Issues Paper on Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying (LRC IP 6-2014)

LAW REFORM COMMISSION/COIMISIÚN UM ATHCHÓIRIÚ AN DLÍ

BACKGROUND TO THIS ISSUES PAPER AND THE QUESTIONS RAISED

This Issues Paper forms part of the Commission's *Fourth Programme of Law Reform*,[1] which includes a project to review the law on cyber-crime affecting personal safety, privacy and reputation including cyber-bullying. The criminal law is important in this area, particularly as a deterrent, but civil remedies, including "take-down" orders, are also significant because victims of cyber-harassment need fast remedies once material has been posted online.[2] The Commission seeks the views of interested parties on the following 5 issues.

1. Whether the harassment offence in section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be amended to incorporate a specific reference to cyber-harassment, including indirect cyber-harassment (the questions for which are on page 13);
2. Whether there should be an offence that involves a single serious interference, through cyber technology, with another person's privacy (the questions for which are on page 23);
3. Whether current law on hate crime adequately addresses activity that uses cyber technology and social media (the questions for which are on page 26);
4. Whether current penalties for offences which can apply to cyber-harassment and related behaviour are adequate (the questions for which are on page 28);
5. The adequacy of civil law remedies to protect against cyber-harassment and to safeguard the right to privacy (the questions for which are on page 35);

Cyber-harassment and other harmful cyber communications

The emergence of cyber technology has transformed how we communicate with others. Using basic mobile technology, individuals can now publish online instantly and to very large audiences. This has had positive effects in allowing us to remain connected with each other by text and visually. However, there have also been negative consequences, primarily because it is possible to publish online not only instantly and to a huge audience, but also anonymously, increasing the potential for harmful effects due to harassment.

This project addresses harassment conducted through cyber technology, or cyber-harassment, and other harmful communications through the use of internet enabled devices such as smart phones, tablets and PCs. "Harmful" in this context includes cyber communications that are abusive, threatening, offensive, obscene, false or invasive of privacy.

---

[1] *Report on Fourth Programme of Law Reform* (LRC 110-2013), Project 6.

[2] This Paper focuses on behaviour between individuals and does not address the liability of internet service providers (ISPs). Under the eCommerce Directive, Directive 2000/31/EC, which was implemented by the *European Communities (Directive 2000/31/EC) Regulations 2003* (SI No. 68 of 2003), ISPs are not liable for content they carry if they do not knowingly act to promote harmful or illegal material and act expeditiously to remove any such content once notified by competent authorities.

There are a number of significant features of harmful cyber communications that contrast with similar offline behaviour:

- When individuals are online they may feel disconnected from their behaviour as it is not occurring in the "real world" but rather from the safety and distance offered by a computer whether a phone, laptop or similar device. This sense of disconnection is increased by the anonymity frequently involved in online communications and may prompt individuals to act in a manner they would not in the offline world.[3]
- Anonymity may also increase the anxiety experienced by the victim as the pool of potential perpetrators may be far wider in the online setting than offline.
- The instant nature of cyber-harassment may exacerbate the harm caused to the victim because it may lead to a greater volume of, and more frequent, communications compared to offline harassment.
- The potential to reach large, even global, audiences and the overwhelming exposure that may result can magnify the harm. This potentially global dimension to the harassment may also raise jurisdictional issues which make application of the law difficult.
- The permanence of material combined with the searchability of the web means that damaging content can survive long after the event and can be used to re-victimise the target each time it is accessed.[4]

2014 Report of the Internet Content Advisory Group

There is a growing awareness internationally of the need to address cyber-harassment and related harmful internet content.[5] The 2014 *Report of the Internet Content Advisory Group*[6] commissioned by the Minister for Communications, Energy and Natural Resources examines the general policy setting and governance arrangements needed to address harmful online material.[7] In accordance with the Advisory Group's terms of reference the 2014 Report emphasises the damaging impact of such harmful material on young people who are active users of social media, including for example poor school performance, depression, self-harm and in some instances suicide. It is equally important to note that there have also been well-publicised cases of adults, both in public life or who have become involved in public online campaigns, who have experienced identical issues when faced with

---

[3] The case of the 63 year old English woman Brenda Leyland appears to illustrate this. In 2014 Ms Leyland sent thousands of tweets under the pseudonym "@sweepyface" stating her view, in an angry and outspoken manner, that the parents of the missing child Madeline McCann were involved in the child's disappearance. Offline, however, Ms Leyland behaved very differently to her Twitter persona, and shortly after she was publicly exposed she committed suicide. See "The Case of Brenda Leyland and the McCanns is a thoroughly modern tale of internet lawlessness" *The Independent* 6 October 2014, available at http://www.independent.co.uk/voices/comment/the-case-of-brenda-leyland-and-the-mccanns-is-a-thoroughly-modern-tale-of-internet-lawlessness-9778262.html.

[4] The decision of the EU Court of Justice in Case C-131/12, *Google Spain SL and Google Inc v Agencia Espanola de Protection de Datos* (judgment of 13 May 2014) may reduce the potential for this in the future, because the Court held that a search engine is obliged, if requested, to remove search results from its index where the data involved is inaccurate, inadequate, irrelevant or excessive. The material itself remains on the relevant source site, so the precise effect of this decision on the "right to be forgotten" has yet to be seen.

[5] See, for example, the comparative survey in the New Zealand Law Commission's Ministerial Briefing Paper *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (2012).

[6] *Report of the Internet Content Governance Advisory Group* (Department of Communications, Energy and Natural Resources, 2014).

[7] The establishment by the Minister of the Advisory Group followed the publication by the Oireachtas Joint Committee on Transport and Communications of its *Report on Addressing the growth of Social Media and tackling Cyberbullying* (Government Publications, 2013).

menacing online comments.[8] The Commission's examination of cyber-harassment and other harmful cyber communications addresses the matter in relation to its impact on all persons.

The 2014 *Report of the Internet Content Advisory Group* contains 30 recommendations whose principal focus is on the need for enhanced awareness and understanding of harmful digital content, together with new national governance arrangements. These include:

- the Office for Internet Safety (OiS) in the Department of Justice and Equality should have a clear oversight role of the system of self-regulation for illegal internet content, including oversight of the current voluntary blocking of illegal internet content undertaken by mobile network operators;
- the Internet Safety Advisory Committee (ISAC) should be reconfigured as the National Council for Child Internet Safety (NCCIS) and be the primary forum for internet safety strategy in Ireland, with representation from industry, relevant government departments, public bodies, civil society including youth representation and child protection interests;
- NCCIS should act as coordinator for the Safer Internet Ireland project (which should become the Safer Internet Ireland Centre (SIIC)), in particular its awareness-raising, education and helpline functions;
- SIIC should be responsible for compiling best practice resources for dealing with online abuse and harassment for parents, teachers and young people; should plan and direct a national awareness campaign on effective measures to deal with reporting cyberbullying and online abuse; and liaise with the Office of the Data Protection Commissioner to raise awareness of privacy issues in the sharing of content online and the most appropriate ways to deal with violations of privacy.

The Report also includes two specific recommendations on legislative reform:

- section 13 of the *Post Office (Amendment) Act 1951*, as amended by the *Communications Regulation (Amendment) Act 2007*, which provides that it is an offence to send by phone or text any message that is grossly offensive, indecent, obscene or menacing, should be amended to include social media and other online communications;
- in the context of civil law remedies, there should be a review of the suitability of current rules of court on discovery and disclosure to bring them into line with technological norms.[9]

The Report noted the Commission's project and left consideration and recommendations for reform in this area, including any proposed reform of the offence of harassment in section 10 of the *Non-Fatal Offences against the Person Act 1997*, to the Commission.[10]

As the policy and governance recommendations in the 2014 Report are currently under consideration by Government, and as the Commission agrees with the proposal to amend section 13 of the 1951 Act, this Issues Paper concentrates on the five issues listed on page 1, above.

---

[8] In England in 2013, Caroline Criado-Perez became the subject of repeated threatening tweets (including threats of mutilation and sexual assault) in response to her online campaign to have a greater number of women (such as Jane Austen) represented on English bank notes. Arising from this, in 2014 two people were convicted of improper use of a communications network under section 127 of the English *Communications Act 2003*, which is broadly similar to section 13 of the *Post Office (Amendment) Act 1951*, as amended by the *Communications Regulation (Amendment) Act 2007*, discussed at paragraph 2.07, below.

[9] This is discussed further at paragraphs 5.16-5.17 below.

[10] *Report of the Internet Content Governance Advisory Group* (Department of Communications, Energy and Natural Resources, 2014) at 45 and 64.

ISSUE 1: WHETHER THERE SHOULD BE A SPECIFIC REFERENCE TO "CYBER-HARASSMENT" IN SECTION 10 OF THE 1997 ACT

1.01 The first matter arising in this Issues Paper is whether section 10 of the *Non-Fatal Offences Against the Person Act 1997* fully captures the various forms of harassing behaviour conducted using cyber technology, such as the internet and mobile phones.

Section 10 of the Non-Fatal Offences Against the Person Act 1997

1.02 Section 10 of the *Non-Fatal Offences Against the Person Act 1997* provides:

> "(1) Any person who, without lawful authority or reasonable excuse, by any means including by use of the telephone, harasses another by persistently following, watching, pestering, besetting or communicating with him or her, shall be guilty of an offence.
>
> (2) For the purposes of this section 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."

1.03 Section 10 derives from a recommendation in the Commission's 1994 *Report on Non-Fatal Offences Against the Person*[11] that:

> "acts of harassment which interfere seriously with a person's right to a peaceful and private life should be captured by the criminal law and not simply those [acts] that give rise to a fear of violence [which are covered by the offence of coercion]."[12]

1.04 The offence created by section 10 of the 1997 Act contains an objective element, because the acts of the defendant must be such that a "reasonable person would realise that the acts would seriously interfere with the peace and privacy of another or cause them alarm, distress or harm." This ensures that self-deluded stalkers cannot escape liability under the section, because even if they believe their behaviour is reasonable they still come within section 10 if their actions are seen as objectively likely to cause interference, alarm, distress or harm.[13]

1.05 The penalties under section 10 consist of a fine and/or imprisonment, which can be for a term not exceeding 12 months on summary conviction and 7 years on conviction on indictment.[14] As an

---

[11] Law Reform Commission *Report on Non-Fatal Offences Against the Person* (LRC 45-1994), paragraph 9.77.

[12] Immediately before this passage, the Commission had recommended that the offence of intimidation in section 4 of the *Conspiracy and Protection of Property Act 1875*, which dealt with acts that give rise to fear of violence, should be replaced by a modern offence of coercion. This recommendation was implemented in section 9 of the 1997 Act which replaced section 4 of the 1875 Act. The offence of coercion corresponds broadly with the tort of intimidation which consists of a threat by a defendant to a person to do an unlawful act which then causes that person "to act or refrain from acting in a manner which he or she is entitled to act either to that person's own detriment or to the detriment of another". See McMahon and Binchy *Law of Torts* 4th ed (Bloomsbury Professional, 2013), paragraph 32.83.

[13] Charleton, McDermott and Bolger, *Criminal Law* (Butterworths, 1999), paragraph 8.205.

[14] Section 10(6) of the *Non-Fatal Offences Against the Person Act 1997:* see the discussion of penalties at paragraph 4.03 below.

alternative or in addition to any other penalty the court may issue an order restraining the defendant from communicating with the other person or requiring him or her to remain a certain distance from the place of residence or employment of the person for such a period as the court may specify.[15] This ensures that the victim can gain relief in cases where imprisonment may not be appropriate.[16] An order can be made even in cases where the defendant is not found guilty of the offence if it is in the interests of justice to do so.[17] The court may also make a "restriction on movement order" under section 101 of the *Criminal Justice Act 2006* where a person is convicted under section 10 of the 1997 Act.[18]

1.06 Section 10 requires that the harassing conduct, "following, watching, pestering, besetting or communicating," must be persistent. Persistence is necessary because the conduct criminalised in section 10 is otherwise lawful and the offence is only committed where it is persistent so that it "seriously interferes with [an]other's peace and privacy or causes alarm, distress or harm to the other." The requirement for persistence was examined by the Commission in its 2013 *Report on Aspects of Domestic Violence*,[19] which noted that the term "persistently" had been interpreted in a manner that was not dependent on a specific number of incidents or a time frame within which those incidents must have occurred.[20] The Commission recommended that while a single protracted act may satisfy the requirement for persistence, isolated incidents which are not protracted should not give rise to liability under section 10.[21] The Commission also recommended that the term "persistently" be retained rather than replaced with a "course of conduct" requirement as in some other jurisdictions.[22]

---

[15] Section 10(3) of the *Non-Fatal Offences Against the Person Act 1997.*

[16] Charleton, McDermott and Bolger, *Criminal Law* (Butterworths, 1999), paragraph 8.206.

