in his view was the fact that freedom of expression under Article 40.6.1 did not figure at all in the balancing equation used by the trial Judge. Indeed, Barrington J. fortified the conclusion of the court on the latter point by reference to the text of Article 10 of the European Convention on Human Rights.

4.11 Secondly, Article 34 merely grants latitude in the Oireachtas to legislate for exceptions to the norm of openness. On a literal reading it therefore appears that *in the absence of any such legislation* a court is utterly powerless to regulate the right of public access and publication. This view was propounded by Walsh J. in his

judgment in *Re R*². However, in his High Court decision in the above *Irish Times* case Morris J. held that where a competing and superior constitutional right is at stake a court has the inherent power to regulate both access and publicity³. The competing right and indeed superior right at stake in that case was the right of the accused to a fair trial. This reasoning - although not the conclusions drawn by the trial Judge - was upheld by the Supreme Court on appeal.

4.12 **Thirdly**, the Supreme Court stressed that the inherent power to regulate public access and press publicity connected with ongoing judicial proceedings was an exceptional power to be used only where absolutely necessary and to the extent necessary. At the same time, and in accordance with its own precedents⁴, the Court recognised that the right of an accused person to a fair trial ranked superior to a right of public access and publicity in circumstances where there was a real risk that the former right might be jeopardised. However, in essence, the Court did not believe that the trial Judge in the instant case could, on the evidence presented, reasonably come to the conclusion that there was such a real risk in the instant case or at least one that warranted such an extreme step as a ban on publicity, howsoever temporary.

4.13 Quite apart from any inherent jurisdiction to regulate or limit a public right of access and related publicity, Article 34 creates the possibility that statute law may be enacted limiting rights of access and publicity. O'Flaherty J. referred usefully to the various situations in which statute law already provides for exceptions to the right of public access or publicity. Such statutory restrictions are sometimes mandatory and sometimes consist of a discretion vested in the judge in the particular case.

4.14 Examples of mandatory provisions excluding members of the public from judicial proceedings include s.2 of the *Criminal Law (Incest Proceedings) Act, 1995*; s.6 of the *Criminal Law (Rape) Act, 1981*; s.34 of the *Judicial Separation and Family Law Reform Act, 1989*; and s.14 of the *Family Law (Protection of Spouses and Children) Act, 1981*. Proceedings under the above legislation normally touch on delicate and sensitive family and private matters.

4.15 Examples of legislation which confer judicial discretion to exclude the public from proceedings include s.45 of the *Courts (Supplemental Provisions) Act, 1951* (applications of an urgent nature, matrimonial causes and matters, lunacy and minor matters, proceedings involving the disclosure of a secret manufacture); s.20 of the

2 [1989] I.R. 126. For an illustration of the narrow view in practice see *Bridget M. Roe v. Blood Transfusion Service Board, The Minister for Health, the National Drugs Advisory Board, Ireland and the Attorney General*, [1996] 3 I.R. 67, per Laffoy J.

3 Unreported High Court judgment, 18 February, 1997.

4 *D. v D.P.P.*, [1994] 2 I.R. 465 and *Z. v D.P.P.*, [1994] 2 I.R. 476.

Criminal Justice Act, 1951 (where the court is satisfied that such exclusion is expedient for the purpose of ensuring that the accused will not be prejudiced in his trial); and s.205(7) of the *Companies Act, 1963* (where the hearing of proceedings would involve the disclosure of information the publication of which would be seriously prejudicial to the legitimate interests of the company).

4.16 Privacy and anonymity is protected even where members of the press are not excluded from attendance under s. 3 of the *Criminal Law (Incest Proceedings) Act, 1995* s.7 of the *Criminal Law (Rape) Act, 1981*.

4.17 The above statutory provisions have not been challenged as going beyond what Article 34 allows - assuming the discretion conferred on the Oireachtas not to be unlimited. Presumably these statutory provisions pass muster on the basis that they protect superior constitutional rights and carve out necessary limitations to Article 34 as needs be.

4.18 The question remains whether similar legislation protecting privacy in the context of the kind of ongoing civil and criminal proceedings we envisage would also pass muster. We believe such legislation would be permissible.

4.19 **First** of all, we envisage that the legislation would merely confer a discretion on a trial judge. This reflects the exceptional nature of the power when set against the imperative of openness implicit in Articles 34 and 40.6.1. **Second**, we further envisage that this discretion should only be used where there is a real risk to privacy and where the potential damage or hurt is not slight to the individual concerned. Obviously, any limitation on publicity must be narrowly tailored to the risk at hand. **Third**, we explicitly provide that the trial judge should advert his mind to all the circumstances arising including particularly whether there is a countervailing argument in the *public interest* that militates in favour of disclosure despite the argument from privacy.

4.20 Accordingly, we recommend that in any proceedings whether civil or criminal based on our recommendations, the court at any stage should have a discretionary jurisdiction to exclude members of the public from proceedings or to regulate or otherwise limit any publicity connected with ongoing proceedings. Such an order may continue in force after the determination of the proceedings since the privacy interest survives the outcome of such proceedings. However, it may be discharge or varied at any time on the application of any interested party.

