

Report

Harmful Communications and Digital Safety

(LRC 116-2016)

© Law Reform Commission 2016

35-39 Shelbourne Road, Dublin 4, Ireland D04 A4E0

T. +353 1 637 7600

F. +353 1 637 7601

info@lawreform.ie

lawreform.ie

ISSN 1393-3132

Law Reform Commission's Role

The Law Reform Commission is an independent statutory body established by the Law Reform Commission Act 1975. The Commission's principal role is to keep the law under review and to make proposals for reform, in particular by recommending the enactment of legislation to clarify and modernise the law. Since it was established, the Commission has published over 200 documents (Working Papers, Consultation Papers, Issues Papers and Reports) containing proposals for law reform and these are all available at www.lawreform.ie. Most of these proposals have contributed in a significant way to the development and enactment of reforming legislation.

The Commission's role is carried out primarily under a Programme of Law Reform. Its Fourth Programme of Law Reform was prepared by the Commission following broad consultation and discussion. In accordance with the 1975 Act, it was approved by the Government in October 2013 and placed before both Houses of the Oireachtas. The Commission also works on specific matters referred to it by the Attorney General under the 1975 Act.

The Commission's Access to Legislation project makes legislation in its current state (as amended rather than as enacted) more easily accessible to the public in three main outputs: the Legislation Directory, the Classified List and the Revised Acts. The Legislation Directory comprises electronically searchable indexes of amendments to primary and secondary legislation and important related information. The Classified List is a separate list of all Acts of the Oireachtas and Statutory Instruments that remain in force organised under 36 major subject-matter headings. Revised Acts bring together all amendments and changes to an Act in a single text. The Commission provides online access to over 100 Revised Acts enacted before 2006, and for all Acts enacted from 2006 onwards (other than Finance and Social Welfare Acts) that have been textually amended.

Membership

President:

Mr Justice John Quirke, former judge of the High Court

Full-time Commissioner:

Raymond Byrne, Barrister-at-Law

Part-time Commissioner:

Donncha O'Connell, Professor of Law

Part-time Commissioner:

Thomas O'Malley, Barrister-at-Law

Part-time Commissioner:

Ms Justice Carmel Stewart, Judge of the High Court

Staff

Law Reform Research

Director of Research:

[Vacant at Present]

Legal Researchers:

Hanna Byrne BCL(Intl) (NUI) MSc(Universiteit Leiden)

Hugh Dromey BCL, LLM(NUI)

Niall Fahy BCL, LLM(LSE). Barrister-at-Law

Owen Garvey BA, LLB (NUI), Barrister-at-Law

Sarah Keating BCL, LLM

Finn Keyes LLB(Dub), LLM(UCL)

Meghan McSweeney BCL with Hist, LLM (Georgetown), Attorney-at-Law (NY)

Jack Nea LLB, LLM (NUI), Barrister-at-Law

Fiona O'Regan BCL, LLM, PhD (NUI)

Access to Legislation

Manager:

Alma Clissmann, BA (Mod), LLB, Dip Eur Law (Bruges), Solicitor

Deputy Manager:

Kate Doran BCL, Barrister-at-Law, LLM (NUIG), PhD (UL)

Administration

Head of Administration:

Deirdre Fleming

Executive Officers:

John Harding

Pearl Martin

Brendan Meskill

Clerical Officer:

Brid Rogers

Library and Information Manager:

Órla Gillen, BA, MLIS

Principal Legal Researcher for this Report

Fiona O'Regan BCL, LLM, PhD (NUI)

Acknowledgements

The Commission would like to thank the following people and organisations who provided valuable assistance:

Mary Aiken, RCSI Cyber-Psychology Research Centre
All Rise- Say No to Cyber Abuse
Emma Ascroft, Director of Public Policy, Yahoo!
Bar Council of Ireland
Barnardos
Fiona Barry, Solicitor, Arthur Cox
Richard Browne, Department of Communications, Climate Action and Environment
Seamus Carroll, Department of Justice and Equality
Rebecca Coen, Office of the Director of Public Prosecutions
Caroline Counihan, Rape Crisis Network Ireland
Sean Corrigan, STOP (Stop Tolerating Oppressive People)
Fergal Crehan, BL, Digital Rights Ireland
Paul Durrant, Internet Service Providers Association of Ireland
Caroline Fanning, Solicitor, Caroline Fanning Solicitors
Sonia Flynn, Former Head of Public Policy, Facebook Ireland
Faye Govan, Data Protection and Privacy Counsel, Facebook Ireland
Detective Sgt. Michael Gubbins, An Garda Síochána
Brian Hallissey, BL
Robert Hanniver, Interim Data Protection Supervisor, Ask.fm
Mairead Healy, Future Voices Ireland
Irish Society for Prevention of Cruelty to Children
Detective Sgt. Paul Johnstone, An Garda Síochána
Aibhinn Kelleher, Facebook
Dr. Gráinne Kirwan
Paul Lambert, Solicitor, Merrion Legal Solicitors
Councillor James Lawless
Carol Lynch, University of Limerick
Angela Long
Ronan Lupton, BL
Roderick Maguire, BL
Chief Superintendent Alf Martin, An Garda Síochána
Dr. Ciarán McMahon, RCSI CyberPsychology Research Centre
Simon McGarr, Digital Rights Ireland
Michael McDowell, SC
Prof. Clare McGlynn, Durham University

Dr. TJ McIntyre, University College Dublin, Digital Rights Ireland
Michael McLoughlin, Youth Work Ireland
Sinéad McSweeney, Senior Director of Public Policy for Europe, the Middle East and Africa, Twitter
Detective Sgt. Jennifer Molony, An Garda Síochána
Gráinne Morrissey, Department of Education and Skills
Dr. Stephen Minton, School of Education, Trinity College Dublin
Dr. Niall Muldoon, Ombudsman for Children
Dualta Ó Broin, Department of Communications, Climate Action and Environment
Éanna Ó Conghaile, Department of Communications, Climate Action and Environment
Cormac Ó Culáin, Solicitor, Public Affairs Executive, Law Society of Ireland
Anne O'Donnell, Department of Children and Youth Affairs
Prof. Brian O'Neill, Dean of the Graduate Research School, Dublin Institute of Technology
Garrett O'Neill, Office of the Data Protection Commissioner
Ian Power, Spunout.ie
Sandra Roe, Research Consultant, *Report of consultations with young people* (Appendix B to this Report)
Jennifer Schweppe, Hate and Hostility Research Group, University of Limerick
Ciaran Shanley, Department of Communications, Climate Action and Environment
Dr. Geoffrey Shannon, Solicitor, Special Rapporteur on Child Protection
Detective Sgt. Michael Smyth, An Garda Síochána
Angela Steen, Former Head of Public Policy, Google Ireland
Niamh Sweeney, Head of Public Policy, Facebook Ireland
Oisín Tobin, Solicitor, Mason Hayes and Curran, Facebook External Counsel
Mr Justice Michael Tugendhat, former Judge of the High Court of England and Wales
Women's Aid
Pauline Walley, SC
Róisín Webb, Head of Policy, Office of the Ombudsman for Children
Karen White, Senior Manager, European Public Policy, Twitter
Richard Willis, Solicitor, Arthur Cox

The Commission would also like to thank all of the young people who participated in the consultations concerning harmful internet communications held in April 2016 and the members of the Department of Children and Youth Affairs and Comhairle na nÓg who facilitated these consultations.

Table of Contents

OVERVIEW AND EXECUTIVE SUMMARY	1
A Background	1
B Guiding Principles in the Report	3
C Reform of Criminal Law Concerning Harmful Communications	5
D Digital Safety Oversight, Take Down Procedure and Civil Law	9
CHAPTER 1 Guiding Principles	15
A The Digital and Online World	15
B 2014 Report of the Internet Content Governance Advisory Group	17
C Principles of Reform	19
(1) Balancing the Right to Privacy and the Right to Freedom of Expression in the internet context	19
(2) Freedom of Expression and Privacy	29
(3) Proportionality and the Harm Principle	39
(4) “Harmful communications” and “cyberbullying”	42
(5) Technology Neutrality	43
CHAPTER 2 Reform of Criminal Law concerning Harmful Communications	47
A Introduction	47
B Reform of the offence of harassment	48
(1) Examples of harmful digital communications	51
(2) Application of section 10 of the 1997 Act to harassment by digital or online means	51
(3) Whether there should be a specific reference to harassment by digital or online means	53
(4) Indirect harassment	56
C Specific Stalking Offence	61
(1) Scotland	63
(2) England and Wales	65
(3) Northern Ireland	67
(4) Does Ireland need a specific stalking offence?	67
D Offences Designed to Target Once-off Harmful Digital Communications	68
(1) Other relevant criminal offences	69

(2)	How once-off harmful digital communications are dealt with in other jurisdictions	79
(3)	Vagueness	90
(4)	Specific offences to target once-off harmful digital communications	95
E	Procedural Issues and Harmful Digital Communications	105
(1)	Protection for privacy of person to whom offence relates	105
(2)	Consent of Director of Public Prosecutions in prosecution of person under 17	106
(3)	Time limits for summary prosecutions	107
F	Jurisdictional Issues and Harmful Communications: Extra-territorial Effect	108
G	Penalties on conviction for offences	111
H	Hate Crime and Harmful Digital Communications	115
	CHAPTER 3 Digital Safety, Takedown Procedure and Civil Law	121
A	Introduction	121
B	Non-statutory Arrangements on Social Media Sites	121
(1)	Content and conduct policies of social media companies	123
(2)	Reporting Harmful Content and Takedown in practice	125
C	Reform of Civil Remedies for Harmful Digital Communications	126
(1)	Existing civil remedies	126
(2)	Alternative civil enforcement mechanisms	134
(3)	Consultation responses	139
(4)	Office of the Digital Safety Commissioner	141
D	Civil Restraint Orders	146
E	Norwich Pharmacal Orders	148
F	Jurisdictional Issues and Civil Remedies Related to Harmful Digital Communications	151
	CHAPTER 4 Summary of Recommendations	155
A	Chapter 2: Reform of Criminal Law Concerning Harmful Communications	155
B	Chapter 3: Digital Safety, Takedown Procedure and Civil Law	157
	Appendix A	
	Draft Harmful Communications and Digital Safety Bill	162
	Appendix B	
	Report of Consultations With Young People	188