[17] Section 10(5) of the *Non-Fatal Offences Against the Person Act 1997.*

[18] Section 101 of the *Criminal Justice Act 2006* provides*:*

"(1) Where a person aged 18 years or more is convicted of an offence specified in Schedule 3 and the court which convicts him or her of the offence considers that it is appropriate to impose a sentence of imprisonment for a term of 3 months or more on the person in respect of the offence, it may, as an alternative to such a sentence, make an order under this section ("a restriction on movement order") in respect of the person.

(2) A restriction on movement order may restrict the offender's movements to such extent as the court thinks fit and, without prejudice to the generality of the foregoing, may include provision—

(a) requiring the offender to be in such place or places as may be specified for such period or periods in each day or week as may be specified, or

(b) requiring the offender not to be in such place or places, or such class or classes of place or places, at such time or during such periods, as may be specified,

or both, but the court may not, under paragraph (a), require the offender to be in any place or places for a period or periods of more than 12 hours in any one day.

(3) A restriction on movement order may be made for any period of not more than 6 months and, during that period, the offender shall keep the peace and be of good behaviour."

Schedule 3 of the 2006 Act includes section 10 of the 1997 Act as well as sections 2 (assault), 3 (assault causing harm) and 9 (coercion) of the 1997 Act. Schedule 3 also includes a number of offences under the *Criminal Justice (Public Order) Act 1994*.

[19] Law Reform Commission *Report on Aspects of Domestic Violence* (LRC 111-2013).

[20] *Ibid*, paragraph 2.23.

[21] *Ibid*, paragraph 2.88.

[22] *Ibid*, paragraph 2.102.

In *Director of Public Prosecutions (O'Dowd) v Lynch*[23] a sister and brother aged 11 and 14 respectively, were in their sitting room watching television. The accused, who was in the children's home to install a kitchen, exposed himself masturbating to the girl. This behaviour was repeated on at least two further separate incidents over a short period of time. Thus there were at least three incidents of exposure while the children were watching television. Over the next three hours, the accused repeatedly looked at the children while making revving noises with his saw. The accused exposed himself, masturbating again, while standing at the back door and this incident was witnessed by the two children. The boy then approached the front of the house and saw the accused repeating similar behaviour. One further incident was witnessed through the window by both children three hours after the first incident. The accused was convicted of harassment under section 10 of the 1997 Act and this conviction was upheld on appeal to the High Court. The Court held that the core requirement of persistence in section 10 is that the behaviour involved is continuous, which means it can consist of either (a) a number of incidents, such as in the case, that are separated by intervening lapses of time, or (b) a single, but continuous, incident such as following a person on an unbroken journey over a prolonged distance.

1.07 *Lynch* illustrates that persistence requires continuing behaviour and will usually involve more than one incident and that it can include a single incident provided it is prolonged thereby meeting the test of continuity. When the Commission proposed the harassment offence in its 1994 Report it gave as an example of a situation where the offence could apply "the acts of the infatuated psychotic who follows a woman in order to gain her affections."[24] By the time of the Dáil debates on section 10 in 1997, the term "stalking" was used to describe it, the Minister for Justice noting that the "new offence of harassment... is aimed at what is commonly called stalking."[25] Stalking is commonly defined in a manner that is almost indistinguishable from harassment and the Oxford English Dictionary defines it as "the action, practice or crime of harassing or persecuting a person with unwanted, obsessive and usually threatening attention over an extended period of time".[26] Stalking is best understood as one form of harassment which is a wider offence that could encompass other behaviour not readily identifiable as stalking.[27] The Commission adopted this view in its *Report on Aspects of Domestic Violence*, concluding that stalking is included as a type of harassment under section 10.[28] Cyber-bullying generally refers to aggressive behaviour through the use of cyber technology which is intentional and involves an imbalance of power and strength.[29] Cyber-stalking has been described as

[23] [2008] IEHC 183, [2010] 3 IR 434: see the more detailed discussion in *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.22ff.

[24] Law Reform Commission *Report on Non-Fatal Offences Against the Person* (LRC 45-1994), paragraph 9.77.

[25] See Vol. 477 *Dáil Éireann Debates*, 15 April 1997, Second Stage debate on Non-Fatal Offences against the Person Bill 1997, where the Minister for Justice Nora Owen referred to the "new offence of harassment which is aimed at what is commonly called stalking." See also Vol. 478 *Dáil Éireann Debates*, 29 April 1997, Committee and Remaining Stages debate on Non-Fatal Offences against the Person Bill 1997, where the Minister of State at the Department of Social Welfare Bernard Durkan referred to the offence in section 10 as "harassment or as it is commonly known, stalking."

[26] As quoted in MacEwan, "The new stalking offences in English Law: will they provide effective protection from cyberstalking" (2012) Crim LR 767, at 768.

[27] Gillespie, "Cyberstalking and the law: a response to Neil MacEwan" (2013) Crim LR 38, at 39.

[28] Law Reform Commission *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.92.

[29] Shannon *Sixth Report of the Special Rapporteur on Child Protection* (Report submitted to the Oireachatas, January 2013) at 90.

involving a relentless pursuit of the victim online often in combination with an offline attack.[30] Just as stalking is commonly characterised as a sub-category of harassment, the Commission suggests that cyber-stalking and cyber-bullying that meet the test of persistence are best described as forms of cyber-harassment.

Examples of harmful internet communications

1.08 The following are examples of harmful internet communications which may or may not be covered by section 10 depending on whether the persistence requirement is met and the activity involved is direct rather than indirect in nature.

- Persistently sending harmful messages through text messaging, instant messaging, email, chat rooms or social networking websites. For example, in a 2013 case, a man was convicted under section 10 of the 1997 Act for sending up to 500 offensive text messages to a teenage boy.[31]
- Targeting the victim's computing technology. This type of behaviour arose in the English case *R v Debnath*,[32] where the accused paid a group of hackers to sabotage the complainant's email account. Computer hacking is an offence under the *Criminal Damage Act 1991.*[33]
- Setting up harmful websites or fake profile pages on social networking sites, in order to impersonate the victim and post harmful or private content in the victim's name. This also featured in *Debnath* where the accused set up a website called "[name of complainant] is gay.com" and registered the complainant on a database for people with sexually transmitted diseases. The accused was convicted of harassment under section 2 of the UK *Protection from Harassment Act 1997*. As noted below, this indirect activity might not come within section 10 of the 1997 Act.
- Posting intimate images or videos online without consent. This type of activity received international attention in 2014 when intimate photos and videos of well-known personalities, including the actress Jennifer Lawrence, were posted online after their iCloud accounts had been hacked. This clearly involved hacking but might not come within section 10 of the 1997 Act.

Application of section 10 of 1997 Act to cyber-harassment in general

1.09 Section 10 of the 1997 Act can be applied to many forms of harmful internet behaviour, including cyber-harassment, because section 10(1) provides that harassment may be carried out "*by any means* including by use of telephone" (emphasis added). The specific reference to the telephone ensures that behaviour such as silent phone calls are captured by the offence. The reference to "by any means" ensures that other forms of communication such as email, messages sent through a social network site or text messages can be classed as harassment, so that the offence is not confined to more traditional, offline stalking activities such as following or watching which are also

---

[30] Jameson, "Cyberharassment: Striking a Balance between Free Speech and Privacy" (2008) 17 Comm Law Conspectus 231, at 236.

[31] Man guilty of 'malicious and evil' bullying of boy through text messages" *Irish Independent* 22 January 2013 available at http://www.independent.ie/irish-news/courts/man-guilty-of-malicious-and-evil-bullying-of-boy-through-text-messages-28947459.html.

[32] *R v Debnath* [2005] EWCA Crim 3472.

[33] The 1991 Act is discussed at paragraph 2.09 below.

listed in section 10. A number of prosecutions under section 10 have involved harassment through sending unwanted, inappropriate or harmful emails, text messages and posting harmful content online.

1.10 The cases outlined below come within section 10 of the 1997 Act because each involved a cyber attack that continued over a prolonged period.

1.11 They show that prosecutions have been brought pursuant to section 10 where there has been cyber-harassment, in particular in cases involving direct contact with the victim. However, difficulties may arise in applying section 10 to certain forms of indirect harassment, that is, harmful behaviour directed towards a person other than the victim but concerning the victim. The ease with which individuals can communicate with others and disseminate content online means that indirect harassment is particularly likely to be carried out through cyber means.[34]

- A 2011 case involved a man who pleaded guilty to harassing his ex-girlfriend over a three year period. The man had sent emails, texts and threatening letters to the victim and had also sent a threatening letter to one of her work colleagues.[35]
- In 2013, a man pleaded guilty to harassment after sending up to 500 text messages to a teenage boy which were "abusive, threatening or sexually explicit" in nature.[36] Text messages were also sent to people living in the local area claiming to be from the victim and signed off by him, resulting in the victim being assaulted by a number of people.
- In a 2014 case, a man pleaded guilty under section 10 after posting explicit items on a website about the victim, whom he had briefly dated seven years before, suggesting she was offering sexual favours.[37]

1.12 Harassment has also been charged in cases involving covert filming.

In 2012, a man who installed a hidden camera in a women's locker room pleaded guilty to harassment of eight women who were staff at the hospital where the locker room was located. The camera had been in place for 6 months before it was spotted. The accused admitted using the camera to record 885 images and 30 videos of the women undressing and in their underwear. The victims, who were previously on good terms with the defendant, said they felt betrayed and repulsed by his actions. One of them was unable to socialise for six months and had made an attempt at suicide.[38]

[34] The Commission noted this in its *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.94.

[35] This case is discussed in Shannon *Sixth Report of the Special Rapporteur on Child Protection* (Report Submitted to the Oireachatas, January 2013) at 95.

[36] "Man guilty of 'malicious and evil' bullying of boy through text messages" *Irish Independent* 22 January 2013 available at http://www.independent.ie/irish-news/courts/man-guilty-of-malicious-and-evil-bullying-of-boy-through-text-messages-28947459.html.

[37] "Man avoids jail for vile internet messages about ex-girlfriend" *Irish Times* 20 March 2014 available at http://www.irishtimes.com/news/crime-and-law/courts/man-avoids-jail-for-vile-internet-messages-about-ex-girlfriend-1.1731368.

[38] "Man hid camera to spy on women in shower" *Irish Independent* 18 December 2012 available at http://www.independent.ie/irish-news/courts/man-hid-camera-to-spy-on-women-in-shower-28948811.html.

1.13 These examples meet the persistence requirement in section 10 because they involved repeated acts over an extended period and also illustrate that it is capable of capturing many types of cyber-harassment.[39]

1.14 Nonetheless, it may be desirable to include a specific reference to cyber-harassment in section 10 as it would clarify the scope of the section and might increase reporting and prosecution of cyber-harassment cases. In 2013 a number of representative groups, in submissions to the Oireachtas Joint Committee on Transport and Communications, agreed that there was a need to clarify that existing law applied to cyber-harassment.[40] A public awareness campaign would educate the public about the dangers of cyber-harassment. Expressly identifying cyber-harassment in the legislation as a particular form of the wider offence of harassment would underline society's recognition of its seriousness and the need to prevent and punish it.

1.15 Studies conducted on cyber-bullying regularly find that individuals are reluctant to report such behaviour.[41] Amongst children and adolescents the most common reasons for under-reporting include the belief that adults will not be able to understand or respond adequately to the problem. This belief arises from the perception on the part of children and adolescents that they possess greater technological understanding and ability than pre-digital era adults. Connected to this belief is the fear that if the child or adolescent tells a parent they are being cyber-bullied their own internet access or devices may be taken away from them.[42] Even where a child tells an adult about cyber-bullying or harassment to which they have been subjected, adults may form the view that reporting the problem to the Gardaí is not a suitable option considering the potentially serious consequences of engaging the criminal law. The anonymous nature of much cyber-harassment also creates challenges for both adult and child victims, who may believe that reporting the behaviour is pointless because the perpetrator cannot be identified.[43] This is despite the fact that anonymity online is largely a misplaced perception because an individual's identity can usually be uncovered through his or her IP address.

---

[39] The Minister for Justice noted in 2012 that section 10 applies to cyber-bullying: see Vol. 781 *Dáil Éireann Debates*, p.754 (7 November 2012), Topical Issues Debate: Cyberbullying, available at www.oireachtas.ie. To the same effect see Joint Committee on Transport and Communications *Report on Addressing the growth of Social Media and tackling Cyberbullying* (Government Publications, 2013) at 34.

[40] These included the Anti-Bullying Coalition, Digital Rights Ireland, the Irish Immigrant Support Centre (Nasc) and Spunout.ie (a youth focused website funded by the HSE): see Joint Committee on Transport and Communications *Report on Addressing the growth of Social Media and tackling Cyberbullying* (Government Publications, 2013) at 34 and 38.