4.21 In so recommending we believe that we are proposing the necessary safeguards to enable the court to protect legitimate rights of privacy arising from the hearing of legal proceedings on the one hand and, by providing for the discretion of the courts, rather than proposing any mandatory provisions, we aim to give the courts full liberty and discretion to do what is just having regard to all the interests involved.

4.22 We are confident that the courts will have regard not only to the interests of the individuals involved but also to the broader public interest in allowing case law in the form of written judgments of all the courts having jurisdiction in such cases to be published in as much detail as the legitimate private interests involved permit, so as to facilitate the development of the body of case law on the interpretation of the legislation proposed in our recommendations which is essential in order to bring those recommendations to full fruition.

ANNEX V

RESOLUTION ON PRIVACY OF THE PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE

COUNCIL OF EUROPE Parliamentary Assembly

Provisional edition

Right to Privacy

Resolution 1165 (1998)¹

1. The Assembly recalls the current affairs debate it held on the right to privacy during its September 1997 session, a few weeks after the accident which cost the Princess of Wales her life.
2. On that occasion, some people called for the protection of privacy, and in particular that of public figures, to be reinforced at the European level by means of a convention, while others believed that privacy was sufficiently protected by national legislation and the European Convention on Human Rights, and that freedom of expression should not be jeopardised.
3. In order to explore the matter further, the Committee on Legal Affairs and Human Rights organised a hearing in Paris on 16 December 1997 with the participation of public figures or their representatives and the media.
4. The right to privacy, guaranteed by Article 8 of the European Convention on Human Rights, has already been defined by the Assembly in the declaration on mass communication media and human rights, contained within Resolution 428 (1970), as "the right to live one's own life with a minimum of interference".
5. In view of the new communication technologies which make it possible to store and use personal data, the right to control one's own data should be added to this definition.

¹ Assembly debate on 26 June 1998 (24th Sitting). See Doc. 8130, report of the Committee on Legal Affairs and Human Rights (rapporteur: Mr Schwimmer), Doc. 8147, opinion of the Committee on Culture and Education (rapporteur: Mr Staes) and Doc. 8146, opinion of the Social, Health and Family Affairs Committee (rapporteur: Mr Mitterrand). Text adopted by the Assembly on 26 June 1998 (24th Sitting).

6. The Assembly is aware that personal privacy is often invaded, even in countries with specific legislation to protect it, as people's private lives have become a highly lucrative commodity for certain sectors of the media. The victims are essentially public figures, since details of their private lives serve as a stimulus to sales. At the same time, public figures must recognise that the position they occupy in society - in many cases by choice - automatically entails increased pressure on their privacy.

7. Public figures are persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain.

8. It is in the name of a one-sided interpretation of the right to freedom of expression, which is guaranteed in Article 10 of the European Convention on Human Rights, that the media invade people's privacy, claiming that their readers are entitled to know everything about public figures.

9. Certain facts relating to the private lives of public figures, particularly politicians, may indeed be of interest to citizens, and it may therefore be legitimate for readers, who are also voters, to be informed of those facts.

10. It is therefore necessary to find a way of balancing the exercise of two fundamental rights, both of which are guaranteed in the European Convention on Human Rights: the right to respect for one's private life and the right to freedom of expression.

11. The Assembly reaffirms the importance of every person's right to privacy, and of the right to freedom of expression, as fundamental to a democratic society. These rights are neither absolute nor in any hierarchical order, since they are of equal value.

12. However, the Assembly points out that the right to privacy afforded by Article 8 of the European Convention on Human Rights should not only protect an individual against interference by public authorities, but also against interference by private persons or institutions, including the mass media.

13. The Assembly believes that, since all member states have now ratified the European Convention on Human Rights, and since many systems of national legislation comprise provisions guaranteeing this protection, there is no need to propose that a new convention guaranteeing the right to privacy should be adopted.

14. The Assembly calls upon the governments of the member states to pass legislation, if no such legislation yet exists, guaranteeing the right to privacy containing the following guidelines, or if such legislation already exists, to supplement it with these guidelines:

- i. an action in civil law should be guaranteed to be able

to claim possible damages for invasion of privacy;

- ii. editors and journalists should be rendered liable for invasions of privacy by their publications, as they are for libel;
- iii. when editors have published information that proves to be false, they should be required to publish equally prominent corrections at the request of those concerned;
- iv. economic penalties should be envisaged for publishing groups which systematically invade people's privacy;
- v. following or chasing persons to photograph, film or record them, in such a manner that they are prevented from enjoying the normal peace and quiet they expect in their private lives or even such that they are caused actual physical harm, should be prohibited;
- vi. a civil action (private lawsuit) by the victim should be allowed against a photographer or a person directly involved, where "paparazzi" have trespassed or used "visual or auditory enhancement devices" to capture recordings that they otherwise could not have captured without trespassing;
- vii. provision should be made for anyone who knows that information or images relating to his or her private life are about to be disseminated to initiate emergency judicial proceedings such as summary applications for an interim order or an injunction postponing the dissemination of the information, subject to an assessment by the court as to the merits of the claim of an invasion of privacy;
- viii. the media should be encouraged to create their own guidelines for publication and to set up an institute with which an individual can lodge complaints of invasion of privacy and demand that a rectification be published.