TABLE OF LEGISLATION

Abusive Behaviour and Sexual Harm (Scotland) Act 2016	2016 asp 22	Scot
Animal Remedies Act 1993	No. 23 of 1993	Irl
Canadian Criminal Code	RSC 1985, c. C-46	Can
Central Bank (Supervision and Enforcement) Act 2013	No. 26 of 2013	Irl
Child Trafficking and Pornography Act 1998	No. 22 of 1998	Irl
Communications Act 2003	2003, c. 21	UK
Communications Regulation (Amendment) Act 2007	No. 22 of 2007	Irl
Companies Act 2014	No. 38 of 2014	Irl
Competition and Consumer Protection Act 2014	No. 29 of 2014	Irl
Consumer Protection Act 2007	No. 19 of 2007	Irl
Criminal Damage Act 1991	No. 31 of 1991	Irl
Criminal Justice (Public Order) Act 1994	No. 2 of 1994	Irl
Criminal Justice Act 2006	No. 26 of 2006	Irl
Criminal Justice and Courts Act 2015	2015, c.2	UK
Criminal Justice and Licensing (Scotland) Act 2010	2010, asp 13	Scot
Criminal Law (Amendment) Act 1935	No. 6 of 1935	Irl
Data Protection Act 1988	No. 25 of 1988	Irl
Data Protection (Amendment) Act 2003	No. 6 of 2003	Irl
Defamation Act 2009	No. 31 of 2009	Irl
Domestic Violence Act 1996	No. 1 of 1996	Irl
Employment Permits Act 2006	No. 16 of 2006	Irl
Enhancing Online Safety for Children Act 2015	No. 24 of 2015	Aus
European Convention on Human Rights Act 2003	No. 20 of 2003	Irl
Harmful Digital Communications Act 2015	No. 63 of 2015	NZ
Immigration Act 2004	No. 1 of 2004	Irl
Information Technology Act 2000	No. 21 of 2000	Ind
New Zealand Bill of Rights Act 1990	No. 109 of 1990	NZ

Offences Against the Person Act 1861	1861, 55 & 56 Vict. c.10	Irl
Petty Sessions (Ireland) Act 1851	1851, 14 & 15 Vict, c.93	Irl
Postal and Telecommunications Services Act 1983	No. 24 of 1983	Irl
Prohibition of Incitement to Hatred Act 1989	No. 19 of 1989	Irl
Protecting Canadians from Online Crime Act 2014	2014, c.31	Can
Protection from Harassment Act 1997	1997, c.40	UK
Protection of Freedoms Act 2012	2012, c.9	UK
Public Order Act 1986	1986, c. 64	UK
Rules of the Superior Courts 1986	S.I. No. 15 of 1986	Irl
Sexual Offences (Jurisdiction) Act 1996	No. 38 of 1996	Irl
Summary Offences Act 1966	No. 7405 of 1966	Aus
Summary Offences Amendment (Upskirting) Act 2007	No. 49 of 2007	Aus
Vagrancy Act 1824	36 & 37 Vict, c.91	Irl

TABLE OF CASES

Attorney General v Paperlink Ltd.	[1984] ILRM 373	Irl
Chambers v DPP	[2012] EWHC 2157	Eng
Cox v DPP	[2015] IEHC 642	Irl
Delfi v Estonia	App. no. 64659/09 (16 June 2015)	ECHR
Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Ors	Joined Cases C-293/12 to C-594/12; 8 April 2014	EU
Director of Public Prosecutions (O'Dowd) v Lynch	[2008] IEHC 183, [2010] 3 IR 434	Irl
Dokie v DPP	[2011] 1 IR 805	Irl
Douglas v DPP	[2013] IEHC 343	Irl
DPP v Collins	(2006) 1 WLR 2223	Eng
EMI Records Ltd. v Eircom plc	[2005] 4 IR 148	Irl
Google France v Louis Vuitton	Joined Cases C-236/08 to C-238/08; 23 March 2010	EU
Google Inc. v Vidal Hall and others	[2015] EWCA Civ 311	UK
Google Spain SL and Google Inc v Agencia Espanola de Protection de Datos	Case C-131/12, 13 May 2014	EU
Handyside v United Kingdom	(1979-1980) 1 EHRR 737	ECHR
Harris v HM Advocate	[2009] HCJAC 80	Scot
Herrity v Associated Newspapers (Ireland) Ltd	[2009] 1 IR 316	Irl
Irish Times Ltd. v Ireland	[1998] 4 IR 343	Irl
Kelly v National University of Ireland	[2010] IEHC 48	Irl
Kennedy v Ireland	[1987] IR 587	Irl
King v Attorney General	[1981] IR 233	Irl
Lindqvist, Bodil, Criminal Proceedings against	(C-101/01) [2004] ECR I 12971	EU
L'Oreal SA v eBay International AG and	Case C-324/09 [2011] OJ C269	EU

Others

Magyar Tartalomszolgáltatók Egyesülete (MTE) and Index.hu Zrt (Index) v Hungary	app. no. 22947/13 (2 February 2016)	ECHR
Mahon v Keena	[2007] IEHC 348	Irl
Mahon v Post Publications Ltd.	[2007] 2 ILRM 1	Irl
McGee v Attorney General	[1974] IR 284	Irl
McInerney v DPP	[2014] IEHC 181	Irl
McKeogh v Doe	[2012] IEHC 95	Irl
McNamee v DPP	[2016] IEHC 286	Irl
Megaleasing UK Ltd v Barrett (No. 2)	[1993] ILRM 497	Irl
Norris v Attorney General	[1984] IR 36	Irl
Ó Raithbheartaigh v McNamara	[2014] IEHC 406	Irl
O'Brien v Red Flag Consulting Ltd & ors	[2015] IEHC 867	Irl
R v Debnath	[2005] EWCA Crim 3472	Eng
R v DeSilva	2011 ONCJ 133	Can
R v Stacey	Crown Court, 30 March 2012	Wal
Rynes v Úrad pro ochranu osobních údajů	Case C-212/13, 11 December 2014	EU
Schrems v Data Protection Commissioner	Case C-362/14, 6 October 2015	EU
Shreya Singhal v Union of India	(2015) Writ Petition (Criminal) No. 167 of 2012	Ind
Sony Music Entertainment (Ireland) Ltd & ors v UPC (No. 1)	[2015] IEHC 317	Irl
The State (Lynch v Cooney)	[1982] 1 IR 337	Irl
Tansey v Gill	[2012] IEHC 42	Irl
Totalise plc v The Motley Fool	[2001] EWCA Civ 1897	Eng
Von Hannover v Germany	[2004] EMLR 379	ECHR
Yahoo! Inc. v LICRA	169 F Supp 2d. 1181 (N.D. Cal 2001)	US

OVERVIEW AND EXECUTIVE SUMMARY

A BACKGROUND

(1) Communications in a digital and online world

1. This Report forms part of the Commission's *Fourth Programme of Law Reform*.¹ It arises against the reality that we live in a truly interconnected digital and online world. The revolution in telecoms and digital media in the first two decades of the 21st century means that we can communicate with the world through social media on smart phones and other digital devices at virtually any time. This has brought enormous positive benefits, because it has facilitated a new form of online and digital consumer society and also allowed us to participate on a national and international level in civic society and in public discourse generally. This has greatly expanded the capacity to enjoy freedom of expression and of opinions in this jurisdiction and in comparable States.
2. This freedom has, however, also brought some negative aspects, including a tendency for some online and digital users to engage in communications that cause significant harm to others, including by posting online intimate images without consent and which involve gross breaches of the right to privacy. Examples include the intentional victim-shaming of individuals (overwhelmingly women) sometimes referred to as "revenge porn" (an unhelpful shorthand because it appears to suggest it is "just porn"). Other negative developments include intimidating and threatening online messages directed at private persons and public figures. New forms of technology have also facilitated a new type of voyeurism, sometimes referred to as "upskirting" and "down blousing" in which intimate images are taken and then posted online. In addition, there have also been many instances of online and digital harassment and stalking, which also mirror to some extent the pre-digital versions of these harmful behaviours.

(2) Harmful communications and digital safety: criminal offences and civil law oversight

3. This project and Report has identified that the existing criminal law already addresses some of the harmful communications described. Not surprisingly, however, it has also identified some gaps that require reform, notably where new forms of communication have been used in harmful ways that could not have been anticipated previously. The Report therefore proposes that the existing criminal law, together with the proposals intended to deal with the new forms of harmful communications, could usefully be consolidated into a single piece of legislation, reflected in Part 2 of the draft *Harmful Communications and Digital Safety Bill* in Appendix A of this Report.
4. In addition, the public consultation carried out by the Commission leading to this Report (including a public seminar in 2015 hosted by the Commission, and a 2 day workshop with young people in 2016 facilitated by the Department of Children and Youth Affairs) has also underlined the need to address harmful communications in a wider context,

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

which would include a system of statutory oversight that promotes and supports positive digital safety.

5. The Report recommends that this should be done under a proposed Office of the Digital Safety Commissioner of Ireland, modelled on comparable offices in Australia and New Zealand, and which could build on the existing Office of Internet Safety located in the Department of Justice and Equality. The proposed Commissioner would have a general oversight and monitoring role, including functions aimed at promoting online and digital safety generally. In this respect the Commissioner would collaborate with other relevant State bodies such as the Ombudsman for Children in the development, with the Department of Education and Skills and the Department of Children and Youth Affairs, of guidance material for young people and schools on what it means to be a safe and responsible digital citizen.
6. The proposed Digital Safety Commissioner would also oversee and monitor an efficient and effective “take down” system so that harmful communications can be removed as quickly as possible from, for example, social media sites. This would include the publication of a statutory code of practice on take down procedures and associated national standards, which would build on the current non-statutory take down procedures and standards already developed by the online and digital sector, including social media sites. The proposed statutory model envisages that applications for take down of harmful communications would initially be made to the relevant digital or online service provider, such as a social media site. The Digital Safety Commissioner would become involved by way of appeal if the take down procedure did not operate in accordance with the statutory standards – and the Commissioner would also have a general monitoring and supervisory role, as is the case in the Australia and New Zealand systems. These standard-setting and oversight proposals are reflected in Part 3 of the draft *Harmful Communications and Digital Safety Bill* in Appendix A of the Report.
7. The Commission is conscious of the important position that Ireland occupies in the digital sector, including the significant presence in the State of many of the leading online and digital multinational firms. In that context, the proposals made in this Report may have an impact not only in Ireland but also some extra-territorial effect outside the State because of the reach of the firms headquartered in Ireland. In this respect, the Report begins in Chapter 1 by noting the increasing regulation internationally of aspects of online and digital communications. This includes through the Council of Europe and the case law of its European Courts of Human Rights, as well as through the European Union and the case law of its Court of Justice, as well as EU legislation that affects this area.
8. It may be that, ultimately, some aspects of harmful communications, such as the extra-territorial scope of criminal and civil law in this area, will be addressed through regional or global agreements or conventions. For the present, this Report makes recommendations on extra-territoriality that reflect existing law, both in the criminal law and civil law oversight areas.