[41] See for example, Doherty *A study of cyberbullying of students in Irish third level education* (NUI Galway, 2014) at 5, which found that over half of those surveyed who were cyber-bullied did not report the cyber-bullying. See also O'Moore and Minton *Cyber-Bullying: The Irish Experience* (Nova Science Publishers, 2011) which investigates the experience of post-primary school children with cyber-bullying and finds that only 6% of children who said they had experienced cyber-bullying reported it to adults at school.

[42] See O'Higgins Norman "Report on Cyberbullying Research and Related Issues" Conference Paper, Ist National Cyberbullying Conference (1 September 2014) at 2. This Paper also notes that the reluctance to report may be "partly attributable to the ambiguity of online comments, whereby it is difficult to prove that a comment or action is directed at a particular individual and/or intended to be hurtful."

[43] Srivastava & Boey "Online Bullying and Harassment: An Australian Perspective" (2012) 6 Massaryk U J L &Tech 299, at 313.

Application of section 10 of 1997 Act to indirect cyber-harassment

1.16 In the Commission's 2013 *Report on Aspects of Domestic Violence*, it was noted that consultees had recommended that indirect harassment should be an offence.[44]

1.17 Indirect cyber-harassment involves persistent harmful communications through email, social networking sites or other cyber means to third parties concerning a complainant but not directly communicated to the complainant. It would include, for example, situations where a defendant spreads harmful information whether true or false to the complainant's friends or family. It might also involve repeatedly posting content online to the public at large concerning a complainant. There may be a gap in Irish law in relation to indirect harassment and this view was shared by the Minister for Communications, Energy and Natural Resources in 2013 when he stated that the 1997 Act dealt with "direct communications with someone" but "it does not deal with communication *about* someone and is being interpreted in a very narrow sense by the courts."[45] Comprehensively criminalising indirect harassment could be done by amending section 10 to include harassing communications with "any person" rather than just the target of the harassing behaviour. In the cyber context, this would clarify that it is a crime to post harassing communications on a publicly available website and to send cyber communications to third parties which are harmful to the victim.

In the English case *R v Debnath,*[46] the defendant was convicted of harassment pursuant to section 2 of the *Protection from Harassment Act 1997*. The defendant and the complainant had a one night stand after which the defendant mistakenly believed she had contracted a sexually transmitted disease. This sparked a year-long campaign by her of harassing the complainant, mainly through cyber means. This included sending the complainant's fiancée emails claiming to be from one of the complainant's friends detailing alleged sexual indiscretions and sending the complainant's former employers an email, also claiming to be from him, which falsely alleged that the complainant had harassed the defendant. The defendant also registered the complainant on a database for individuals with sexually transmitted diseases seeking sexual liaisons and on a gay American prisoner exchange. The defendant also set up a website claiming that the complainant was gay.

1.18 Section 10 of the Irish 1997 Act requires that the accused engage in "following, watching, pestering, besetting or communicating with" the victim. The requirement to communicate with the victim means that it is unlikely that section 10 could be interpreted as applying to all forms of indirect activity. So where the offending communication is sent not to the victim but to others there may be no communication with the victim. The specific language used in section 10 would appear to exclude the indirect type of behaviour involved in *Debnath.* Similarly, harmful messages posted on a private social networking page such as on Facebook may also not be covered by section 10 if they do not involve direct communication with the subject.

1.19 Nonetheless, in 2014 a prosecution was taken against a man who pleaded guilty to an offence under section 10 after posting explicit items on a website about the victim, whom he had briefly dated seven years before, suggesting she was offering sexual favours.[47] This suggests that there is a view that section 10 may extend to some situations where a complainant is exposed

---

[44] Law Reform Commission *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.21.

[45] Joint Committee on Transport and Communications *Report on Addressing the growth of Social Media and tackling Cyberbullying* (Government Publications, 2013) at 34.

[46] *R v Debnath* [2005] EWCA Crim 3472.

[47] See "Man avoids jail for vile internet messages about ex-girlfriend" *Irish Times* 20 March 2014, available at http://www.irishtimes.com/news/crime-and-law/courts/man-avoids-jail-for-vile-internet-messages-about-ex-girlfriend-1.1731368.

indirectly to publicly available content. So just as persistently displaying abusive placards about a person in public places might amount to traditional harassment, in the cyber context posting abusive content on publicly accessible websites or social networking profiles might amount to cyber harassment.

1.20 Indirect harassment is covered by the English *Protection from Harassment Act 1997* because it defines harassment in more general terms than section 10. It criminalises engaging in a "course of conduct" not necessarily against the victim, but which constitutes harassment of the victim.[48] In its *Report on Aspects of Domestic Violence*, the Commission recommended that the term "persistently" should be retained rather than adopting the "course of conduct" requirement as the "persistently" term is wider in scope.[49] This is because, as defined in the English Act, "course of conduct" requires at least two incidents, so that a single but continuous act cannot constitute harassment as it can under the Irish Act (as in *Director of Public Prosecutions (O'Dowd) v Lynch*[50]).

Indirect "revenge porn" may not be covered by section 10 of the 1997 Act

1.21 A particular form of indirect cyber activity is the persistent distribution to third parties of videos or images with embarrassing or intimate content occurring after a relationship breaks down. This activity is sometimes now referred to as "revenge porn".[51] The proliferation of mobile technology and the development of sites and apps that facilitate posting such material online mean that recording and distribution of content can easily be done. The mass release in 2014 of intimate photographs hacked from the online accounts of well-known personalities illustrates the potential for such behaviour to be carried out on an industrial scale.[52]

In the Canadian case *R v DeSilva*,[53] the defendant made a sexually explicit video of the complainant without her knowledge while they were in a relationship. After the relationship ended, the defendant posted the video on his Facebook page and then sent 13 friends and family an email inviting them to view the video which was sent as an attachment to the emails. The defendant also made threats to the victim including through a series of emails where he taunted the victim about the video. The defendant was convicted of the offence of voyeurism[54] for making and distributing the video and harassment in relation to the threats he made to the victim. Although the video was not widely

[48] Section 2(1) of the UK *Protection from Harassment Act 1997* provides that "[a] person who pursues a course of conduct in breach of section 1 is guilty of an offence". Section 1 of the UK 1997 Act provides:

> "A person must not pursue a course of conduct—
> (a) which amounts to harassment of another, and
> (b) which he knows or ought to know amounts to harassment of the other."

Harassment is not defined in the UK 1997 Act.

[49] Law Reform Commission *Report on Aspects of Domestic Violence* (LRC 111-2013) at paragraph 2.101.

[50] [2008] IEHC 183, [2010] 3 IR 434.

[51] For a discussion of one individual's experience with "revenge porn" see "I was a victim of revenge porn. I don't want anyone else to face this" *The Guardian* 19 November 2013 available at http://www.theguardian.com/commentisfree/2013/nov/19/revenge-porn-victim-maryland-law-change.

[52] "Nude photos of Hollywood actors posted online by alleged hacker" *The Irish Times* 1 September 2014 available at http://www.irishtimes.com/news/technology/nude-photos-of-hollywood-actors-posted-online-by-alleged-hacker-1.1914402.

[53] *R v DeSilva* 2011 ONCJ 133.

[54] The voyeurism aspect of the case is discussed at paragraph 2.16 below.

distributed in this case, because the police were alerted at a relatively early stage resulting in the video being removed from Facebook, the court could still not be satisfied that the video was confined to the 13 people who were sent it.

1.22 If the *DeSilva* case had arisen in Ireland, the series of email threats made directly to the victim by the defendant would probably meet the persistence requirement in section 10 of the 1997 Act.[55] If, however, the case had only involved the emails and video sent by the defendant to his friends, it is unlikely that this would meet the requirement in section 10 that the defendant had been "communicating with" the victim. Posting the video on a Facebook page might possibly be prosecuted successfully under section 10 if the complainant had access to the page.

Jurisdictional issues and cyber-harassment: extra-territorial effect

1.23 The extent to which the offence of cyber-harassment should have extra-territorial effect is important.[56] The internet is not confined to "a single geographical area nor is it neatly divisible along territorial boundaries into distinct local networks."[57] People may be subject to cyber-harassment from perpetrators or sites located outside the State and, conversely, perpetrators based in the State may harass individuals based outside it. Article 29.8 of the Constitution provides that the State may legislate with extra-territorial effect, which must be done expressly, so it is permissible to provide that the harassment offence should have extra-territorial effect but this has not been done. The EU, in a Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law has also stated that Member States "shall take necessary measures" to establish extra-territorial jurisdiction in cases involving offences relating to racism and xenophobia.[58]

1.24 If section 10 of the 1997 Act were amended to provide for extra-territorial effect, it would be desirable that there be a connection to the State before jurisdiction could be exercised so that the State's jurisdiction would be effective in practice. This would limit extra-territorial jurisdiction to situations where either the victim was based within the State but the perpetrator was not, or the perpetrator was based within the State and the victim was not. There are a number of examples where the Oireachtas has expressly provided that offences have extra-territorial effect which could offer guidance in this respect. Under the *Criminal Damage Act 1991*[59] an offence of criminal damage to data[60] committed by a person outside the State in relation to data kept within the State may be prosecuted and the offence may for all purposes be treated as having been committed in any place in the State. Similarly, the *Sexual Offences (Jurisdiction) Act 1996*, which applies to sexual offences involving children, provides that where a citizen of the State or a person who is ordinarily resident in

---

[55] As noted at paragraph 1.12 above, section 10 has been used in cases involving covert filming.

[56] Similar considerations arise in the context of the offence proposed in Issue 2, below; and in the context of civil remedies, which are discussed in Issue 5, below.

[57] Biswas "Criminal liability for cyber defamation: jurisdictional challenges and related issues from Indian jurisprudence" (2013) CLTR 121, at 125.

[58] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law. This Framework Decision is discussed further at paragraph 3.09 below.

[59] Section 7(1) of the *Criminal Damage Act 1991* provides:

> "Proceedings for an offence under section 2 or 5 alleged to have been committed by a person outside the State in relation to data kept within the State or other property so situate may be taken, and the offence may for all incidental purposes be treated as having been committed, in any place in the State."

[60] The offences under the 1991 Act are discussed at paragraph 2.09 below.

the State does an act in another country involving a child that is an offence in that country and, if done in the State, would also be an offence in the list of offences scheduled to or specified for the 1996 Act (including child trafficking and child pornography), [61] he or she can be prosecuted in the State for such a scheduled or specified offence.[62]

1.25 Notwithstanding these existing examples, it should also be noted that, in the specific context of harmful internet behaviour, the possible extension of section 10 of the 1997 Act to activity committed outside the State may involve a conflict between behaviour that constitutes an offence under Irish law but which may be regarded as the permissible exercise of free speech in another jurisdiction.[63]

1(a): Do you consider that section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be amended to include a specific reference to harassment by cyber means?

1(b): Do you consider that section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be amended to include indirect forms of harassment, including persistent posting online of harmful private and intimate material in breach of a victim's privacy?

1(c): Do you consider that section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be amended to provide expressly that it should have extra-territorial effect, provided that either the victim or the perpetrator is based within the State?

Please type your comments (if any)

[61] The offences in section 3 (child trafficking and taking etc. child for sexual exploitation) and section 4 (allowing a child to be used for child pornography) of the *Child Trafficking and Pornography Act 1998* are specified offences for the purposes of the *Sexual Offences (Jurisdiction) Act 1996*.

[62] Section 2(1) of the *Sexual Offences (Jurisdiction) Act 1996.*

[63] See the comparable considerations in extra-territorial civil proceedings, including the discussion at paragraph 5.23, below, of *Yahoo! Inc v LICRA*, 169 F Supp 2d 1181 (ND Cal, 2001); 433 F 3d 1199 (9th Circuit, 2006).

ISSUE 2: WHETHER THERE SHOULD BE AN OFFENCE OF SERIOUSLY INTERFERING THROUGH CYBER TECHNOLOGY WITH ANOTHER PERSON'S PRIVACY

2.01 The amendments to section 10 of the 1997 Act canvassed in Issue 1 above are limited to considering whether the offence of harassment should explicitly include cyber-harassment and whether it should be extended to include indirect forms of harassment. The Commission recommended in its 2013 *Report on Aspects of Domestic Violence* that harassment should be confined to persistent behaviour,[64] as described in *Director of Public Prosecutions (O'Dowd) v Lynch*,[65] namely behaviour that is continuous in that it consists of either (a) a number of incidents that are separated by intervening lapses of time or (b) a single incident but of a prolonged type.[66]

2.02 Limiting harassment to persistent behaviour means that posting content online by a single upload which seriously interferes with a person's privacy will not amount to harassment because the communication will not have been made persistently. Where material is uploaded once on to the internet it is not certain that the requirement in section 10 of the 1997 Act of "persistence" is met. This is so even though the single once-off upload may be available permanently to large communities of users or the world at large. Such a posting can nowadays be done almost instantly at the press of a button. This issue explores whether such an interference with a person's privacy should be criminalised where it is sufficiently damaging to the person and where there is no public interest involved in the dissemination of the content sufficient to justify it. Alternatively, civil remedies available to individuals in such situations of damages and appropriate take-down orders may be considered adequate (see Issue 5 below).