15. It invites those governments which have not yet done so, to ratify without delay the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

16. The Assembly also calls upon the governments of the member states to:

- i. encourage the professional bodies that represent journalists to draw up certain criteria for entry to the profession, as well as standards for self-regulation and a code of journalistic conduct;
- ii. promote the inclusion in journalism training programmes of a course in law, highlighting the importance of the right to privacy *vis-à-vis* society as a whole;
- iii. foster the development of media education on a wider scale, as part of education about human rights and responsibilities, in order to raise media users' awareness of what the right to privacy necessarily entails;
- iv. facilitate access to the courts and simplify the legal procedures relating to press offences, in order to ensure that victims' rights are better protected.

ANNEX VI: LIST OF PERSONS FROM WHOM WRITTEN SUBMISSIONS HAVE BEEN RECEIVED

1. National Union of Journalists
2. R.T.É.
3. National Newspapers of Ireland (two)
4. Department of Justice, Equality and Law Reform
5. Confederation of Irish Detectives
6. Department of Public Enterprise
7. Provincial Newspaper Association of Ireland (submission and amended submission)

ANNEX VII: LIST OF PERSONS WHO PARTICIPATED AT OUR LISTENING EXERCISE

List of Persons who attended "Listening Exercise" on Privacy - Thursday, 17 July 1997

Ronan Brady, National Union of Journalists

Richard Barrett, Office of the Attorney General

Aileen Harrington} Department of Justice, Equality and
Geraldine Larkin} Law Reform

Frank Cullen }
Paul Drury } Provincial Newspaper Association of Ireland
Neville Galloway}

Thomas Geoghegan}
Nicholas Nally } Provincial Newspaper Association of Ireland

James Dunne, The Star Newspaper

Anne Doyle, Solicitors' Office, Telecom Éireann

Peter Kirwan, Garda Síochána

Marie McGonagle, University College Galway

Eoin McVey, The Irish Times

Eoin O'Dell, Trinity College

John O'Dowd, {University College Dublin,
{Irish Council for Civil Liberties

Hugh O'Reilly, An Post

Professor Patrick Riordan SJ, Milltown Institute of Theology and Philosophy

Sinéad Ryan, Department of Public Enterprise

Peter Somers, B.L.

Professor Dermot Walsh, University of Limerick

Tim Doyle, Human Rights Unit, Department of Foreign Affairs

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] [photocopy available]**
[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)**[out of print]**
[£ 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 Harboursing of a Spouse (Dec 1978)**[out of print]**
[£ 1.00 Net]
- Working Paper No. 6-1979, The Law Relating to Seduction and the Enticement and Harboursing 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)
[£ 3.50 Net]
- Third (Annual) Report (1980) (Prl. 9733) [75p Net]
- First Report on Family Law - Criminal Conversation, Enticement and Harboursing 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 (<u>Annual</u>) 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 (<u>Annual</u>) 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 (<u>Annual</u>) 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 (<u>Annual</u>) 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 (<u>Annual</u>) 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 (<u>Annual</u>) 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) [out of print]	[£ 4.00 Net]
Report on Debt Collection: (1) The Law Relating to Sheriffs (LRC 27-1988) (Oct 1988)	[£ 5.00 Net]
Tenth (<u>Annual</u>) Report (1988) (Pl 6542)	[£ 1.50 Net]

Report on Debt Collection: (2) Retention of Title (LRC 28-1989) (April 1989) [out of print]	[£ 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 (<u>Annual</u>) Report (1989) (PI 7448)	[£ 1.50 Net]
Report on Child Sexual Abuse (September 1990) (LRC 32-1990)	[£ 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 (<u>Annual</u>) 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)[out of print] [£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]

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 (<u>Annual</u>) Report (1995) (PN. 2960)	[£2.50 Net]
Report on Sentencing (LRC 53-1996) (August 1996)	[£ 8.00 Net]
Consultation Paper on Privacy: Surveillance and the Interception of Communications (September 1996)	[£20.00 Net]
Report on Personal Injuries (LRC 54-1996) (December 1996)	[£10.00 Net]
Eighteenth (<u>Annual</u>) Report (1996) (PN. 3760)	[£ 2.50 Net]
Consultation Paper on The Implementation of the Hague Convention on Protection of Children and Co-operation in Respect of Intercountry Adoption, 1993 (September 1997)	[£10.00 Net]
Report on The Unidroit Convention on Stolen or Illegally Exported Cultural Objects (LRC 55-1997) (October 1997)	[£15.00 Net]
Consultation Paper on Aggravated, Exemplary and Restitutionary Damages (April 1998)	[£15.00 Net]
Report on Land Law and Conveyancing Law: (6) Further General Proposals Including the Execution of Deeds (LRC 56) (May 1998)	[£ 8.00 Net]