(3) Consultation process

9. This Report is the culmination of an extensive consultation process for this project. In November 2014, the Commission published a consultative Issues Paper.² This was followed by a public seminar on 22 April 2015, as well as subsequent meetings and discussions in 2015 and 2016 with a number of individuals and bodies, including representatives from Government, the social media sector, legal practitioners, law enforcement and academia.
10. The Commission also recognises that the views of young people on the issues covered by this project need to be considered, because they are one of the groups most affected by harmful digital communications. The Commission therefore organised two consultative workshops with young people aged between 13 and 17 years, facilitated by the Department of Children and Youth Affairs. This consultation involved two sessions on 27 and 28 April 2016, with 36 young people attending on the first day and 34 young people attending on the second day. An independent report of the consultations, prepared by Ms Sandra Roe, is included in Appendix B to this Report.³ The Commission very much appreciates the enthusiastic and reflective approach of the participants at these workshops. The Commission also wishes to record its appreciation of the highly professional manner in which the Department's representatives organised these workshops, and for the high quality of the report prepared by Ms Roe.
11. There was considerable consensus at the workshops on the need for an efficient and effective take down procedure to deal with harmful digital communications, and on the need for education on good digital citizenship. The independent report in Appendix B contains a review of national and international literature that underlines the need to address harmful digital communications in a holistic manner. The views expressed at these workshops, as reflected in the report in Appendix B, greatly assisted the Commission in the development of its proposals in this Report on the role and functions of the proposed Digital Safety Commissioner.
12. The Commission also very much appreciates the views expressed in various ways, including in submissions received and in discussions, with a very wide range of other interested parties in meetings and discussions held during the consultative process. In particular, the Commission expresses its sincere thanks for the time and expertise given by many people to discuss with the Commission aspects of harmful communications and digital safety. These contributions have also been taken into account by the Commission in preparing its final recommendations in this Report.

B Guiding Principles in the Report

13. As noted above, this Report examines harmful communications and, in particular, harmful digital communications. This includes posting images or videos (especially those of an intimate nature) without consent where this involves gross breaches of privacy, setting up fake or offensive websites or social media profiles, sending

² Law Reform Commission *Issues Paper on Cybercrime Affecting Personal Safety, Privacy and Reputation Including Cyberbullying* (LRC IP 6-2014).

³ Appendix B: *Report of consultations with young people concerning harmful internet communications including cyber bullying.*

intimidating or threatening messages, as well as harassment and stalking. Particular features of digital communication exacerbate the harm caused by this behaviour, including the permanence of digital communication, its instant nature, the capacity to reach very large audiences and its facility for (actual or, in some instances, perceived) anonymity.

14. **Chapter 1** of this Report describes the Commission's general approach to reform in this area. It discusses how the Commission was guided by key principles, including:
 - the wider context within which law reform proposals should be considered, in particular the need to have in place solutions that involve education and empowerment concerning harmful digital and online communications;
 - the need to take account of relevant rights and interests, including to ensure that the law contains an appropriate balance between the right to freedom of expression on the one hand and the right to privacy on the other hand;
 - the principle of technology neutrality, which requires a focus on regulating actions and behaviour rather than simply the means used; and
 - the requirement for a proportionate legal response that recognises the respective roles of criminal law and of civil law and regulatory oversight: namely, that criminal law is used only where activity causes significant harm, and that civil law and regulatory oversight includes an efficient and effective take down procedure and a suitable statutory framework.
15. The wider context for this Report was fully analysed in the 2014 *Report of the Internet Content Governance Advisory Group* (ICGAG Report),⁴ which examined the general policy setting and governance arrangements needed to address harmful online material. In preparing this Report, the Commission has had the benefit of the discussion in the ICGAG Report of this wider context.
16. In relation to the need to balance the rights to freedom of expression and privacy, the Report discusses their recognition in the Constitution of Ireland as well as in the European Convention on Human Rights (ECHR) and EU law.
17. As to technology neutrality, this requires that the form of regulation neither imposes, nor discriminates in favour of, the use of a particular type of technology. However, technology neutrality does not necessarily require the same rules online and offline, but rather that the rules in both contexts achieve the same effect. This may require technology specific laws in certain cases.
18. With regard to proportionality, this Report applies the harm principle, which requires that responses based on policy, education and the civil law should be prioritised and that the criminal law should only be employed to deal with serious harm. The Report therefore recommends a three level hierarchy of responses to target harmful digital communications:
 - **Education:** to create user empowerment and foster safe and positive digital citizenship;

⁴ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014). See the discussion of the ICGAC Report in Chapter 1, below.

- **Civil law and regulatory oversight:** where education and related responses are ineffective and the law needs to be employed, civil law should be favoured as it is less onerous than the criminal law;
 - **Criminal law:** only the most serious harm should be subject to the criminal law.
19. This hierarchical approach is particularly important in the context of harmful digital communications because the ease with which individuals can post content online means that much internet communication is spontaneous and impulsive, and thus a vast amount of content is posted every day. A hierarchical approach is also necessary because this type of harmful communication often involves children and young people for whom the criminal justice process should be seen as a last resort and only after other responses, such as education or suitable diversion programmes, have been applied.

C Reform of Criminal Law Concerning Harmful Communications

(1) Harassment should include online or digital means of communication, and indirect forms

20. **Chapter 2** of the Report begins with a discussion of whether the harassment offence in section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be extended to incorporate a specific reference to harassment by online or digital means of communication.
21. Section 10 of the 1997 Act already applies to direct harassment of a person “by any means”. However, as the Report describes, while this probably applies to direct online or digital harassment, it does not clearly address other forms of online harassment about a person, such as posting fake social media profiles. The Commission therefore recommends that the harassment offence should be amended to include a specific reference to harassment of or about a person by online or digital means: this would offer important clarification as to the scope of the offence.
22. The Commission also recommends that section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be repealed and replaced with an harassment offence that expressly applies to harassment by all forms of communication including through digital and online communications such as through a social media site or other internet medium. As already noted, the Commission considers that this reformed harassment offence should be included in a single piece of legislation that also includes the other offences discussed in this Report: see Part 2 of the draft *Harmful Communications and Digital Safety Bill* in Appendix A.

(2) Specific offence of stalking

23. Stalking is an aggravated form of harassment characterised by repeated, unwanted contact that occurs as a result of fixation or obsession and causes alarm, distress or harm to the victim. This element of intense obsession or fixation, which creates an unwanted intimacy between the stalker and the victim, differentiates stalking from harassment.
24. The Report discusses developments in Scotland and England and Wales where specific stalking offences were introduced in 2010 and 2012 respectively. The experiences of these jurisdictions strongly suggest that the introduction of specific stalking offences led

to an increase in reporting and prosecution of stalking. Specifically naming stalking as an offence also carries great significance for victims of stalking, because of the “hidden” nature of the crime as well as its aggravated nature compared to harassment. The Commission therefore recommends that a specific stalking offence should be enacted.

(3) Need to address once-off harmful communications

25. The Report also considers whether offences are required to target once-off harmful communications. Section 10 of the *Non-Fatal Offences Against the Person Act 1997* is limited to persistent behaviour and thus does not apply to a single act that seriously interferes with a person's peace and privacy or causes him or her alarm, distress or harm. This gap has become particularly apparent with the advance of digital and online communication, because the internet enables instant communication to large audiences, often anonymously (actual or, in some cases, perceived). These features of the online and digital environment mean that even a single communication has the capacity to interfere seriously with a person's peace and privacy or cause alarm, distress or harm, particularly as internet communications are also difficult to erase completely.
26. A number of offences other than the harassment offence can be applied to some forms of harmful once-off behaviour, such as sending threatening messages in section 13 of the *Post Office (Amendment) Act 1951*, misuse of personal data under the *Data Protection Acts 1988 and 2003* or “hacking” under the *Criminal Damage Act 1991*. However, none of these offences deals comprehensively with, for example, non-consensual distribution of intimate images of adults where this is done on a once-off basis, as opposed to persistently.
27. The Report examines how other jurisdictions, such as Canada, England and Wales, Scotland and the Australian state of Victoria, have legislated for this type of criminal behaviour. This includes offences designed to target non-consensual distribution of intimate images with intent to cause harm (the victim-shaming offence often called “revenge porn”) and other offences designed to target once-off harmful communications (to address what is often referred to as “upskirting” and “down-blousing”).
28. One of the most significant challenges when legislating for harmful online behaviour is to ensure that any offences are drafted with sufficient precision so that they are not vulnerable to being found unconstitutional on grounds of vagueness. The Report explores how the vagueness doctrine has been applied in the Irish courts as well as discussing pertinent examples of legislation dealing with harmful internet communications that have been found to be unconstitutionally vague in Ireland and other jurisdictions.

(4) Offence of sending or threatening or indecent messages should apply to online communications

29. The Commission reiterates the recommendation in the 2014 *Report of the Internet Content Governance Advisory Group* (ICGAG Report)⁵ that the offence of sending threatening or indecent messages, in section 13 of the *Post Office (Amendment) Act*

⁵ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014).

1951 (which is currently limited to communication by letter, phone and SMS text), should be extended to apply to online communications. The Report recommends that the section 13 offence should be repealed and replaced with an offence of distributing a threatening, false, indecent or obscene message by any means of communication and with the intent to cause alarm, distress or harm or being reckless as to this.

(5) New offence to address once-off intentional online victim-shaming (“revenge porn”)

30. The Report recommends that there should be a new offence to target the non-consensual distribution of intimate images, including where this involves a once-off incident. This would deal with the victim-shaming behaviour where a person posts or otherwise distributes intimate images such as photos or videos with the intention of causing another person harm or distress (the so-called “revenge porn” cases). The Commission therefore recommends the enactment of an offence involving the distribution of intimate images without the consent of the person depicted in the image and where there is intent to cause alarm, distress or harm or being reckless as to this.

(6) New offence to address other once-off posting of intimate images without consent (“upskirting”)

31. In some instances, including in the case of young people, intimate images obtained are shared spontaneously or without considering the impact on the person concerned, or are re-distributed by third parties without consent. These cases may not be capable of being prosecuted under the victim-shaming offence recommended above because the intent to cause alarm, distress or harm element may not be present. The Commission therefore recommends that a separate offence should be introduced to target the non-consensual taking and distribution of intimate images without intent to cause alarm, distress or harm. This would address the so-called “upskirting” and “down-blousing” behaviour, which is a form of voyeurism.