2.03 The internet and other digital communications technologies have created new and potentially insidious ways in which individual privacy can be compromised. The online world leaves individuals vulnerable to serious privacy violations through the posting of private, false, humiliating, shameful or otherwise harmful content, notably through social networking websites such as Facebook, Twitter or YouTube, without the consent of the subject. The harm that is caused by such violations of privacy can be significant because content that is posted online can be spread instantly and widely, possibly reaching global audiences.[67]

2.04 The permanence of online content as well as the potential for such content to go viral and remain in the public consciousness and publicly available after the initial upload means that such interferences with privacy can have substantial long term consequences, such as harming future employment prospects and having harmful effects on the individual's physical or mental health. This is despite the fact that the content may only have been uploaded once.

2.05 Before discussing whether such behaviour should be made subject to the criminal law it is important to consider to what extent existing offences capture once-off harmful activity.

---

[64] *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.97.

[65] [2008] IEHC 183, [2010] 3 IR 434, discussed at paragraph 1.06 above.

[66] *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraphs 2.93-2.94.

[67] See O'Higgins Norman "Report on Cyberbullying Research and Related Issues" Conference Paper, Ist National Cyberbullying Conference (1 September 2014) at 3, where the author notes that "a single action, which is then shared or repeated by others, may be as harmful as repeated incidents".

Other relevant criminal offences

2.06 Offences, in section 13 of the *Post Office (Amendment) Act 1951* (as amended in 2007) and in the *Criminal Damage Act 1991* are capable of capturing some but not all forms of harassment, including cyber-harassment.

Section 13 of the Post Office (Amendment) Act 1951 (as amended in 2007)

2.07 Section 13 of the *Post Office (Amendment) Act 1951* (as amended by the *Communications Regulation (Amendment) Act 2007*) provides:

> "(1) Any person who—
> (a) sends by telephone any message that is grossly offensive, or is indecent, obscene or menacing, or
> (b) for the purpose of causing annoyance, inconvenience, or needless anxiety to another person—
> (i) sends by telephone any message that the sender knows to be false, or
> (ii) persistently makes telephone calls to another person without reasonable cause,
> commits an offence...
> (5) In this section, 'message' includes a text message sent by means of a short message service (SMS) facility."

2.08 Section 13, as amended, only applies to telephone and text messages. By contrast with section 10 of the 1997 Act, it catches once-off events where there is no persistence or where it would be difficult to prove. As noted above, the 2014 *Report of the Internet Content Governance Advisory Group* has recommended that section 13 be amended to include electronic communications in the definition of measures dealing with the "sending of messages which are grossly offensive, indecent, obscene or menacing"[68] and the Commission agrees with this recommendation. At the launch of the 2014 Report, the Minister for Communications, Energy and Natural Resources stated that the Government would prepare legislation to implement this recommendation.[69]

Criminal Damage Act 1991

2.09 The *Criminal Damage Act 1991*[70] replaced 19th century legislation on criminal damage. It took account of advances in technology, so that it can be applied to cyber communication where an individual's computing technology is targeted by unauthorised access or hacking of their email, social

---

[68] *Report of the Internet Content Governance Advisory Group* (Department of Communications, Energy and Natural Resources, 2014) at 9.

[69] At the launch of the Report, the Minister for Communications, Energy and Natural Resources, Pat Rabbitte TD, stated that "It is a clarificatory statement rather than a major change. But I am committed to it and we should do it". See "Online and text message bullying to be criminalised" *Irish Times* 24 June 2014 available at http://www.irishtimes.com/news/politics/online-and-text-message-bullying-to-be-criminalised-1.1843858.

[70] The 1991 Act implemented the Commission's 1988 *Report on Malicious Damage* (LRC 26–1988), which recommended that the English *Malicious Damage Act 1971* be used as a model for reform. The Commission's 1988 Report noted (at paragraph 20) that "[a]dvances in technology can also result in new applications of the concept of 'damage'." The Commission also noted that the English 1971 Act was able to take account of such developments and referred to *Cox v Riley* [1986] Crim L Rev 460, in which the defendant was convicted of criminal damage under the 1971 Act when he erased programmes from a plastic circuit card used to operate a computerised saw. As the Commission noted, this was because the card was undoubtedly "property of a tangible nature" under the 1971 Act and the erasure of the programmes constituted damage.

networking or other type of internet-based account to send harmful messages or post harmful material. The 1991 Act extends to the deletion and modification of data.[71] Section 2(1) provides:

> "A person who without lawful excuse damages any property belonging to another intending to damage any such property or being reckless as to whether any such property would be damaged shall be guilty of an offence."

2.10 "Damage" in relation to data is defined in section 1(1) of the 1991 Act as:

> "(i) to add to, alter, corrupt, erase or move to another storage medium or to a different location in the storage medium in which they are kept (whether or not property other than data is damaged thereby), or
>
> (ii) to do any act that contributes towards causing such addition, alteration, corruption, erasure or movement."

In 2014, a man was fined €2,000 after pleading guilty to criminal damage under the 1991 Act for posting an offensive "status update" on his ex-girlfriend's Facebook page.[72] The accused stole the woman's phone which he then used to log in to Facebook to post a status update in her name stating that she was a "whore" and would take "any offers"- an example of what has come to be known as "fraping."[73] The DPP stated that the offence had more in common with harassment than criminal damage and that the harm was reputational rather than monetary. The Court noted that there was no relevant procedure to guide sentencing in the case but stated that it was a reprehensible offence that seriously damaged the woman's good name.

2.11 This case was the first and to date only prosecution in Ireland for criminal damage to a social media account and illustrates the merits of the clear but relatively general language of the 1991 Act which was drafted over a decade before the first social media site appeared. By contrast with the requirement for persistence in section 10 of the 1997 Act, the 1991 Act applies to once-off activity.

Data Protection Acts 1988 and 2003

2.12 The *Data Protection Act 1988*, as amended by the *Data Protection (Amendment) Act 2003*, protects an individual's right to privacy with regard to the collection, use and disclosure of personal information or "data" by organisations. The Acts provide remedies where personal data is posted online without the consent of the subject. As the unlawful activity contrary to the Acts does not have to be done "persistently" once-off incidents are capable of being an offence. "Personal data" includes harmful content such as harmful messages, videos or images. The Acts involve the implementation of

---

[71] Section 1(1) of the *Criminal Damage Act 1991* defines "property" to include data, as follows:

> " 'property' means—
> (a) property of a tangible nature, whether real or personal, including money and animals that are capable of being stolen, and
> (b) data."

Section 1(1) defines "data" as "information in a form in which it can be accessed by means of a computer and includes a program."

[72] "Man avoids jail for 'criminal damage to Facebook page'" *Irish Times* 30 June 2014 available at http://www.irishtimes.com/news/crime-and-law/courts/man-avoids-jail-for-criminal-damage-to-facebook-page-1.1850417.

[73] The process of accessing someone's Facebook page and posting an embarrassing status update as a prank is often referred to as "fraping." See "Court's ruling on 'fraping' sets legal precedent" *Irish Independent* 01 July 2014 available at http://www.independent.ie/opinion/comment/courts-ruling-on-fraping-sets-legal-precedent-30396062.html.

a 1981 Council of Europe Convention[74] and a 1995 EU Directive on Data Protection[75] and therefore this is a matter that has been largely harmonised across Europe which makes remedies more accessible and enforceable where the personal information is being hosted in another country. However, as noted by both the Oireachtas Committee on Transport and Communications and the Internet Content Governance Advisory Group, there appears to be limited public awareness of data protection rights and the remedies provided by the Acts are not often pursued.[76]

2.13 For individuals to avail of the remedies under the Data Protection Acts, the content posted online must be "personal data" defined as "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". [77] This includes images, videos, comments about the person and other identifying information including his or her phone number or address. The data must be held by a "data controller"[78] and this definition includes social networking and other websites.[79] The Acts do not apply to "personal data kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes."[80] This is known as the "household exemption" and it will generally exclude personal data posted on private social networking pages.[81] However, where individuals post personal data on a public website about another person without that other's consent the exemption will not apply because making information available for all to see is not regarded as a purely personal or recreational purpose and the user will assume the full responsibility of a data controller[82]. It has been stated that where a user has "a high number of third party contacts some of whom he may not actually know" this may be an indication that

---

[74] Council of Europe, Convention for the Protection of individuals with regard to Automatic Processing of Personal Data (28 January 1981).

[75] Directive 95/46/EC. A new Data Protection Regulation, to replace the 1995 Directive, is expected to be adopted in 2015. See Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (January 2012) 2012/0011 (COD).

[76] See Oireachtas Joint Committee on Transport and Communications, *Report on Addressing the growth of Social Media and tackling Cyberbullying* (Government Publications, 2013) at 35; and *Report of the Internet Content Governance Advisory Group* (Department of Communications, Energy and Natural Resources, 2014) at 41.

[77] Section 1 of the *Data Protection Act 1988.*

[78] Section 1 of the *Data Protection Act 1988* defines a "data controller" as "a person who, either alone or with others, controls the contents and use of personal data."

[79] See Article 29 Data Protection Working Party *Opinion 5/2009 on online social networking* 01189/09/EN WP 163 (June 2009) at 5.

[80] Section 1(4)(c) of the *Data Protection Act 1988*, implementing the "household exemption" in Article 3.2 of Directive 95/46/EC.

[81] Article 29 Data Protection Working Party *Opinion 5/2009 on online social networking* 01189/09/EN WP 163 (June 2009) at 5.

[82] See *Lindqvist, Bodil, Criminal Proceedings against* (C-101/01) [2004] ECR I 12971, paragraph 47, in which the EU Court of Justice stated in connection with the "household exemption" in Article 3.2 of Directive 95/46/EC:

> "That exception [the household exemption] must therefore be interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people."

This case concerned a woman who was charged with breaching Swedish Data Protection legislation for publishing on her internet site personal data on a number of people she worked with. A number of questions were referred to the EU Court of Justice including whether the woman was a data controller.

the household exemption does not apply and the user would be considered a data controller.[83] Therefore, if an individual posts personal information about another person on a publicly available website or even a social networking page which is accessible to a large number of people the individual may be a data controller and the person harmed may have rights under the Data Protection Acts.

2.14 For the Data Protection Acts to apply, the data controller must either be established in the State and the data in question processed in the context of that establishment[84] or in the case of data controllers not established in the State or in any other EEA state, they must be using "equipment in the State for processing the data otherwise than for the purpose of transit through the territory of the State.[85]"

2.15 Individuals have the right to request the removal or rectification of personal data. These rights can be exercised at first instance through making a written request directly to the data controller.[86] In the event that a request is not complied with by the data controller, the individual can refer a complaint to the Office of the Data Protection Commissioner[87] who will attempt to settle the dispute by amicable resolution and will notify the individual if this is not possible.[88] If the Commissioner is of the opinion that a person contravened or is contravening a provision of the Acts, other than a provision the contravention of which is a criminal offence, then he or she may issue an enforcement notice requiring the person to take such steps specified in the notice within a required

---

[83] See Article 29 Data Protection Working Party *Opinion 5/2009 on online social networking* 01189/09/EN WP 163 (June 2009) at 6.

[84] Section 1(3B)(a)(i) of the *Data Protection Act 1988.* See also section 1(3B)(b) which provides that for the purposes of section 1(3B)(a) each of the following shall be treated as established in the State:

> "(i) an individual who is normally resident in the State,
> (ii) a body incorporated under the law of the State,
> (iii) a partnership or other unincorporated association formed under the law of the State, and
> (iv) a person who does not fall within subparagraphs (i), (ii) or (iii) of this paragraph, but maintains in the State—
> (I) an office, branch or agency through which he or she carries on any activity, or
> (II) a regular practice, and the reference to establishment in any other state that is a contracting party to the EEA Agreement shall be construed accordingly."