(7) Protecting the privacy of victims

32. The distribution of intimate images has the potential to cause the persons depicted in such images significant harm in the form of distress, humiliation and shame. The victims of such activity may thus be discouraged to report to the Gardaí and pursue a prosecution for fear of generating more publicity for the images in question. The Commission therefore recommends that in any prosecution for a harmful communications offence provided for in the Report, the privacy of the person in respect of whom the offence is alleged to have been committed should be protected.

(8) Consent of DPP for cases involving persons under 17

33. The Commission recommends that no prosecution for the offences discussed in the Report may be brought against children under the age of 17 except by or with the consent of the Director of Public Prosecutions. The procedural protection reflects the Commission’s strong view that it would be highly undesirable to criminalise children under the age of 17 years for behaviour undertaken as a result of their inherent immaturity and where there is no intention to cause serious distress. It also reflects one of the Commission’s guiding principles in this Report, that in the case of children and young people, the criminal justice process should be seen as a last resort and only after other responses, such as education or suitable diversion programmes, have been applied.

(9) 2 year time limit for summary prosecutions

34. The Commission recommends that the general 6 month time limit for bringing a summary prosecution (in the District Court), in section 10(4) of the *Petty Sessions (Ireland) Act 1851*, should not apply. Instead a 2 year time limit should apply for summary prosecution of harmful communications offences. Frequently, these cases require the collection of evidence from websites with servers located outside the jurisdiction. Such content can only be obtained through the use of the Mutual Legal Assistance Treaty procedure, which can take up to 18 months to be completed. This is a significant problem in summary proceedings because the 6 month time limit will have expired before the relevant content has been received and so extending this time limit for harmful communications offences to 2 years would ensure that summary prosecutions for such offences will not be prevented by a restrictive time limit. No specific time limit applies to prosecutions on indictment.

(10) Jurisdiction and extra-territoriality in criminal law

35. In general, criminal jurisdiction is territorial, meaning that it is usually limited to offences committed within the territory of the State. Article 29.8 of the Constitution provides that the State may legislate with extra-territorial effect, which must be done expressly. There are a number of examples where the Oireachtas has expressly provided that offences have extra-territorial effect, including under the *Criminal Damage Act 1991* and the *Sexual Offences (Jurisdiction) Act 1996*. The Report recommends extra-territorial effect should apply to the harmful communications offences discussed in the Report, and that the approach taken in the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*, which concerns a comparable area, should be adopted.
36. This would allow for extra-territorial jurisdiction for harmful communications offences where: (a) a harmful communications offence is committed by a person in the State in relation to a means of communication that is located outside the State, (b) a harmful communications offence is committed by a person outside the State in relation to a means of communication in the State or (c) a harmful communications offence is committed by a person outside the State if the person is an Irish citizen, a person ordinarily resident in the State, an undertaking established under the law of the State, a company formed and registered under the *Companies Act 2014* or an existing company within the meaning of the *Companies Act 2014* and the offence is an offence under the law of the place where the act was committed.

(11) Penalties on conviction

37. The Report outlines the current penalties that apply on conviction for offences relating to harmful digital communications and makes recommendations for the penalties that should accompany the offences provided for in the Report.
38. The Commission considers that the maximum penalties for the harassment offence under section 10 of the *Non-Fatal Offences Against the Person Act 1997* are sufficient and provide a suitable upper level for penalties that should apply to the reformed harassment offence and to the other 3 intent-based offences proposed in the Report. The Commission therefore recommends that the intent-based offences in the Report should carry, on summary conviction, maximum penalties of a Class A fine (currently, a fine not exceeding €5,000) and/or up to 12 months imprisonment, and on conviction on indictment, an unlimited fine and/or up to 7 years imprisonment.

39. The Commission recommends that the fifth offence dealt with in the Report, of taking or distributing an intimate image without consent (to deal with so-called “upskirting” and “down-blousing”), should be a summary offence only, and that the maximum penalties on conviction under this offence should be a Class A fine and/or up to 6 months imprisonment.

(12) Intersection with hate crime

40. The Report has also explored the extent to which the current law on hate crime intersects or overlaps with harmful online and digital communications.
41. The main legislation designed to deal with hate crime is 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.” Incitement includes publication, broadcast and preparation of materials. The 1989 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.” However, the 1989 Act has been subject to significant criticism for its perceived inefficacy, illustrated by the limited number of prosecutions that have been taken under it.
42. Ireland intends to ratify the Council of Europe Convention on Cybercrime,⁶ and has been encouraged to ratify the Additional Protocol to the Convention concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.⁷ Ireland is also obliged to implement the 2008 EU Framework Decision on combating racism and xenophobia.⁸
43. In this respect it is clear that comprehensive reform of hate crime legislation is due to be enacted in the future, and the Commission considers that it would not therefore be appropriate to address separately, in this Report, online hate speech only. Because wide-ranging reform of hate speech is outside of the scope of this project, the Commission recommends that online hate speech should be addressed as part of the general reform of hate crime law.

D Digital Safety Oversight, Take Down Procedure and Civil Law

(1) Absence of effective oversight system or civil remedies

44. **Chapter 3** of the Report addresses the need for an oversight system to promote digital safety, including an efficient take down procedure for harmful digital communications.
45. The chapter begins by describing the existing, non-statutory, content and conduct policies of social media companies and their reporting and takedown processes. The Report then discusses the existing civil remedies that apply in relation to harmful digital

⁶ Council of Europe, Convention on Cybercrime (23 November 2001). Ireland signed this Convention on 28 February 2002. The Government Legislation Programme, Summer Session 2016, states that work on a Bill to implement the Convention is underway.

⁷ 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).

⁸ 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.

communications including the remedies available under the *Defamation Act 2009* and remedies for breach of the constitutional right to privacy. The remedies under the *Data Protection Acts 1988 and 2003* are also considered as well as the developments that have taken place in EU law on data protection and privacy, including case law of the EU Court of Justice and the 2016 General Data Protection Regulation.⁹

46. The Report acknowledges that available processes and remedies may not be effective, and that the potential cost, complexity and length of civil proceedings may prevent victims of harmful digital communications from obtaining redress in court. A victim of harmful communications should be able to have a readily accessible and effective take down procedure available to him or her.
- (2) Digital Safety Commissioner would promote internet safety and oversee take down procedures**
47. The Report describes the enactment of New Zealand's *Harmful Digital Communications Act 2015* and Australia's *Enhancing Online Safety for Children Act 2015*, which have established statutory bodies to promote online and digital safety and to provide oversight of take down procedures operated by online service providers such as social media sites.
 48. The Report recommends that an Office of the Digital Safety Commissioner of Ireland should be established on a statutory basis, broadly modelled on the Australian approach. The Digital Safety Commissioner would have functions related to promoting online safety as well as overseeing and monitoring an efficient and effective procedure for takedown of harmful digital communications.
 49. The Commission considers that the Office of Internet Safety, which was established in the Department of Justice and Equality to take a lead role for internet safety in Ireland, may be a suitable body to take on the role of the Digital Safety Commissioner. The Report notes that this would require decisions by the Government and Oireachtas on the necessary funding and staffing of the Office of the Commissioner, and that these are matters outside the scope of this Commission's role.
- (3) The Commissioner's educational and promotional roles**
50. The Report recommends that the Digital Safety Commissioner's functions should include an educational and promotional role concerning digital safety in collaboration with relevant Government Departments and State bodies. In the specific context of internet safety for children and young people, the Report envisages that the Commissioner would liaise with the Ombudsman for Children in the development, with the Department of Education and Skills and the Department of Children and Youth Affairs, of guidance material for young people and schools on what it means to be a safe and responsible digital citizen. It would also include guidance on the use of mediation and restorative processes.

⁹ Regulation (EU) 2016/679 (the General Data Protection Regulation, GDPR). In 2018, the GDPR will repeal Directive 95/46/EC, the 1995 Directive on data protection, which had been implemented by the *Data Protection (Amendment) Act 1993*.

(4) The Commissioner's oversight and supervision functions

51. The oversight and supervision functions of the Commissioner would operate in a similar way to the Australian e-Safety Commissioner, requiring digital service undertakings to comply with a statutory code of practice, developed after suitable consultation by the Digital Safety Commissioner. The statutory framework would also include National Digital Safety Standards, which would require the digital service undertaking to have in place a provision prohibiting the posting of harmful digital communications, a complaints scheme whereby users can request free of charge the removal of harmful digital communications, a timeline for responding to complaints and a contact person to engage with the Commissioner.
52. If the Commissioner were to be satisfied that a digital service undertaking complied with the code of practice and the National Digital Safety Standards, the Commissioner would be empowered to issue a certificate of compliance, which would have the presumptive effect that the digital service undertaking was in compliance with the code and the standards. The Report proposes that the Digital Safety Commissioner should have responsibility for harmful content involving all individuals, adults and children.

(5) Proposed take down procedure

53. The proposed take down procedure would require a user initially to make his or her complaint directly to the relevant digital service undertaking, such as a social media site. If the content was not taken down in accordance with the time specified in the code of practice, the user could make a complaint to the Commissioner. The Commissioner would then investigate the complaint and if the complaint were to be upheld, the Commissioner would direct the digital service undertaking to remove the specified communication and would revoke the certificate of compliance issued to the provider. If the digital service undertaking were to refuse to comply with the direction of the Commissioner to remove the communication, the Commissioner could apply to the Circuit Court for an order requiring compliance by the undertaking.

(6) Civil restraining orders for harmful communications

54. Section 10 of the *Non-Fatal Offences Against the Person Act 1997*, unlike the English and Welsh *Protection from Harassment Act 1997*, does not allow separate civil proceedings to be brought based on its provisions. However, section 10(3) of the 1997 Act empowers a court to make a restraining order restricting a person from communicating and/or approaching the victim where the person has been convicted of harassment. Section 10(5) of the 1997 Act also allows restraining orders to be made where a person has been acquitted of harassment.
55. The Report recommends that, in cases involving the harmful communications discussed in this Report, restraining orders should be available without the need to initiate criminal proceedings. This would provide victims with a valuable remedy in cases where criminal proceedings may be unsuitable or undesirable from the perspective of the victim.

(7) Court powers in intended civil proceedings: *Norwich Pharmacal* orders

56. *Norwich Pharmacal* orders allow for the disclosure of the name and IP address of parties unknown to the plaintiff against whom the plaintiff intends to issue civil proceedings for alleged wrongful conduct.
57. At present, *Norwich Pharmacal* orders are not provided for in legislation, and only the High Court can issue them as part of its inherent jurisdiction. This means that the cost of obtaining such orders is high and the remedy is not available to many individuals. The 2014 *Report of the Internet Content Governance Advisory Group* recommended that the power to make such orders should be placed on a statutory basis and extended to the Circuit Court. The Commission agrees with this recommendation.
58. Currently, *Norwich Pharmacal* orders usually involve a two-step mechanism whereby an individual has to first seek an order against the relevant website to disclose user and IP details. Once furnished, these details may lead to data held by a telecoms company, many of whom require a second *Norwich Pharmacal* order before agreeing to disclosure. The Commission therefore recommends that a one-step procedure be adopted for such orders whereby only one application would be required which would apply to both the relevant website and the telecoms company.
59. The Commission also recommends that the person alleged to have posted the harmful communication should be given the opportunity of appearing and making representations before the court makes a *Norwich Pharmacal* order, because at present such orders are granted on an *ex parte* basis (without notice to the affected party), which may infringe the right to fair procedures and to anonymous speech.

(8) Jurisdiction and extra-territoriality in civil law

60. The Report also makes recommendations in relation to the extra-territorial role of the proposed Digital Safety Commissioner and in connection with the civil remedies discussed above.
61. The Report recommends that the territorial scope of these civil aspects of harmful communications should, in general, apply to harmful communications where: (a) such harmful communications affect an Irish citizen or a person ordinarily resident in the State, and (b) the means of communication used in connection with such harmful communications are within the control of an undertaking or company established under the law of the State.
62. The Commission also recommends that they should have some extra-territorial effect in connection with an Irish citizen or a person ordinarily resident in the State. This should reflect the approach taken in connection with the extra-territorial enforcement of civil proceedings generally, including under the “service out” procedures in the *Rules of the Superior Courts 1986*.¹⁰ The Report therefore recommends that this extra-territorial effect would be where the means of communication used in connection with harmful communications are within the control of an undertaking established under the law of another State but where an Irish court would have jurisdiction to give notice of service

¹⁰ *Rules of the Superior Courts 1986* (SI No.15 of 1986), Orders 11-11D.

outside the State in respect of civil proceedings to which such harmful communications refer.

- 63. **Chapter 4** contains a list of the 32 recommendations made in the Report.
- 64. **Appendix A** contains a draft *Harmful Communications and Digital Safety Bill* to implement the recommendations for reform in the Report.
- 65. **Appendix B** contains the text of an independent report, prepared by Ms Sandra Roe, of the two consultative workshops held with young people on 27 and 28 April 2016, facilitated for the Commission by the Department of Children and Youth Affairs.

CHAPTER 1 GUIDING PRINCIPLES

A The Digital and Online World

- 1.01 We now live in a truly interconnected digital and online world. The emergence of digital technology, notably social media, in the early part of the 21st century has transformed how we communicate with each other. This has brought enormous positive benefits, because we can: keep in visual and written contact with family and friends who are half way around the world; order and buy food, clothes, books and services online; plan and book holidays, flights and holiday insurance online; obtain an almost endless amount of digital information about the world and its history; and participate on a national and international level in civic society and in public discourse generally. This has greatly expanded the capacity to enjoy freedom of expression and of opinions in this jurisdiction and in comparable States. It has facilitated a new form of online and digital consumer society and also allowed us to participate on a national and international level in civic society and in public discourse generally. This has greatly expanded the capacity to enjoy freedom of expression and of opinions in this jurisdiction and in comparable States.
- 1.02 This freedom has, however, also brought some negative aspects, including a tendency for some online and digital users to engage in communications that cause significant harm to others, including by posting online intimate images without consent and which involve gross breaches of the right to privacy. This project and Report examines harmful communications, including harmful digital communications that affect personal safety, privacy and reputation. Such content can be uploaded on websites, particularly social media websites such as Facebook or Twitter or video sharing websites such as YouTube, or can be distributed by email, instant messenger, SMS or appear in chat rooms.
- 1.03 This can include a wide spectrum of activities, at one end of which are repeated communications that are intended to be harmful and to cause fear and at the other end are one-off communications that involve invasions of privacy of an embarrassing or hurtful kind but might be described as being at the lower end of harmful. This spectrum therefore includes:
 - repeatedly sending messages *directly to a person* that are harmful and are neither sought or wanted by that person: in other words the online version of offline stalking, harassment or threatening communications;
 - creating a fake profile on a social media site *about a person* that includes harmful material intended to be damaging or shaming to the person: when created about a former partner, this is sometimes referred to as “revenge porn”, but the Commission does not support the use of that phrase, because it may appear to suggest that it is “just porn”;
 - one-off posting online of an image or video of an intimate nature without the consent of the person involved: a version of voyeurism, also referred to as “upskirting”;
 - posting personal information online without consent;
 - posting embarrassing information online.

- 1.04 Harmful digital activity thus sometimes involves persistent, repeated, acts and is therefore directly comparable with offline harassment and stalking. The Commission has, however, also taken into account that a “one-off” online act may have harmful ripple effects that are particular to the online and digital environment: the one off upload can very quickly be spread globally and have virtually an immediate impact that may in fact be more damaging than offline persistent harmful behaviour.
- 1.05 Indeed, there are a number of significant features of harmful digital communications that contrast with similar offline behaviour:
- **Disconnection:** 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 phone, laptop or similar device.
 - **Anonymity:** This sense of disconnection is increased by the air of anonymity (frequently perceived rather than actual) involved in digital communications and may prompt individuals to act in a manner they would not in the offline world.¹ This air of 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.
 - **Instant communication:** The instant nature of digital communications 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.
 - **Global audiences:** 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.
 - **Permanence:** 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.²
- 1.06 While this Report therefore deals with a wide spectrum of harmful digital and online activities, it is important to note that it is limited to activities directed at a specific person or about that person. This can include children and young persons as well as adults. It therefore includes some activity that is already currently covered by the criminal law, notably the offence of harassment (which includes stalking) in section 10 of the *Non-Fatal*

¹ 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>.

² 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. This case is discussed further in Chapter 3 at paragraph 3.35.

Offences against the Person Act 1997. As noted below in this Report section 10 of the 1997 Act probably does not cover, for example, the creation of fake social media profiles or the victim shaming (so-called “revenge porn”). The Report also overlaps with other existing law and procedures that deal with illegal online activity. This includes for example the *Data Protection Acts 1998 and 2003* (harmful communications often involve unlawful use of personal data), the *Criminal Damage Act 1991* (“hacking” may have taken place) or the *Child Pornography and Trafficking Act 1998* (posting intimate images of young people online).

- 1.07 Nonetheless, although the recommendations in this Report concerning reform of the criminal law (Chapter 2) and reform of civil law and oversight of digital safety (Chapter 3) may overlap with aspects of such existing laws, they differ in important respects from those statutory provisions and are intended to operate quite separately. For example, although Chapter 2 of the Report recommends the enactment of offences that involve the distribution of intimate images without consent, those offences are not proposed as sexual offences, but rather offences that involve an intention to cause serious harm to the person, including a serious breach of the person’s right to privacy. The Report also overlaps to some extent with the regulation of hate speech, but as this is usually directed at a general group of people rather than a specific person, and because this area is to be reformed in the near future in the wider context of reform of hate crime, it falls outside the scope of this Report (see the discussion at the end of Chapter 2).

B 2014 Report of the Internet Content Governance Advisory Group

- 1.08 There is a growing awareness internationally of the need to address related harmful internet content, including harmful digital communications.³ In 2013, the Oireachtas Joint Committee on Transport and Communications published a *Report on Addressing the Growth of Social Media and Tackling Cyberbullying*,⁴ which identified gaps in the governance and law concerning harmful internet content and recommended the need for a general review of this area. In response to this Report, the Minister for Communications, Energy and Natural Resources (now the Minister for Communications, Climate Action and the Environment) established the Internet Content Governance Advisory Group. This led to the publication of the 2014 *Report of the Internet Content Governance Advisory Group* (ICGAG Report),⁵ which comprehensively examined the general policy setting and governance arrangements needed to address harmful online material.
- 1.09 In accordance with the Advisory Group’s terms of reference the ICGAG 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

³ 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).

⁴ *Report on Addressing the Growth of Social Media and Tackling Cyberbullying* (Houses of the Oireachtas, 2013).

⁵ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014).

campaigns, who have experienced identical issues when faced with menacing online comments.⁶ The Commission's examination of harmful communications addresses the matter in relation to its impact on all persons.

- 1.10 The ICGAG Report 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 following:
- 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; and
 - 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.
- 1.11 The ICGAG 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; and
 - 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.⁷
- 1.12 The ICGAG Report noted this project and therefore left to the Commission consideration and recommendations for law reform in this area, including any proposed reform of the

⁶ 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 in Chapter 2, paragraphs 2.83-2.88.

⁷ This is discussed further in Chapter 3, paragraphs 3.106-3.108.

offence of harassment in section 10 of the *Non-Fatal Offences against the Person Act 1997*.⁸ Following publication of the 2014 Report, a cross departmental group was established in July 2014. This group is chaired by the Department of Communications, Climate Action and Environment and includes representatives from the Departments of Justice and Equality, Children and Youth Affairs, Education and Skills and Health. At the time of writing (September 2016) the group is understood to be preparing a document for Government outlining a set of measures to implement the 2014 Report.⁹ The focus of this present Report is on the reform of the criminal law concerning harmful communications and on a statutory oversight model to promote digital safety and for an effective civil law take down procedure. The policy and governance recommendations in the 2014 Report, and in this Report, remain a matter for the Government and Oireachtas to consider, notably in terms of staffing and funding of any oversight body for harmful digital communications.

C Principles of Reform

1.13 A number of key principles have guided the Commission's approach to reform in this area, including:

- the wider context within which law reform proposals should be considered, as discussed in the 2014 ICGAG Report, above, in particular the need to have in place solutions that involve education and empowerment concerning harmful digital and online communications;¹⁰
- the need to take account of relevant rights and interests, including to ensure that the law contains an appropriate balance between the right to freedom of expression on the one hand and the right to privacy on the other hand;
- the principle of technology neutrality, which requires a focus on regulating actions and behaviour rather than simply the means used; and
- the requirement for a proportionate legal response that recognises the respective roles of criminal law and of civil law and regulatory oversight: namely, that criminal law is used only where activity causes significant harm, and that civil law and regulatory oversight includes an efficient and effective take down procedure and a suitable statutory framework.