[85] Section 1(3B)(a)(ii) of the *Data Protection Act 1988.*

[86] Section 6 of the *Data Protection Act 1988* provides for a right of rectification or erasure, which allows an individual to request a data controller who keeps personal data relating to him or her to rectify or where appropriate, block or erase such data in relation to which there has been a contravention by the data controller of the data protection principles in section 2(1) of the 1988 Act. Section 2(1) provides that a data controller shall, as respects personal data kept by him or her, comply with the following data protection principles:

> "(a) the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly,
> (b) the data shall be accurate and complete and, where necessary, kept up to date,
> (c) the data—
> (i) shall have been obtained only for one or more specified, explicit and legitimate purposes,
> (ii) shall not be further processed in a manner incompatible with that purpose or those purposes,
> (iii) shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed, and
> (iv) shall not be kept for longer than is necessary for that purpose or those purposes,
> (d) appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."

[87] Section 10(1) of the *Data Protection Act 1988*. The Commissioner can also investigate where it is believed that there is a contravention even where no complaint is received.

[88] Section 10(1)(b)(ii) of the 1988 Act. This decision they may be appealed to the Circuit Court within 21 days.

time.[89] If a data controller is found to have contravened the data protection principles contained in section 2(1) of the Acts, this enforcement notice may require him or her to block, rectify erase or destroy the data concerned or supplement the data with a statement approved by the Commissioner.[90] It is an offence to fail or refuse to comply, without reasonable excuse, with an enforcement notice.[91] A person found guilty of an offence under the Acts is liable for a fine not exceeding €3,000 on summary conviction and to a fine not exceeding €100,000 for conviction on indictment.[92] Where a person is convicted under the Acts, the court may order any data which appears to the court to be connected with the commission of the offence to be forfeited or destroyed and any relevant data erased.[93]

How once-off interferences with privacy are dealt with in other jurisdictions: voyeurism and upskirting offences

2.16 As noted above, the Canadian case *R v DeSilva*[94] was dealt with as a voyeurism offence, which is not an offence in Irish law. Voyeurism involves observation or recording of another person doing a private act without their consent. This used to be referred to as a "Peeping Tom" offence and, more recently where it involves recording, as an "upskirting" offence. A key difference between harassment and voyeurism is that voyeurism may involve a single, once-off event that would not necessarily meet the persistence test in section 10 of the 1997 Act. Voyeurism is usually, though not always, done for the purposes of obtaining sexual gratification. Because of this, in some jurisdictions where it has been made an offence such as in the United Kingdom the offence is limited to circumstances where, for the purpose of obtaining sexual gratification, a person observes another person doing a private act, and the offence therefore forms part of the law on sexual offences.[95]

2.17 In other jurisdictions, voyeurism and covert filming, or "upskirting," is dealt with by an offence that is not necessarily connected with sexual offences law. For example, in Victoria, the *Summary Offences Amendment (Upskirting) Act 2007* inserted three new offences into its *Summary Offences Act 1966.* The first offence (section 41A) involves intentionally observing with the aid of a device such as a phone, another person's genital or anal region in circumstances in which it would be reasonable for that other person to expect that this region could not be observed. The second offence (section 41B) involves intentionally visually capturing an image of another person's genital or anal region in circumstances in which it would be reasonable for that other person to expect that this region could not be observed. The third offence (section 41C) provides that a person who visually captures or has visually captured an image of another person's genital or anal region (whether or not in contravention

[89] Section 10(2) of the *Data Protection Act 1988*.

[90] Section 10(3) of the *Data Protection Act 1988*. Under section 10(4), the person who is subject to the enforcement notice may appeal to the Circuit Court within 21 days of the notice being served on him or her.

[91] Section 10(9) of the *Data Protection Act 1988.*

[92] Section 31(1) of the *Data Protection Act 1988.*

[93] Section 31(2) of the *Data Protection Act 1988.*

[94] *R v DeSilva* 2011 ONCJ 133: see paragraph 1.21 above.

[95] See for example, section 67 of the English *Sexual Offences Act 2003* and Article 71 of the *Sexual Offences (Northern Ireland) Order 2008.* These voyeurism offences also extend to operating equipment to enable another person to observe, for the purpose of obtaining sexual gratification, a third person doing a private act.

of section 41B) must not intentionally distribute that image.[96] The court in *DeSilva* observed that the voyeurism element of that case was unusual because the defendant's actions were not motivated by a sexual purpose but rather by a desire to embarrass or humiliate the victim.[97] Voyeurism defined in this way could apply to some so-called "revenge porn" cases where intimate images or videos are posted online for the purposes of humiliating victims.

Should there be a specific offence of a once-off serious interference with privacy conducted through cyber technology?

2.18 The question here is whether an interference with a person's privacy carried out using cyber technology involving by a single action (i.e. a once-off action and not persistently) which can be shown to have the capacity to cause serious harm to the subject should be criminalised. The permanence and global reach of material when published on the internet makes any interference with privacy especially damaging and difficult to limit. Making this type of activity a crime has greater potential to discourage and prevent it than civil law remedies because of the greater deterrent effect of the criminal law and its superior ability to shape public behaviour. People tend to have more knowledge of the criminal than the civil law and are more likely to alter their behaviour to avoid its more serious consequences compared to the civil law. Once-off incidents conducted through cyber technology which seriously interfere with privacy are frequently carried out impulsively, facilitated by the technology being fast and easy to use and largely anonymous which creates a sense of distance between the person posting the material and the subject of it. Putting the matter in the hands of the Director of Public Prosecutions will remove the burden of prosecution from the victim and also the expense and initiative required for civil proceedings.

2.19 Two examples illustrate the type of material in question:

---

[96] In Canada, the *Protecting Canadians from Online Crime Bill* (which was passed by the Canadian House of Commons in October 2014) seeks to insert a similar offence into section 162.1 of the *Canadian Criminal Code*, which would provide:

> "(1) Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty
> (a) of an indictable offence and liable to imprisonment for a term of not more than five years; or
> (b) of an offence punishable on summary conviction."

This proposed offence would be confined to the publication and distribution of intimate images which are defined as "visual recording[s] of a person made by any means including a photographic, film or video recording" and:

> "(a) in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;
> (b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and
> (c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed."

[97] *R v DeSilva* 2011 ONCJ 133, paragraph 14. The Canadian voyeurism offence, under section 162 of the *Canadian Criminal Code*, does not require that the recording or observation be for a sexual purpose. Scotland's voyeurism offence under section 9 of the *Sexual Offences (Scotland) Act 2009* is also not confined to activities conducted to obtain sexual gratification and can apply to behaviour done for the purposes of "humiliating, distressing or alarming". In contrast, section 67 of the English *Sexual Offences Act 2003* and article 71 of the *Sexual Offences (Northern Ireland) Order 2008* require that the voyeuristic activity be done for the purposes of sexual gratification and any other purpose, in particular intent to humiliate or embarrass, would not be captured.

- In 2013, a teenage girl was filmed performing a sex act at a concert. This video was posted on a number of social networking sites and subsequently went viral. No charges were brought in this case as the girl made no complaint to the Gardaí.[98]

- In 2013, a teenage girl was filmed making embarrassing comments while drunk. This video also went viral and it would appear that in this instance there was no prosecution.[99]

2.20 In the first case, had the victim involved been under 17 years (which she was not) the individual responsible for the filming and upload might have been prosecuted under section 5 of the *Child Trafficking and Pornography Act 1998.*[100] The filming and upload of such a video might be an offence pursuant to section 13 of the *Post Office (Amendment) Act 1951* were that Act amended to include internet communications as that offence extends to "indecent" messages.[101]

2.21 The second case was not an offence under the 1951 Act as the content was not "grossly offensive, indecent, obscene or menacing" – it was embarrassing. While there might have been a breach of the *Data Protection Acts* if an enforcement notice made by the Data Protection Commissioner to remove the video had been made and not complied with, a data protection offence might not adequately reflect the serious interference with the subject's privacy that was involved in this case. In this case the video was instantly notorious and the young woman's privacy immediately and seriously damaged.

2.22 The question to be considered is whether there are breaches of privacy that are sufficiently serious that they should be criminalised because they have the capacity to interfere to a such a degree with a person's privacy and reputation that civil remedies alone, including remedies under civil privacy and defamation laws, are an inadequate response and deterrence and publication is unmatched by a public interest in having the information published. It would be necessary to ensure in any such offence that the law strike a proper balance between protecting privacy and guaranteeing freedom of expression. The breach of privacy should have to be more serious than just causing embarrassment to the victim. There should have to be significant humiliation involved not matched by a public interest in having the information published. The nature of the content disseminated would be a significant factor with the offence designed to capture serious interferences with privacy such as cases involving the upload of intimate content without consent or where the victim was engaging in behaviour that had the potential to be very harmful to his or her reputation.

2.23 Assessing the seriousness of the interference in the context of online content disseminated without consent would involve consideration of the extent to which the material was disseminated and the exposure it received. For example, if the material was sent only to one other person by email the interference would be unlikely to reach the necessary threshold of seriousness, unlike material posted on a public site such as YouTube or a public Facebook page. The age of the victim and the offender involved would also be important - behaviour between children or adolescents would in some cases be unsuitable for prosecution. Another significant factor would be the profile of the victim. The interference with privacy is likely to be much greater in the case of a private individual who engaged in humiliating behaviour filmed and disseminated online, in contrast to a celebrity seeking publicity and who suffered a similar fate.

---

[98] "No charges in 'Slane girl' case" *Irish Independent* 8 November 2013 available at http://www.independent.ie/irish-news/no-charges-in-slane-girl-case-29737095.html.

[99] See "KPMG asks staff to warn them of 'inappropriate coverage' of firm on net" *The Journal.ie* 23 January 2013 available at http://www.thejournal.ie/kpmg-social-media-kpmg-girl-765736-Jan2013/.

[100] Section 5 (producing, distributing etc., child pornography) of the *Child Trafficking and Pornography Act 1998.*

[101] See paragraph 2.08 above.

2.24 Where the seriousness threshold was not met, the civil law remedies would remain available for interferences with privacy.[102] So, in *Von Hannover v Germany*,[103] the European Court of Human Rights held that the plaintiff's right to privacy under the European Convention on Human Rights, though not her reputation, had been unlawfully interfered with when she was photographed in a public place without her consent and she was entitled to a civil remedy. Under the offence being suggested in this Paper, individuals would not face prosecution for disseminating content online that, while embarrassing, was not seriously damaging to the victim's reputation or privacy.

2.25 If such an offence were to be created, it is suggested that an intention to cause harm or recklessness as to whether harm was caused should be an essential element of the offence in order to protect the right to freedom of expression. This would ensure that the behaviour of individuals, particularly children or young people, who uploaded content without realising the potential for such behaviour to cause serious harm, would not commit the offence. For the correct balance to be struck between the right to privacy and freedom of expression, an essential element of the offence might be that there was no sufficient public interest in disseminating the material. Thus, if the material related to a public figure and the person who published the material reasonably believed that publication of the material was in the public interest, then the offence might not apply.

In *Herrity v Associated Newspapers (Ireland) Ltd,*[104] the High Court held that the right to privacy prevailed over the right to freedom of expression in a case involving material published by the defendant that was obtained unlawfully and where there was no overriding public interest in its publication.

2.26 Consideration would also have to be given to appropriate penalties were this new offence to be created. A person found guilty of an offence under section 10 of the 1997 Act is liable on summary conviction to a Class B fine (a fine not exceeding €2,500) and/or to imprisonment for a term not exceeding 12 months and on conviction on indictment to a fine and/or imprisonment for a term not exceeding 7 years.[105]

2.27 In summary, such an offence might contain the following elements:

- a serious interference with privacy;
- content that is disseminated online with the potential to cause serious harm because of the permanence and global reach of internet publication;
- no sufficient public interest in publication online; and
- intention or recklessness about causing harm on the part of the accused.

2.28 The offence of harassment in section 10 of the *Non-Fatal Offences Against the Person Act 1997* provides that otherwise lawful behaviour, such as watching and following, becomes criminal through the persistent nature of the behaviour and its harmful impact on a person's privacy. Similarly, the offence proposed would provide that publishing otherwise lawful information would become criminal because posting it on the internet and being accessible to the world at large has a permanent quality that corresponds to the persistent element in section 10 of the 1997 Act.

---

[102] See Issue 5 below.

[103] *Von Hannover v Germany* [2004] EMLR 379.

[104] *Herrity v Associated Newspapers (Ireland) Ltd* [2009] 1 IR 316. This case is discussed further at paragraph 5.12 below.

[105] Section 10(6) of the *Non-Fatal Offences Against the Person Act 1997* (as affected by section 6 of the *Fines Act 2010*).