(1) Balancing the Right to Privacy and the Right to Freedom of Expression in the internet context

1.14 Limited restraint on freedom of speech is an ideal upon which the internet was built. As John Perry Barlow stated in his famous paper "A Declaration of the Independence of Cyberspace", the internet is a "world where anyone, anywhere may express his or her

⁸ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014) at 45 and 64.

⁹ See website of the Department of Communications, Climate Action and Environment, "Internet Content" available at <http://www.dcenr.gov.ie/communications/en-ie/Internet-Policy/Pages/Internet-Content.aspx>.

¹⁰ See also generally Department of the Taoiseach, *Regulating for a Better Future: A Government Policy Statement on Sectoral Economic Regulation* (Department of the Taoiseach, Government Publications, 2013).

beliefs, no matter how singular, without fear of being coerced into silence or conformity.”¹¹

- 1.15 The internet allows people to connect with each other globally, to share ideas and opinions as well as creative content, to maintain contact and participate in debate. It allows individuals to establish contact with broad groups of people worldwide as well as foster closer ties with family, friends and other “real world” contacts. The internet also enables individuals to contribute to and shape debates on important political and social issues, and within states with repressive regimes, the internet can be a particularly valuable means of allowing people to have their voices heard. Freedom of expression is therefore the lifeblood of the internet and needs to be protected. As David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, notes in a 2015 Report, the internet “has profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within reach of everyone who has access to it” so much so that it has become, within a relatively brief period “the central global forum”.¹² Thus, he states, “an open and secure Internet should be counted among the leading prerequisites for the enjoyment of the freedom of expression today”.¹³
- 1.16 However, other rights also need to be safeguarded in the online setting, most notably, the right to privacy which can encapsulate related rights including rights to safety, reputation and dignity. The internet leaves individuals vulnerable to serious privacy violations through the non-consensual posting of private, false, humiliating, shameful or otherwise harmful content. Often the potential consequences of uploading harmful content is not appreciated by those responsible for such actions as it can be difficult to foresee how quickly or widely content may spread. For example, the fellow students of the so-called “Star Wars Kid” were unlikely to have predicted when they uploaded an embarrassing video of their classmate emulating lightsabre movements with a golf club that the video would go “viral” and remain in public consciousness more than 10 years after the upload.¹⁴ The subject of this video had to withdraw from mainstream education and receive counselling. Although this is an extreme example, it is by no means an exceptional one: the media has reported many other cases of videos uploaded online that have gone viral with potentially devastating consequences.¹⁵
- 1.17 Images uploaded online without consent can have similarly far-reaching effects, particularly where such images are of an intimate nature. In particular, the phenomenon of victim shaming (so-called “revenge porn”) where intimate images taken during a relationship are later uploaded online when the relationship ends, sometimes through

¹¹ John Perry Barlow “A Declaration of the Independence of Cyberspace”, 8 February 1996, available at <https://projects.eff.org/~barlow/Declaration-Final.html>. This declaration was widely distributed and displayed on websites during the 1990s and early 2000s.

¹² UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, 22 May 2015, A/HRC/29/32 at paragraph 11.

¹³ *Ibid.*

¹⁴ “Ten Years Later, Star Wars Kid Speaks” available at <http://news.yahoo.com/blogs/sideshow/10-years-later-star-wars-kid-speaks-231310357.html>; See also Solove “Speech, Privacy and Reputation on the Internet” in Levmore and Nussbaum (eds) *The Offensive Internet: Speech, Privacy and Reputation* (Harvard University Press, 2010) at 15.

¹⁵ For example, the “Slane girl” discussed further in Chapter 2, paragraph 2.164.

emails, SMS or other forms of electronic communication (a practice often referred to as “sexting”), can have serious psychological consequences for the victim involved.¹⁶ The threat of uploading such content can also be used to threaten or attempt to control the subject.

(a) Social Media Sites

- 1.18 A focal point for many concerns relating to online privacy is the use of social media sites, as they can frequently be the setting for harassment and privacy violations. Although there are other types of websites which can also be the hosts of harmful activity and should not be overlooked, such as online gaming sites, blogs, message boards (such as Reddit) and specialised sites such as those dedicated to so-called revenge porn, the enormous popularity of social media sites and the extent to which they have become embedded in 21st century society suggests that they are, for the typical internet user, the most likely site of harm and therefore deserving of scrutiny.¹⁷

(i) Social Media v Social Networking

- 1.19 Although some commentators argue that the terms “social media” and “social networking” are distinct, with social media focused on sharing content and social networking based around creating and fostering relationships,¹⁸ the terms are frequently used synonymously, and this Report follows that approach. In general, “social media” and “social media site” are favoured in this Report as these terms have come to be more popular in general usage and potentially encompass a broader range of activity. However, there are a number of instances in which “social networking” and “social networking sites” are used, mainly where these terms are used by a particular group, such as the discussion of the MRBI polls on social networking, or in a particular context, notably that of data protection, as “social networking” has been used by the Article 29 Working Group¹⁹ and in the text of the 2016 EU General Data Protection Regulation.²⁰

¹⁶ “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>.

¹⁷ For example, half of the respondents to a 2016 European Parliament study on *Cyberbullying among young people* identified social media sites as a channel for cyberbullying. See European Parliament, Directorate General for Internal Policies, *Cyberbullying Among Young People* (EU Parliament Policy Department for Citizen’s Rights and Constitutional Affairs, September 2016) at 29. Similar findings were made in studies by the UN Special Representative of the Secretary General on Violence against Children and the 2014 Net Children Go Mobile Report, both of which concluded that social media sites are the most common technologies used by children for cyberbullying. See Office of the UN Special Representative of the Secretary-General on Violence against Children, *Thematic Report: Releasing children’s potential and minimizing risks: information and communication technologies, the internet and violence against children*, (2014) at 31; Mascheroni and Ólafsson, *Net Children Go Mobile: Risks and Opportunities Second Edition* (2014) at 64.

¹⁸ “Social Media vs. Social Networking” *The Huffington Post* 2 October 2013 available at http://www.huffingtonpost.com/fauzia-burke/social-media-vs-social-ne_b_4017305.html.

¹⁹ Article 29 Data Protection Working Party *Opinion 5/2009 on online social networking* 01189/09/EN WP 163 (June 2009).

²⁰ Recital 18 of *Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.

(ii) Definition and Examples

- 1.20 Social media sites are an extremely significant element of modern internet usage and have many valuable functions, in particular, they are an important communication tool allowing individuals to create and nurture relationships and connections as well as share content. Social media sites have been defined as:

“web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.”²¹

Therefore, the key feature of social media sites is a public or a semi public profile through which users connect with other users. The nature of these connections can vary from site to site, with some social media sites used predominantly to connect with friends, family and acquaintances known to the user in the offline world, others used to make professional or career based connections and other sites used to connect people based on interests who may not know each other outside of the online setting. However, it appears that most social media sites are not used to meet new people but rather to communicate with people who are already part of the user’s extended social network, which includes individuals who may only be distantly connected to the user offline.²²

- 1.21 With over one billion users, Facebook is currently the world’s most popular social media site. According to an April 2016 Ipsos MRBI Poll on Social Networking, 64% of people in Ireland have Facebook accounts.²³ In addition, 72% of these account holders use Facebook daily which is significantly more than other social networking sites²⁴ and illustrates the extent to which Facebook has become embedded in the lives of many members of Irish society. Facebook allows users to set up a profile in their own name, share information, post pictures and videos, message others and comment on content shared by others.
- 1.22 Twitter is the second most popular social media site in Ireland with 29% of the population having Twitter accounts.²⁵ Twitter is a “micro-blogging” site, which allows users to post short messages or updates (in general, 140 characters or less) known as “tweets” and “follow” others, including people known to the user as well as celebrities. Users of Twitter can use their real names, as is required for users of Facebook, but may also use pseudonyms.
- 1.23 Ask.fm is a social media site which appears to be more popular with teenagers and young people unlike other social networking sites which tend to have users of all ages.²⁶ Ask.fm

²¹ Boyd and Ellison, “Social Network Sites: Definition, History, and Scholarship” (2008) 13 J Comput Mediat Commun 210, at 211.

²² *Ibid.*

²³ Ipsos MRBI, *Social Networking Quarterly* April 2016 available at http://ipsosmrbi.com/wp-content/uploads/2016/05/SN_Apr16.png.

²⁴ *Ibid.* The second highest “engagement” figures belonged to Instagram, with 50% of account holders using it daily, followed by Twitter (39%), Google+ (19%), Pinterest (15%) and LinkedIn (14%).

²⁵ *Ibid.*

²⁶ Ask.fm was not included in the Ipsos MRBI poll.

allows users to set up profiles and ask other users questions, with the option of doing so anonymously. Other significant general social media sites include Tumblr and Google+.²⁷

- 1.24 Niche social media sites also exist including LinkedIn, which is based on forming professional or work related connections,²⁸ video sharing sites like YouTube and Vine and photo-sharing sites such as Instagram (which is owned by Facebook), Pinterest and Snapchat. Some social media sites are extremely popular within particular countries without enjoying the worldwide usage of sites such as Facebook and Twitter including Mixi (Japan), VK (Russia), Qzone and Sina Weibo (China).
- 1.25 There have also been a number of social media sites which once enjoyed great popularity but have declined significantly in usage in more recent times, including MySpace, which was once the world's most popular social media site, and Bebo which had a very large user base in Ireland and the UK. The growth in popularity of Facebook is generally accepted as the main reason why both MySpace and Bebo, both of which had similar functions to Facebook, declined in usage.²⁹
- 1.26 The majority of social media users are under the age of 35. According to a 2013 Report, 63% of all Facebook users in Ireland were under 35.³⁰ Of this figure, only 11% of users were under the age of 18, illustrating that while social media use is commonly associated with teenagers, it is young people between the ages of 18 and 35 which appear to comprise the greatest number of users. However, this is slowly changing and gradually social media sites are attracting users from a broader age demographic, with individuals over the age of 50 increasingly availing of such services.³¹ Privacy concerns relating to social media sites are therefore a matter of growing concern for all members of society.

(iii) ***Financing of Social Media Sites***

- 1.27 Social media sites are free to join, to encourage the greatest number of people to sign up to their services. Revenue for such sites is generated by advertising. A significant amount of this advertising is targeted at users based on the information which users of the site consent to be made publicly available. Thus, although there is no financial cost to using social media sites, users pay for their usage through supplying information. Therefore,

²⁷ Google+ is the third most popular social networking site in Ireland according to the Ipsos MRBI poll with 27% of people living in Ireland having accounts. The MRBI Poll also found that 3% of the population have Tumblr accounts.

²⁸ LinkedIn, according to the Ipsos MRBI poll, is the fourth largest social networking site in Ireland, with 25% of the population having accounts. The next most popular sites are Instagram (23%) and Pinterest (16%).

²⁹ Besides being unable to hold off competition from Facebook, there were other reasons for the decline of MySpace and Bebo. Safety concerns contributed to the decline of MySpace, in particular, the site was implicated in a series of sexual interactions between adults and minors - see Boyd and Ellison, "Social Network Sites: Definition, History, and Scholarship" (2008) 13 J Comput Mediat Commun 210, at 217; Bebo was effected by a lack of financing from parent company AOL. See "Bebo: where did it all go wrong?" *The Guardian* 7 April 2010 <http://www.theguardian.com/media/2010/apr/07/bebo-facebook>.

³⁰ "Social Media Statistics Ireland [Infographic]" *EightyTwenty* 24 April 2013 available at <http://www.eightytwenty.ie/blog/social-media-statistics-ireland-infographic/>.

³¹ According to a survey of US Facebook users carried out by the Pew Research Center in 2014, 63% of adults aged between 50-64 have Facebook accounts (up from 60% in 2013) and 56% of adults over 65 have accounts (up from 45% in 2013). See Pew Research Center, *Social Media Update 2014* (January 2014), page 5, available at http://www.pewinternet.org/files/2015/01/PI_SocialMediaUpdate20144.pdf.

while users generally do not view their relationship with social media sites as a commercial one, the “transaction between user and site is essentially economic”.³² Such is the popularity of the largest social media sites that some are very profitable and have a high market value. For example, as of June 2016, Facebook’s market value was estimated to be over \$340 billion making it the seventh largest company by market capitalisation.³³ As publicly available information generates revenue for social media sites, it is at least arguable that there is a risk that user privacy may take a subordinate role to the, legitimate, goal of profitability.

(iv) ***Social Media Sites and Privacy***

- 1.28 Social media sites are premised on the notion of sharing content with others and as the popularity of such sites illustrates, a large section of society appears to have become comfortable with habitually sharing personal information with a wide social network. This has been acknowledged by Mark Zuckerberg, the founder of Facebook: “people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time”.³⁴ However, this does not necessarily mean that users of social media sites do not also value some form of privacy, albeit an evolving one.
- 1.29 It has been argued that users of social media continue to value privacy, but that their definition of privacy differs to traditional understandings of the concept. Thus, privacy in the context of social media means that while a user may consent to disclosing information to a select group this does not indicate that the user has consented to broader public disclosure.³⁵ In other words, privacy in this setting emphasises the importance of control over one’s own information. However, individuals often use social media sites without realising how much of their personal information is public or appreciating the large number of users who may have access to it. In addition, removing content from social media sites can be very difficult as sites appear to be reluctant to remove material unless it is obviously illegal in nature, such as child pornography.³⁶ There a number of reasons for this reluctance, including a desire to protect freedom of expression. However, the immunity from liability that such sites enjoy under the EU 2000 eCommerce Directive³⁷ and the lack of clarity around the notice and takedown procedure provided for under the Directive is also a factor.

³² Rodrigues, “Privacy on Social Networks” in Levmore and Nussbaum (eds) *The Offensive Internet: Speech, Privacy and Reputation* (Harvard University Press, 2010), at 243.

³³ “Largest Companies by Market Cap Today” *Dogs of the Dow* 2 June 2016 available at <http://dogsofthedow.com/largest-companies-by-market-cap.htm>.

³⁴ “Privacy no longer a social norm, says Facebook founder” *The Guardian* 11 January 2010 available at <http://www.theguardian.com/technology/2010/jan/11/facebook-privacy>.

³⁵ Rodrigues, “Privacy on Social Networks” in Levmore and Nussbaum (eds) *The Offensive Internet: Speech, Privacy and Reputation* (Harvard University Press, 2010), 250, referencing Strahilevitz, “A Social Network’s Theory of Privacy” (2005) *U Chi L Rev* 919.

³⁶ The content and conduct policies of social media sites are discussed more extensively in Chapter 3 at paragraphs 3.04–3.13.

³⁷ Directive 2000/31/EC (the eCommerce Directive), which was implemented in Ireland by the *European Communities (Directive 2000/31/EC) Regulations 2003* (SI No. 68 of 2003).

- (b) ***2000 eCommerce Directive: general immunity for “mere conduits” of information and of internet content hosts for illegal content Social Media Sites and Privacy***
- 1.30 Article 12 of the eCommerce Directive, implemented by Regulation 16 of the *European Communities (Directive 2000/31/EC) Regulations 2003*, provides that an internet service provider, such as a telecoms company or social media site, “shall not be liable” for information transmitted by it in a communication network provided it acts as a “mere conduit” of the information in question. Similarly, Article 13 of the eCommerce Directive, implemented by Regulation 17 of the 2003 Regulations, provides that a site that provides a caching service also enjoys, in effect, immunity from liability for the cached content.
- 1.31 Article 14 of the eCommerce Directive, implemented by Regulation 18 of the 2003 Regulations, provides that an internet site that hosts content, which includes a social media site, is not liable for this content, provided the site either (a) “does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent”; or (b) “upon obtaining such knowledge or awareness, [the site] acts expeditiously to remove or disable access to the information.”³⁸
- 1.32 Article 15 of the eCommerce Directive also provides that EU Member States “shall not impose a general obligation on [internet service] providers to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.” Article 15 provides, however, that Member States “may” establish obligations on internet service providers “promptly to inform the

³⁸ Article 14 (hosting) of the 2000 eCommerce Directive provides:

“1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States’ legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.”

Article 14 was implemented by Regulation 18 of the *European Communities (Directive 2000/31/EC) Regulations 2003* (SI No. 68 of 2003), which provides:

“(1) An intermediary service provider who provides a relevant service consisting of the storage of information provided by a recipient of the service shall not be liable for the information stored at the request of that recipient if—

(a) the intermediary service provider does not have actual knowledge of the unlawful activity concerned and, as regards claims for damages, is not aware of facts or circumstances from which that unlawful activity is apparent, or

(b) the intermediary service provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

(2) Paragraph (1) shall not apply where the recipient of the service is acting under the authority or the control of the intermediary service provider referred to in that paragraph.

(3) This Regulation shall not affect the power of any court to make an order against an intermediary service provider requiring the provider not to infringe, or to cease to infringe, any legal rights.”

competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.”³⁹ Article 15 was not directly transposed into Irish law, but in 1999 a system for reporting illegal internet content, hotline.ie, was established on foot of the 1998 *Report of the Working Group on the Illegal and Harmful Use of the Internet*, which recommended that a non-statutory industry self-regulatory framework should be established. Hotline.ie is operated by the Internet Service Providers Association of Ireland (ISPAI), and is co-funded by the ISPAI and the EU Commission, under the Commission’s Connecting Europe Facility Telecom – Safer Internet – Programme. Hotline.ie is overseen by the Office for Internet Safety in the Department of Justice and Equality.⁴⁰

- 1.33 The purpose of the immunity provisions in Articles 12 to 15 of the eCommerce Directive is to facilitate the free movement of “information society services” and is a specific reflection in EU law of a more general principle, namely, freedom of expression.⁴¹ Thus, the Directive contributes to the continued growth of such online sites and ensures that online freedom of expression is protected. It should be noted, however, that because liability only arises where a site becomes actually aware of harmful or illegal material, this has the effect that the less internet service providers engage with the content they host the less responsibility they will incur and consequently, the more likely they will be able to avoid liability.⁴² The relevant case law of the Court of Justice of the European Union (CJEU) confirms this view.
- 1.34 In *Google France v Louis Vuitton*,⁴³ the CJEU held that for a service provider to avail of the hosting defence in Article 14 of the eCommerce Directive, “it is necessary to examine whether the role played by that service provider is neutral, in the sense that its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data it stores”.⁴⁴ Thus if the service provider plays an active role such as to give it knowledge or control over the data, then it cannot avail of the liability exemption.

³⁹ Article 15 (No general obligation to monitor) of the eCommerce Directive provides:

“1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.”

⁴⁰ Aside from this non-statutory arrangement, McCarthy has suggested that “[m]ost likely, Article 15 can be directly relied upon in domestic proceedings given that it meets the requisite standard of being ‘unconditional and sufficiently precise’ in its formulation”. See McCarthy, “Is The Writing on the Wall for Online Service Providers? Liability For Hosting Defamatory User-Generated Content Under European and Irish Law” (2015) *Hibernian LJ* 16 at 23.

⁴¹ Recital 9 of the eCommerce Directive.

⁴² See McCarthy, “Is The Writing on the Wall for Online Service Providers? Liability For Hosting Defamatory User-Generated Content Under European and Irish Law” (2015) *Hibernian L.J.* 16 at 18.

⁴³ Joined Cases C-236/08 to C-238/08 *Google France v Louis Vuitton* OJ C134/2.

⁴⁴ *Ibid* at paragraph 113.

- 1.35 In *L'Oréal SA v eBay International AG and Others*,⁴⁵ the CJEU considered the knowledge requirements in Article 14(1)(a) and (b) of the Directive, stating that a service provider would be unable to avail of the liability exemption if it is "aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality in question and acted in accordance with Article 14(1)(b) of the Directive."⁴⁶ The CJEU added that in order for the rules set out in Article 14(1)(a) not to be "rendered redundant, they must be interpreted as covering every situation in which the provider concerned becomes aware, in one way or another, of such facts or circumstances".⁴⁷ This broad definition of knowledge places a considerable responsibility on internet service providers because, as McCarthy states, "it fixes a lower knowledge threshold at which they must react".⁴⁸ However, what constitutes "actual knowledge" in practice is disputed. In a 2010 public consultation on eCommerce and the implementation of the eCommerce Directive,⁴⁹ rights holders claimed that "even a general awareness of the possible existence of illegal content should be sufficient to constitute actual knowledge"⁵⁰ while internet intermediaries felt that "notification in itself was insufficient to constitute 'actual knowledge' because notices do not necessarily possess the level of detailed information required to identify and locate an infringement"⁵¹ and that a court judgment or a notice from an administrative authority should be required for an intermediary to have 'actual knowledge'.
- 1.36 Thus, social media sites will generally only remove content once they are made aware of it, and unless the content is clearly illegal in nature such as child pornography or hate speech, or otherwise clearly violates their content and conduct policies, such sites can be reluctant to comply with user requests to remove content. However, the European Commission has indicated in its May 2015 Communication *A Digital Single Market Strategy for Europe* that the intermediary liability regime provided for in the eCommerce Directive may be reviewed, as "[r]ecent events have added to the public debate on whether to enhance the overall level of protection from illegal material on the internet".⁵² These recent events may include the decision of the CJEU in the *Google Spain*⁵³ case (the "right to be forgotten" case) and the European Court of Human Rights decision in *Delfi v Estonia*⁵⁴ (where a strict standard was applied in relation to the measures internet

⁴⁵ C-324/09, *L'Oréal SA and Others v eBay International AG and Others* [2011] OJ C269.