2.29 The table below illustrates the comparison that may be made between section 10 and the proposed offence.

Section 10 of the *Non-Fatal Offences Against the Person Act 1997*	**Proposed offence of seriously interfering through cyber technology with another person's privacy**
Persistent behaviour	Once-off incidents involving content that has the capacity for permanence because it is posted online
Lawful behaviour that becomes criminal through persistence	Behaviour that becomes criminal because it has the capacity for permanence and global reach as it is conducted through cyber-technology
Intentional or reckless serious interference with another's peace and privacy or causes alarm, distress or harm	Intentional or reckless serious interference with another's peace and privacy and causes serious harm
No lawful authority or reasonable excuse	No lawful authority or reasonable excuse, no public interest in publication online

2.30 The question also arises whether to provide that the offence should have extra-territorial effect.[106]

2(a): Do you consider that there should be an offence introduced that would criminalise once-off serious interferences with another person's privacy where carried out through cyber technology?

2(b): If such an offence were to be introduced, do you consider that it should have extra-territorial effect?

2(c): Do you consider that any further reforms to the criminal law are needed to target harmful cyber behaviour affecting personal safety, privacy and reputation?

Please type your comments (if any)

[106] See the discussion of this in Issue 1 above in connection with the harassment offence in section10 of the 1997 Act. Similar considerations also arise in the context of civil remedies, which are discussed in Issue 5, below.

ISSUE 3: WHETHER CURRENT LAW ON HATE CRIME APPLIES TO ACTIVITY THAT USES CYBER TECHNOLOGY AND SOCIAL MEDIA

3.01 The Commission's project involves exploring the extent to which the current law on hate crime intersects or overlaps with cybercrime affecting personal safety, privacy and harassment.

3.02 The internet offers a substantial means to promote hatred and facilitate hate speech as it allows groups to mobilise, offer information to youthful or impressionable audiences and make verbal attacks on an instantaneous basis to wide audiences.[107] Increasingly, hate speech is found on mainstream and popular websites in particular social networking sites including Facebook and Twitter.

3.03 Online hate speech is criminalised by the *Prohibition of Incitement to Hatred Act 1989*. The 1989 Act prohibits incitement to hatred against a group of persons on account of their "race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation."[108] Incitement includes publication, broadcast and preparation of materials. The Act is not limited to offline behaviour as it extends to words used, behaviour or material displayed in "any place other than inside a private residence."[109] In 2011, a prosecution for online hate speech was taken under section 2 of the 1989 Act:

> In the so-called "Traveller Facebook case," the accused had created a Facebook page entitled "Promote the use of knacker babies for shark bait".[110] The accused was charged with an offence under section 2 of the 1989 Act. The case was dismissed in the District Court in 2011 on the basis that there was a reasonable doubt that there had been an intent to incite hatred against the Traveller community. The Court also took into account that the accused had only posted on the site once and had given an apology. However, while the accused only posted on the page once and sent it to three others before forgetting about it until notified by Facebook to remove it, 644 people had joined the page and many others may have viewed the page.[111] Some of those who joined also contributed further abusive material to the page.

3.04 This case illustrates the difficulties with online hate speech compared to its offline equivalents. Once an abusive comment is made it can spread very fast, be viewed by many people and remain accessible long after the content was posted.

3.05 Other legislation may also be used to prosecute in relation to online hate speech. This includes section 13 of the *Post Office (Amendment) Act 1951* (as amended by the *Communications Regulation (Amendment) Act 2007*), discussed above, because it applies to "grossly offensive" and

---

[107] Whine "Cyberhate, anti-semitism and counter legislation" (2006) Comms L 124, at 124.

[108] Section 1(1) of the *Prohibition of Incitement to Hatred Act 1989.*

[109] Section 2 of the 1989 Act provides:

> "(1) It shall be an offence for a person—
> (a) to publish or distribute written material,
> (b) to use words, behave or display written material—
> (i) in any place other than inside a private residence, or
> (ii) inside a private residence so that the words, behaviour or material are heard or seen by persons outside the residence, or
> (c) to distribute, show or play a recording of visual images or sounds,
> if the written material, words, behaviour, visual images or sounds, as the case may be, are threatening, abusive or insulting and are intended or, having regard to all the circumstances, are likely to stir up hatred."

[110] See Cummisky "Facebooked: Anti-Social Networking and the Law" 105(9) Law Society Gazette, November 2011 at 16.

[111] *Ibid* at 17.

"menacing" messages when sent by text or telephone (and would, if amended as recommended in the 2014 *Report of the Internet Content Advisory Group*, apply to online communications, including social media).[112]

3.06 Section 6 of the *Criminal Justice (Public Order) Act 1994* makes it an offence to "use or engage in any threatening, abusive or insulting words or behaviour with intent to provoke a breach of the peace or being reckless as to whether a breach of the peace may be occasioned". In England and Wales, public order offences committed online have been prosecuted under section 4(1) of the *Public Order Act 1986*,[113] which is broadly similar to section 6 of the 1994 Act:

In *R v Stacey*, the accused published, while drunk, an offensive tweet mocking the footballer Fabrice Muamba after he collapsed during a football match.[114] When other Twitter users criticised the accused for his comment, he responded with a series of "extremely abusive and insulting" as well as some racist tweets.[115] The accused was convicted under section 4(1)(a) of the *Public Order Act 1986* and sentenced to 56 days imprisonment.

3.07 Section 10 of the *Non-Fatal Offences Against the Person Act 1997* may be more difficult to apply to cases involving online hate speech as it requires the harassing behaviour to be carried out against an individual rather than a particular group.

3.08 Ireland has been encouraged to ratify the Council of Europe Convention on Cybercrime,[116] and the Additional Protocol to the Convention concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.[117] The Convention aims to facilitate the pursuit of a common policy on criminal law to protect society against cybercrime through the adoption of legislation and the fostering of international co-operation, while the Additional Protocol aims to ensure adequate legal responses to propaganda of racist and xenophobic nature committed through computer systems.

3.09 In 2008 the EU adopted Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law,[118] which contains very similar provisions to the Additional Protocol the Council of Europe Convention on Cybercrime. Thus, the Framework Decision requires that Member States take necessary measures to ensure that the following intentional conduct is punishable: (a) publicly inciting to violence or hatred directed against a

---

[112] See paragraph 2.08 above.

[113] Section 4(1) of the English 1986 Act provides that it is an offence to use towards another person "threatening, abusive or insulting words or behaviour" with "intent to cause that person to believe that immediate unlawful violence will be used against him or another by any person, or to provoke the immediate use of unlawful violence by that person or another, or whereby that person is likely to believe that such violence will be used or it is likely that such violence will be provoked."

[114] *R v Stacey* Crown Court 30 March 2012, judgment available at http://www.judiciary.gov.uk/Resources/JCO/Documents/Judgments/appeal-judgment-r-v-stacey.pdf.

[115] *Ibid* at paragraph 8 of the judgment.

[116] Council of Europe Convention on Cybercrime (23 November 2001). Ireland signed this Convention on 28 February 2002. See Schweppe and Walshe *Combating Racism and Xenophobia through the Criminal Law* (2008) at 161.

[117] Council of Europe*, Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (28 January 2003). See Schweppe, Haynes and Carr, *A Life Free From Fear: Legislating for Hate Crime in Ireland: An NGO Perspective* (2014).

[118] Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law.

group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin; (b) the commission of an act referred to in (a) by public dissemination or distribution of tracts, pictures or other material; (c) publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes, including those dealt with by the Nuremburg Tribunal after World War II (concerning the Holocaust).[119] The Framework Decision also requires that Member States ensure that their legislation extends to cases where the conduct is committed through an information system and the offender is within the territory of the Member State, even if the content hosted is not, and to cases where the material is hosted within the territory of the Member State whether or not the offender commits the conduct when physically present in its territory.[120] In its 2014 report on the implementation of the Framework Decision, the EU Commission noted that online hate speech is one of the most prevalent ways of manifesting racist and xenophobic attitudes and that Member States should have a means to intervene in such cases.[121] The Framework Decision also provides that a Member State shall take necessary measures to establish jurisdiction where the conduct has been committed by one of its nationals.[122] In this respect, the EU Commission's Report notes that the 1989 Act does not extend to such cases.[123] It also points out that infringement proceedings may be taken against Member States for failure fully to implement the Framework Decision from 1 December 2014.[124]

3.10 The general reform of hate crime, including the provisions in the 1989 and 1994 Acts, fall outside the scope of this project as this has become primarily a matter of EU law under the 2008 Framework Decision. The issue on which the Commission seeks views is therefore limited to whether the 1989 Act and other legislation including the 1951 Act and the 1994 Act adequately address online hate speech.

Q3: Do you consider that the *Prohibition of Incitement to Hatred Act 1989* and the *Criminal Justice (Public Order) Act 1994* adequately address hate speech activity disseminated through cyber technology and social media?

Please type your comments (if any)

[119] *Ibid* Article 1(1).

[120] *Ibid* Article 9(2).

[121] Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (January 2014) at 8.

[122] Article 9(1)(b) Council Framework Decision 2008/913/JHA. However, Article 9(3) provides:

> "A Member State may decide not to apply, or to apply only in specific cases or circumstances, the jurisdiction rule set out in paragraphs 1(b) and (c)."

Article 9(1)(c) applies to conduct that has been committed "for the benefit of a legal person that has its head office in the territory of that Member State."

[123] Report From the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (January 2014) at 8.

[124] *Ibid* at 2:

> " In accordance with Article 10(1) of Protocol No 36 to the Treaties, prior to the end of the transitional period expiring on 1 December 2014, the Commission does not have the power to launch infringement proceedings under Article 258 TFEU with regard to Framework Decisions adopted prior to the entry into force of the Treaty of Lisbon."

ISSUE 4: PENALTIES ON CONVICTION FOR OFFENCES

4.01 A number of recent high-profile prosecutions in the UK in connection with internet trolling have involved the offence of sending communications with intent to cause distress of anxiety under the *Malicious Communications Act 1988* for which at present the maximum sentence of imprisonment on conviction is six months. Section 29 of the UK *Criminal Justice and Courts Bill*, which at the time of writing is being debated in Parliament, proposes to increase the maximum sentence on conviction on indictment to two years. It is notable that the broadly equivalent offence in the State under section 13(1) of the *Post Office (Amendment) Act 1951* (as amended by *Communications Regulation (Amendment) Act 2007*) already carries a maximum sentence of five years.

4.02 The Commission seeks views on the appropriate maximum sentences that offences in this area should carry. It may be noted that in its 2013 *Report on Mandatory Sentences*, the Commission stated that the introduction of additional presumptive minimum sentences would not be an "appropriate or beneficial" response to other forms of criminality. [125] This recommendation was supported by the Department of Justice in its 2014 Strategic Review of Penal Policy.[126] The Commission's recommendation was based on the failure to establish that such sentences achieve the relevant sentencing aims of deterrence, retribution and rehabilitation and thus whether they further the overall aim of the criminal justice system to reduce criminality. The Commission observed that the presumptive minimum sentence regimes that apply to drugs and firearms offences frequently result in inconsistent and disproportionate sentencing due to the rigidity of such regimes which constrain the ability of the courts to punish offenders on an individualised basis.[127] Low level offenders are also disproportionately affected by presumptive minimum sentencing.[128]

4.03 The table below sets out the penalties under the current legislative provisions that apply to cyber-harassment and related behaviour.

Offence	**Section**	**Penalties**
S. 10 *Non-Fatal Offences Against the Person Act 1997*	s. 10(6)	Summary conviction: Class C fine (fine not exceeding €2,500) or imprisonment for a term not exceeding 12 months, or both. Conviction on indictment: an unlimited fine or imprisonment for a term not exceeding 7 years, or both.
S. 13(1) *Post Office (Amendment) Act 1951, as amended by Communications Regulation (Amendment) Act 2007*	s. 13(2)	Summary conviction: Class A fine (fine not exceeding €5,000) or imprisonment for a term not exceeding 12 months, or both. Conviction on indictment: fine not exceeding €75,000 or imprisonment for a term not exceeding 5 years, or both.

[125] Law Reform Commission *Report on Mandatory Sentences* (LRC 108-2013) at paragraph 4.237.

[126] *Strategic Review of Penal Policy Final Report* (Department of Justice and Equality, 2014) at 98.

[127] The Commission recommended that these regimes be repealed. See Law Reform Commission *Report on Mandatory Sentences* (LRC 108-2013), paragraph 4.238.

[128] *Ibid*, paragraph 4.226.

S. 2(1) *Criminal Damage Act 1991*	s. 2(5)	Summary conviction: Class C fine (fine not exceeding €2,500) or imprisonment for a term not exceeding 12 months, or both. Conviction on indictment: fine not exceeding €22,220 or imprisonment for a term not exceeding 10 years, or both.
S. 10(9) *Data Protection Act 1988, as amended by Data Protection (Amendment) Act 2003*	s. 31	Summary conviction: Class B fine (fine not exceeding €4,000). Conviction on indictment: fine not exceeding €100,000.
S. 2 *Prohibition of Incitement to Hatred Act 1989*	s. 6	Summary conviction: Class C fine (fine not exceeding €2,500) or imprisonment for a term not exceeding 6 months, or both. Conviction on indictment: fine not exceeding €25,400 or imprisonment for a term not exceeding 2 years, or both.
Ss. 6 and 7 Criminal Justice (Public Order) Act 1994	s. 6(2) s. 7(2)	Summary conviction: Class D fine (fine not exceeding €1000) or imprisonment for a term not exceeding 3 months, or both. Summary conviction: Class D fine (fine not exceeding €1000) or imprisonment for a term not exceeding 3 months, or both.

4.04 Although there have been a limited number of prosecutions for cyber-harassment and related activity, a preference for suspended sentences and fines rather than custodial sentences can nonetheless be observed. Thus, in cases involving convictions for cyber-harassment under section 10 of the 1997 Act, suspended sentences have frequently been applied:

- A 2011 case involved a man who pleaded guilty to harassing his ex-girlfriend through emails, texts and letters over a three year period.[129] He was sentenced to four months imprisonment which was suspended for 12 months.
- In 2013, a man pleaded guilty to harassment after sending up to 500 text messages to a teenage boy which were "abusive, threatening or sexually explicit" in nature. He also sent text messages to other people claiming to be from the victim.[130] The man was sentenced to six months

[129] This case is discussed in Shannon *Sixth Report of the Special Rapporteur on Child Protection* (Report submitted to the Oireachatas, January 2013) at 95.

[130] "Man guilty of 'malicious and evil' bullying of boy through text messages" *Irish Independent* 22 January 2013 available at http://www.independent.ie/irish-news/courts/man-guilty-of-malicious-and-evil-bullying-of-boy-through-text-messages-28947459.html.

imprisonment which was suspended for 12 months provided he had no contact with the victim and continued to receive psychiatric treatment and counselling. He was also fined €600.[131]

- In a 2014 case, a man pleaded guilty under section 10 after posting explicit items on a website about the victim.[132] He was given a four year sentence which was suspended for four years.
- In 2012, a man who installed a hidden camera in a women's locker room pleaded guilty to harassment of eight women who were staff at the hospital where the locker room was located. The court imposed a four year suspended sentence.

Q4: Do you consider that the current penalties under the offences which can apply to cyber-harassment and related behaviour are appropriate?

Please type your comments (if any)

[131] "Westport man given suspended sentence for harassing teenage boy" *The Mayo News* 26 February 2013 available at http://www.mayonews.ie/index.php?option=com_content&view=article&id=17206:westport-man-given-suspended-sentence-for-harassing-teenage-boy&catid=23:news&Itemid=46

[132] "Man avoids jail for vile internet messages about ex-girlfriend" *Irish Times* 20 March 2014 available at http://www.irishtimes.com/news/crime-and-law/courts/man-avoids-jail-for-vile-internet-messages-about-ex-girlfriend-1.1731368.

ISSUE 5: WHETHER CURRENT CIVIL LAW REMEDIES ARE ADEQUATE

5.01 The fifth question is whether existing civil law remedies and procedures are adequate to address cyber-harassment. The civil law may be more suitable for less serious cyber-harassment cases where civil remedies including damages or injunctions would be adequate. The current law provides for some civil remedies but these may not be either readily accessible or effective.

Non-Fatal Offences Against the Person Act 1997

5.02 Section 10(3) of the 1997 Act provides:

> "Where a person is guilty of an offence under subsection (1), the court may, in addition to or as an alternative to any other penalty, order that the person shall not, for such period as the court may specify, communicate by any means with the other person or that the person shall not approach within such distance as the court shall specify of the place of residence or employment of the other person."

5.03 The Court is thus empowered to make a restraining order, restricting a person from communicating and/or approaching the victim, where the person has been convicted of harassment. In addition, section 10(5) of the 1997 Act empowers a court to make such a restraining order even where the person has been acquitted of harassment:

> "If on the evidence the court is not satisfied that the person should be convicted of an offence under subsection (1), the court may nevertheless make an order under subsection (3) upon an application to it in that behalf if, having regard to the evidence, the court is satisfied that it is in the interests of justice so to do."

5.04 A restraining order under section 10(3) cannot be made unless criminal proceedings have been taken against the alleged perpetrator of the harassment, and this has given rise to difficulties.

In *Ó Raithbheartaigh v McNamara*[133] the applicant had been charged in the District Court with harassment under the 1997 Act, the particulars alleging that the applicant had put up posters of a defamatory or inflammatory nature about the complainant. The complainant gave evidence of the effect of the posters on her. The applicant did not go into evidence and argued that the case should be dismissed on the ground that the only evidence adduced against him were admissions made by him in custody after his arrest under the Public Order Acts, which he argued were inadmissible. The respondent judge of the District Court agreed and the applicant was acquitted. The prosecution then applied for a restraining order under section 10(5) of the 1997 Act, which the respondent granted on the basis of the "very sincere and impressive testimony" of the complainant and that it was in the "interests of justice," as provided for in section 10(5), to do so. On judicial review, the High Court quashed the order on the ground that the respondent had acted in breach of the applicant's right to fair procedures, in particular because the applicant had not been given an opportunity to adduce evidence, whether from the applicant himself or by cross-examination of the complainant, as to whether it was appropriate to make such an order.

5.05 The Court in the *Ó Raithbheartaigh* case acknowledged that a restraining order under section 10, as a form of "preventative justice," was an important element in the administration of justice, but that it was equally important to ensure that fair procedures were observed where the accused has been acquitted on the criminal charge, especially having regard to the "unusual" and "extraordinary"

[133] [2014] IEHC 406.

powers conferred by section 10.[134] The decision in this case illustrates a difficulty in providing for a civil-law type remedy in the context of a criminal trial, especially where the accused has been acquitted.

Defamation Act 2009

5.06 Section 6(2) of the *Defamation Act 2009* provides:

> "The tort of defamation consists of the publication, by any means, of a defamatory statement concerning a person to one or more than one person (other than the first-mentioned person), and "defamation" shall be construed accordingly".

5.07 As the 2009 Act provides that a defamatory statement can be published by any means, it applies to publication through the cyber medium. In cases of online defamation, plaintiffs generally prioritise the removal of the content over an award of damages because the speed and ease with which content can spread online increases the urgency to have it removed. Injunctions are therefore an important remedy in this context, yet ensuring their efficacy can be challenging.

In *Tansey v Gill*,[135] the plaintiff, a solicitor, had been defamed on the website "www.rate-your-solicitor.com". The plaintiff was granted interlocutory injunctions restraining the publication of any further material, ordering the removal of the defamatory material and ordering the termination of the website upon which the material was posted. A *Norwich Pharmacal* order[136] was also granted.

5.08 In *Tansey*, Peart J stated that damages are an empty remedy in the context of online defamation as the harm caused can be so serious and irreversible. This is because the "inexpensive, easy and instantaneous" nature of internet publication allows individuals to make very serious allegations with "relative impunity and anonymously" "whereby reputations can be instantly and permanently damaged and where serious distress and damage"[137] can be caused. Peart J thus suggested that interlocutory injunctions should be granted more readily in cases of online defamation. However, injunctions are frequently ineffective in the context of internet communications as *McKeogh v Doe* illustrates:

In *McKeogh v Doe*[138] the plaintiff was defamed by an anonymous YouTube user who wrongly identified him as a person who ran from a taxi without paying. In addition, The plaintiff received "vitriolic messages" on Facebook calling him, amongst other things, a "scumbag" and a "thief."[139] This abuse continued even after the plaintiff obtained interim injunctions to prohibit such messages. The falsity of this claim was not at issue because the plaintiff could show that at the time of the incident he was in Japan. The High Court accepted that the incorrect identification amounted to defamation.

[134] *Ibid* at paragraph 42.

[135] *Tansey v Gill* [2012] IEHC 42.

[136] *Norwich Pharmacal* orders are discussed at paragraph 5.14 below.

[137] *Tansey v Gill* [2012] IEHC 42 at paragraph 25.

[138] *McKeogh v Doe* [2012] IEHC 95.

[139] "Crucified by vigilantes of the internet: MoS proves that innocent young man was falsely branded a thief on the world's biggest websites" *Daily Mail* 22 January 2012 available at http://www.dailymail.co.uk/news/article-2090070/Eoin-McKeogh-falsely-branded-thief-worlds-biggest-websites.html.

However, the interim orders granted were not effective, because newspapers continued to name the plaintiff in reports about the video and in some cases did not report the plaintiff's statements that he could not have been the taxi fare evader.

5.09 *McKeogh* also underlines the potentially great cost of civil proceedings, with the plaintiff reportedly facing a legal bill of over €1,000,000.[140]

5.10 Another difficulty with injunctions in the context of internet communications is that often the material ordered to be removed can spread beyond the control of the individual ordered to remove the content.

In *Kelly v National University of Ireland*[141] the plaintiff was ordered to remove content from the internet which had as its object or effect the scandalising or undermining of the reputation or authority of the court. At a subsequent hearing, the defendant claimed that this order had been breached as the plaintiff had redirected visitors to his site to other websites where the material could be found. The High Court granted a second order requiring the removal from any website, whether controlled by the plaintiff or otherwise, of references to the information specified in the previous order, but the plaintiff said that he would be unable to remove anything from websites which he did not control. The Court held that if the plaintiff had no knowledge, either actual, constructive or implied, he would not breach the order. However, were he to pass on the material to another who then published it or were he to redirect visitors to his website to other websites publishing the material, then he would be in breach.

Data Protection Acts 1988 and 2003

5.11 Individuals have the right under the *Data Protection Acts 1988 and 2003* to request the rectification and removal of personal data, which includes videos and images, from data controllers.[142] Where this request is not complied with, individuals can refer a complaint to the Office of the Data Protection Commissioner. The Acts also provide a separate means to obtain compensation against data controllers or processors for breach of a duty of care,[143] but this remedy is very difficult to obtain as actual injury or damage must be proven before compensation is awarded.[144]

---

[140] "Student in YouTube taxi row facing €1m legal costs" *Irish Independent* 22 July 2014 available at http://www.independent.ie/irish-news/courts/student-in-youtube-taxi-row-facing-1m-legal-costs-30448556.html. See also the English case involving Daniel Hegglin against Google. Hegglin is seeking the automatic blocking of defamatory and abusive posts from Google. He tried to cap the costs for the trial as Google had already run up costs of £1.25 million and were estimating further costs of £400,000, figures Mr Hegglin's counsel described as "extraordinary" and grotesque". The High Court reserved its decision on the issue. See "Google has £1.6m war chest to fight 'troll post' test case" *The Times* 7 November 2014.

[141] *Kelly v National University of Ireland* [2010] IEHC 48.

[142] The *Data Protection Acts* are discussed more extensively at paragraphs 2.12-2.15 above.

[143] Section 7 of the *Data Protection Acts 1988.*

[144] See *Michael Collins v FBD Insurance PLC* [2013] IEHC 137.

Civil remedy for breach of a constitutional right

5.12 A number of recent cases have highlighted the remedies available to plaintiffs based on breach of a constitutional right by another person.[145] Such a cause of action could be particularly beneficial in the cyber-harassment context if based on the constitutional right to privacy. A cause of action based on the breach of the right to privacy by an individual was successfully taken in *Herrity v Associated Newspapers (Ireland) Ltd*[146]:

In *Herrity v Associated Newspapers (Ireland) Ltd,* the plaintiff claimed her constitutional right to privacy was breached by the defendant who had published details of her extra-marital affair with a priest. These details had been supplied to the defendant by the plaintiff's husband who had tapped her telephone illegally in breach of section 98 of the *Postal and Telecommunications Services Act 1983*. The High Court held that the constitutional right to privacy could be derived from the nature of the underlying information communicated, or as a result of the method by which the information was obtained. The Court held that the plaintiff's right to privacy prevailed over the defendant's right to freedom of expression, especially because the material had been obtained unlawfully and there was no demonstrable public interest in publishing it.

5.13 The approach in *Herrity* could therefore apply to a situation where content is disseminated online by a private individual in breach of another individual's privacy provided the material was obtained unlawfully and there was no public interest element involved. An example of this might be the case mentioned above of the humiliating video of a teenage girl making drunken remarks, as the video was uploaded without her consent and no public interest element was involved.

Norwich Pharmacal Orders

5.14 *Norwich Pharmacal* orders[147] allow for the disclosure of personal information, particularly the IP address in the cyber context, of parties unknown to the plaintiff against whom a plaintiff seeks to assert a legal right to redress.

In the UK case concerning Nicola Brookes, the plaintiff was subjected to online abuse following her defence on her Facebook page of an X-Factor contestant. Among the actions carried out against Brookes was the setting up of a profile on Facebook using her name which was used to send explicit messages to children and contained personal information, including her email address and photographs of her daughter.[148] Brookes successfully applied for a *Norwich Pharmacal* Order compelling Facebook to reveal the identities of seven users who had abused her.[149]

5.15 Clear wrongdoing has to be established before such an order will be granted. The jurisdiction to grant a *Norwich Pharmacal* order is discretionary and necessitates that the requirements of justice and privacy be balanced. In *EMI Records v Eircom plc*[150] the court noted that the party against whom a *Norwich Pharmacal* order is sought to be enforced will often through statute, contract or common law owe the third party a duty of confidentiality and/or privacy. Thus, the requirement for

---

[145] *Sullivan v Boylan (No. 2)* [2013] IEHC 104; *Herrity v Associated Newspapers (Ireland) Ltd* [2009] 1 IR 316.

[146] *Herrity v Associated Newspapers (Ireland) Ltd* [2009] 1 IR 316.

[147] *Norwich Pharmacal Co. v Commissioners of Customs and Excise* [1974] AC 133

[148] "Police officer arrested over Nicola Brookes Facebook abuse" BBC News 29 August 2012 available at http://www.bbc.co.uk/news/uk-england-19414045

[149] See Khan, "Can the trolls be put back under the bridge?" (2013) CTLR 9, at 11.

[150] *EMI Records v Eircom and BT Communications* [2005] 4 IR 148 at paragraph 10.

clear wrongdoing and the potential for the procedure to interfere significantly with the right to privacy mean that such orders are rarely granted. *Norwich Pharmacal* orders are not provided for in court rules and the jurisdiction to grant them forms part of the inherent jurisdiction of the High Court flowing from the Constitution. Neither the Circuit nor District Court has this jurisdiction being courts of local and limited jurisdiction.[151] This means that the cost of obtaining such an order is high and the remedy is not available to many individuals.

Proposed reforms to discovery to facilitate tracing persons involved in cyber-harassment

5.16 The 2014 *Report of the Internet Content Governance Advisory Group* has described existing civil procedures for tracing persons involved in cyber-harassment as "expensive, lacking detail and out of date".[152] The Report recommended that the *Rules of the Superior Courts 1986* be amended to provide specifically for the jurisdiction to grant *Norwich Pharmacal* orders. The Report also recommended extending the availability of such orders to litigants in the lower courts "in order to save on delay, expense and effort".[153]

5.17 Thus, the Report recommended the introduction of three new rules to facilitate the tracing of publishers and perpetrators:

> 1. A pre-action procedure allowing a person to seek access to material, including to identify the perpetrator of cyber-harassment, before issuing proceedings (*Norwich Pharmacal* order) ;
>
> 2. Reform of the existing rule on discovery after proceedings have been issued against a person not a party to the proceedings;[154]
>
> 3. A rule on discovery after proceedings have been issued against a person not a party to the proceedings and where that person is not yet known.

New Zealand proposals on civil remedies

5.18 The potential cost, complexity and length of civil proceedings may deter victims of cyber-harassment from taking them and available processes and remedies may not be effective. A key matter is the extent to which a victim of harassment, such as the plaintiff in *McKeogh v Doe*,[155] may obtain a "take-down" order in a speedy and inexpensive manner. This has also been provided for in other jurisdictions. For example, in 2012 the New Zealand Law Commission recommended reform of its laws on civil remedies to deal with cyber-harassment and other harmful online material, including the need to establish an independent body with a remit to resolve cyber-harassment complaints

---

[151] Abrahamson, Dwyer and Fitzpatrick *Discovery and Disclosure* 2nd ed (Round Hall, 2013) at 207.

[152] *Report of the Internet Content Governance Advisory Group* (Department of Communications, Energy and Natural Resources, 2014) at 45.

[153] *Report of the Internet Content Governance Advisory Group* (Department of Communications, Energy and Natural Resources, 2014) at 46.

[154] This rule would seek to modernise and enhance Order 31, Rule 29 of the *Rules of the Superior Courts 1986*.

[155] *McKeogh v Doe* [2012] IEHC 95, discussed at paragraph 5.08 above.

quickly through a mediation-type process.[156] Such a body might perform the enhanced role of the Office of Internet Safety envisaged in the 2014 *Report of the Internet Content Governance Advisory Group.*[157]

5.19 In response to the New Zealand Law Commission's recommendation the *Harmful Digital Communications Bill* was introduced in the New Zealand Parliament in 2013.[158]

5.20 The 2013 Bill provides that cyber-harassment complaints be made initially to a specialist body to investigate and attempt to resolve them by negotiation, mediation or persuasion.[159] If this fails, the Bill provides that an individual may apply to the District Court for a number of civil orders including: a "take- down" order, an order requiring the defendant to cease the harmful conduct and/or an order to identify the author of any anonymous communication.[160] These orders might be made against individuals or online content hosts.[161] The Bill also provides that the court may make a declaration that a communication breaches a "communication principle",[162] which would be intended primarily to have a persuasive effect on website hosts or internet service providers operating outside New Zealand.[163]

5.21 The introduction of this type of a civil enforcement regime would have the advantage of offering victims of cyber-harassment a potentially quick and cost effective means of obtaining civil remedies. The prospect of informal resolution by an independent body would also reduce delays and provide victims with valuable support and advice. However, mediation and similar methods will only be effective where the wrongdoer is identifiable and cooperative. Therefore, situations involving experienced hackers or individuals with no respect for the law, such as those responsible for the mass leak of intimate pictures of female celebrities, are unlikely to be resolved through such mechanisms. The Commission also notes that the New Zealand Bill has not yet been enacted and that some elements of it have been criticised for insufficiently safeguarding freedom of expression.

---

[156] New Zealand Law Commission, Ministerial Briefing Paper *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (2012).

[157] *Report of the Internet Content Governance Advisory Group* (Department of Communications, Energy and Natural Resources, 2014) at 32.

[158] In May 2014, the New Zealand Parliament's Justice and Electoral Committee recommended that the Bill be passed with amendments: Justice and Electoral Committee *Report on the Harmful Digital Communications Bill* (May 2014). The text of the Bill referred to in this paper is the amended text recommended by the Committee.

[159] Sections 7 and 8 of the NZ *Harmful Digital Communications Bill 2013.*

[160] Sections 10 and 17 of the NZ *Harmful Digital Communications Bill 2013.*

[161] Section 17(1) (defendants) and section 17(2) (online content hosts) of the NZ *Harmful Digital Communications Bill 2013.*

[162] Section 6 of the NZ *Harmful Digital Communications Bill, 2013* sets out ten communication principles, stating that a digital communication should not "disclose sensitive personal facts about another individual" (principle 1) "be threatening intimidating or menacing" (principle 2), "be grossly offensive to a person in the position of the affected individual" (principle 3), "be indecent or obscene" (principle 4), "be used to harass an individual" (principle 5), "make a false allegation" (principle 6), "contain a matter that is published in breach of confidence" (principle 7), "incite or encourage anyone to send a message to an individual for the purposes of causing harm to the individual" (principle 8) "incite or encourage another individual to commit suicide" (principle 9) and "denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation or disability" (principle 10).

[163] Section 17(3)(b) of the *Harmful Digital Communications Bill 2013.*

Jurisdictional issues and civil remedies related to online material

5.22 Concerns have also been raised as to whether the remedies proposed in the New Zealand Bill would be effective, particularly where the harm relates to overseas websites because any orders made could prove difficult to enforce.[164] Such jurisdictional questions have also arisen in the State, notably in connection with online defamation cases involving foreign defendants.[165] While it may be possible for a plaintiff to secure a judgment in the Irish courts it may prove difficult to enforce. The Brussels 1 Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters,[166] provides that in general persons shall be sued in the State in which they are domiciled.[167] For tort actions, however, a person may be sued "in the courts for the place where the harmful event occurred."[168] In *Shevill v Presse Alliance SA*[169] the EU Court of Justice held that this allows a plaintiff to bring civil proceedings either in the courts where the publication is based for the entirety of the damage or in the courts of each Member State in which the publication was distributed, but only in respect of any damage done to the plaintiff's reputation within each particular Member State. However, a more recent EU Court of Justice decision, *eDate Advertising GmbH v X; Olivier Martinez v MGN Ltd*,[170] adapted this rule in the context of online defamation, allowing a person who has been defamed online to bring civil proceedings in respect of all the damage caused in the EU in the place where the person has his or her "centre of interests," which will usually be his or her place of habitual residence. In *Martinez* the Court also held that publication takes place in the internet context where the content has been placed online or otherwise made accessible in the country of receipt.[171]

5.23 In cases involving online defamation by individuals located outside the EU, the Irish courts generally have jurisdiction "if any significant element occurred within this jurisdiction".[172] However, the real issue with regard to cases involving defendants outside of the EU is securing recognition and enforcement of the judgment. This may be a particular problem in cases involving US defendants as

---

[164] "HDC Bill reported back by Select Committee" *Tech Liberty NZ* 27 May 2014 available at http://techliberty.org.nz/hdc-bill-reported-back-by-the-select-committee/.

[165] See also the discussion at paragraphs 1.23 - 1.25 above, of the similar considerations that arise in connection with jurisdiction and extra-territorial effect in the context of the criminal offence of harassment in section 10 of the *Non-Fatal Offences against the Person Act 1997*.

[166] *Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters* OJ L 12, 16.1.2001. Jurisdiction in relation to EU states was originally governed by the Brussels Convention which was implemented in Ireland in the *Jurisdiction of Courts and Enforcement of Judgments Act 1998*. The 2001 Regulation substantially replaces this Convention. A recast Brussels 1 Regulation was adopted in 2012 which will replace the 2001 regulation in 2015: *Regulation (EU) No 1215/2012 of the European Parliament and the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)*.

[167] Article 2 of Brussels 1 Regulation. Article 60(1) provides that for the purposes of the Regulation, a company or other legal person or association of natural or legal persons is domiciled at the place where it has its statutory seat (which means the registered office or place of incorporation or the place under the law of which the formation took place) or central administration or principal place of business.

[168] Article 5(3) of the Brussels 1 Regulation.

[169] *Shevill v Presse Alliance SA* [1995] ECR I-415.

[170] Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH v X; Olivier Martinez v MGN Ltd* (25 October 2011).

[171] This means that if the material is placed on a foreign based subscription only website it has to be proved that it was accessed within the jurisdiction. See *CSI Manufacturing Ltd v Dun and Bradstreet Ltd* [2013] IEHC 547 and *Coleman v MGN Ltd* [2012] IESC 20.

[172] *Grehan v Medical Inc* [1986] ILRM 629.

the US courts may not enforce court orders that are in conflict with the guarantee of free speech in the First Amendment of the US Constitution.[173]

5(a): Do you consider that in addition to section 10(5) of the 1997 Act there should be a separate statutory procedure, to provide for civil remedies for cyber-harassment and serious interferences with an individual's privacy, without the need to institute a criminal prosecution?

5(b): Do you consider that any further reform of civil proceedings, over and above those in the 2014 *Report of the Internet Content Governance Advisory Group*, are required?

5(c): Do you consider that complaints of cyber-harassment and other harmful cyber activity affecting personal safety, privacy and reputation should, without prejudice to any criminal proceedings, be considered by a specialist body that would offer non-court, fast yet enforceable remedies?

5(d): Do you consider that further reforms are required to make effective any orders in civil proceedings that would have extra-territorial effect, including in their application to websites located outside the State; and if so do you have any comments on the precise form they should take?

Please type your comments (if any)

[173] See *Yahoo! Inc v LICRA* 169 F Supp 2d. 1181 (N.D. Cal 2001) at 1185-6. The American website Yahoo! Inc hosted an auction site offering Nazi paraphernalia for sale and a link to this site was offered on the French Yahoo! site. Yahoo! Inc was ordered by a French court to take all necessary measures to make access to the site impossible but it refused, claiming that the French court lacked jurisdiction and that the order could have no application in the US because of the First Amendment. Yahoo! Inc did not comply with the ruling but instead took a case in the US where the French decision was found to be inapplicable within the US as it was inconsistent with the First Amendment. The United States District Court held that in the absence of international standards on internet hate speech, the principle of comity was outweighed by the Court's obligation to uphold the First Amendment, stating that "it is preferable to permit the non-violent expression of offensive viewpoints rather than to impose viewpoint-based governmental regulation upon speech". However, LICRA successfully appealed this ruling on the basis that there was no longer any dispute between the parties as Yahoo! had changed its policy so that it largely complied with the French orders: *Yahoo! Inc v LICRA* 433 F.3d. 1199 (9TH Ci. 2006).

Please fill in your name and contact details below. Click submit button to email your submission. If submitting by webmail please check your drafts folder and sent items to ensure that your email has been submitted

First name *

Surname *

Telephone/mobile number

Email address*

Organisation

* Denotes required field

Click to submit