⁴⁶ *Ibid* at paragraph 120.

⁴⁷ *Ibid* at paragraph 121.

⁴⁸ McCarthy, "Is The Writing on the Wall for Online Service Providers? Liability For Hosting Defamatory User-Generated Content Under European and Irish Law" (2015) *Hibernian L.J.* 16 at 20.

⁴⁹ European Commission, *Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce* (2000/31/EC).

⁵⁰ *Ibid* at 10.

⁵¹ European Commission, *Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce* (2000/31/EC) at 10.

⁵² Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions "A Digital Single Market Strategy for Europe" (May 2015) at paragraph 3.3.2.

⁵³ *Google Spain SL and Google Inc v Agencia Espanola de Protection de Datos*, Case C-131/12, 13 May 2014.

⁵⁴ *Delfi v Estonia*, application no. 64659/09 (16 June 2015). However, in a more recent case, *Magyar Tartalomsgéltatók Egyesülete (MTE) and Index.hu Zrt v Hungary*, app. no. 22947/13 (2 February 2016), a violation of article 10 was found where an online news portal was held liable by domestic

intermediaries are required to take in response to illegal content). Thus, the European Commission stated that the need for “new measures to tackle illegal content on the Internet” will be examined including “whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems- a duty of care”.⁵⁵

- 1.37 The European Commission addressed this issue again in its May 2016 Communication on *Online Platforms and the Digital Single Market*.⁵⁶ In this Communication, the European Commission stated that it will maintain the existing intermediary liability regime but that further guidance may be required on its provisions if more effective self-regulation by intermediaries is to be encouraged. The EU Commission referred to a public consultation on online platforms that it organised, where a number of online platforms raised the concern that if they were to introduce voluntary measures to target harmful content then they may no longer be able to benefit from the liability exemptions.⁵⁷ Thus, the EU Commission considered that greater clarity on the liability exemptions under the Directive would enable platforms to take more effective self-regulatory measures. The EU Commission also felt that there is a need to monitor existing procedures on notice and takedown to ensure the coherence and efficiency of the liability regime.⁵⁸ However, before any further action would be taken on this front, the EU Commission stated that it would assess the results of other reforms including the updated audio-visual and copyright frameworks and other on-going self-regulatory and co-regulatory initiatives including the EU internet forum.⁵⁹ Thus, while the EU Commission appears to be committed to maintaining the existing liability regime, it nevertheless recognises that further guidance on its provisions may be required if intermediaries are to be encouraged to take a more pro-active stance on harmful content.
- 1.38 In addition, while social media sites have traditionally taken a “hands-off” approach to harmful content posted on their platforms, this approach has changed in recent years.⁶⁰ In 2015, several sites banned revenge porn from their sites including Facebook, Twitter, Reddit and Google.⁶¹ A number of social media sites have also changed their policies on

courts for user comments. *Delfi* was distinguished on the grounds that the present case did not involve hate speech while *Delfi* did. These two decisions are discussed at paragraph 1.57ff, below.

⁵⁵ Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions *A Digital Single Market Strategy for Europe* (May 2015) at paragraph 3.3.2.

⁵⁶ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe* (May 2016).

⁵⁷ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe* (May 2016), page 9; European Commission, *Synopsis Report on the Public Consultation on the Regulatory Environment for Platforms, Online Intermediaries and the Collaborative Economy* (September 2015).

⁵⁸ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *Online Platforms and the Digital Single Market Opportunities and Challenges for Europe* (May 2016), page 9.

⁵⁹ *Ibid.*

⁶⁰ The content and conduct policies of social media companies are discussed further in Chapter 3, paragraphs 3.04-3.13.

⁶¹ See “Why did it take so long to ban revenge porn?” *Fusion* 29 June 2015 available at <http://fusion.net/story/157734/revenge-porn-bans-were-long-time-coming/>.

harassment and abusive content, including Twitter, which announced new tools to allow users to more easily flag and report abuse as well as unveiling, in April 2015, a new filter which allows users from seeing abusive messages.⁶² Sites such as Facebook and Instagram also updated their Community Standards pages in 2015, setting out in greater detail the type of content that is not permitted on their sites.⁶³

(2) Freedom of Expression and Privacy

- 1.39 Thus, there are three primary privacy concerns connected to social media sites. Firstly, social media sites are very powerful platforms because they have a huge volume of users, many of whom use their services daily and on multiple occasions, something which the growth in use of smartphones has particularly added to. Use of social media has therefore become a central feature of modern society, particularly for young people, but increasingly for other age demographics as well. This high usage means that content published on such sites has the capacity to reach very large audiences.
- 1.40 Secondly, social media sites have affected norms relating to privacy. Although privacy is not “dead”, a large section of society has nevertheless become comfortable with sharing content with a broad group of social connections some of whom are only loosely connected to the user. However, many users do not appreciate the extent of the audience to which their content could be accessible to as well as failing to understand that once such content is posted it becomes for all practical purposes permanent.
- 1.41 The permanence of digital and online content is connected to the final privacy concern, which is that while many social media sites have improved their policies on harassment and other harmful content, their traditional approach has been a hands-off one, marked by a reluctance to remove content. This reluctance stems from a number of sources, concerns about not restricting freedom of expression, an inability to respond to all requests for removal given the volume of users and the immunity such sites enjoy under the terms of the eCommerce Directive. Although some of the leading social media sites have taken positive steps to update their policies on abusive content, it remains to be seen how effectively such policies will be implemented.
- 1.42 Robust responses are therefore needed to assist individuals who may suffer harassment and other privacy interferences while online, as social media sites, potentially the most significant locations for such violations, are unable to provide the level of protection for privacy that users require. Yet, any solutions proposed need to strike the appropriate balance and not interfere unjustifiably with freedom of expression. Before discussing how this balance can be struck, it is necessary to examine the right to freedom of expression and the right to privacy in greater detail.

⁶² See “The Top Social Media Platforms’ Efforts To Control Cyber-Harassment” *Socially Aware* 31 August 2015 available at <http://www.sociallyawareblog.com/2015/08/31/the-top-social-media-platforms-efforts-to-control-cyber-harassment/>.

⁶³ *Ibid.*

(a) The Right to Freedom of Expression

- 1.43 The right to freedom of expression is considered “the primary right in a democracy”⁶⁴ and the basis for many other fundamental freedoms. The importance of the right has been eloquently expressed by the German Constitutional Court:

“The basic right to freedom of opinion is the most immediate expression of the human personality in society and, as such, is one of the noblest of human rights... It is absolutely basic to a liberal-democratic order because it alone makes possible the constant intellectual exchange and the contest among opinions that form the lifeblood of such an order; it is the matrix, the indispensable condition of nearly every other form of freedom.”⁶⁵

- 1.44 The importance of the right to freedom of expression is reflected in the fact that it enjoys protection in all of the key human rights instruments including article 19 of the International Covenant on Civil and Political Rights and article 10 of the European Convention on Human Rights (ECHR). Freedom of expression is also protected in most domestic constitutions, with the first amendment of the US Constitution offering a particularly strong guarantee of protection for the right.⁶⁶

- 1.45 In Ireland, the right to freedom of expression is contained in article 40.6.1.i of the Constitution which provides:

“The State guarantees liberty for the exercise of the following rights, subject to public order and morality: –

i The right of the citizens to express freely their convictions and opinions.

The education of public opinion being, however, a matter of such grave import to the common good, the State shall endeavour to ensure that organs of public opinion, such as the radio, the press, the cinema, while preserving their rightful liberty of expression, including criticism of Government policy, shall not be used to undermine public order or morality or the authority of the State.

The publication or utterance of blasphemous, seditious, or indecent matter is an offence which shall be punishable in accordance with law.”

- 1.46 In contrast to the wording of other freedom of expression guarantees, Article 40.6.1.i describes the right in particularly qualified terms. Rather than setting the right out clearly before outlining the necessary qualifications (that the right be subject to public order and morality), as Article 10 of the European Convention on Human Rights (ECHR) does,⁶⁷

⁶⁴ See Daly, “Strengthening Irish Democracy: A Proposal to Restore Free Speech to Article 40.6.1°(i) of the Constitution” (2009) 31(1) DULJ 228, 228, referring to the judgment of Lord Steyn in *R v Secretary of State for the Home Department, ex p Simms* [2000] 2 AC 115 at 126.

⁶⁵ *Luth case*, 7 Berf GE (1958), quoted in *Report of the Constitutional Review Group* (Dublin, Stationary Office, 1996) at 268.

⁶⁶ The First Amendment to the US Constitution provides:

“Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.”

⁶⁷ Article 10 (Freedom of Expression) of the European Convention on Human Rights provides: “1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

Article 40.6.1.i qualifies the right from the outset and thus appears to offer much weaker protection. This view has been expressed by a number of groups who have reviewed the Article including the Constitutional Review Group who referred to the Article as “weak and heavily circumscribed”.⁶⁸ Similarly, the Oireachtas Joint Committee on the Constitution in its 2008 Report described the wording of Article 40.6.1.i as “unsatisfactory” as it is drafted “in such a way that the limitations on free speech are accorded undue prominence”.⁶⁹ Both of these groups recommended that the Article be amended with wording adopted similar to Article 10 ECHR.

- 1.47 It has only been in relatively recent years that cases involving Article 40.6.1.i have come before the courts. This historical lack of judicial development of Article 40.6.1.i has further marginalised the right to freedom of expression compared to other fundamental rights protected by the Constitution. Indeed, Daly argues that the “central obstacle to adequate free speech protection [in Ireland] has been a lack of judicial commitment to free speech”.⁷⁰ This conclusion is based on his assessment of the case law generated by our courts on freedom of expression which the author considers to be “not only weak but highly inconsistent”.⁷¹ A striking feature of this case law is that for the first 45 years of its existence, Article 40.6.1.i was not litigated.
- 1.48 One of the first cases involving Article 40.6.1.i was *The State (Lynch) v Cooney* in 1982,⁷² which concerned an order made under section 31 of the *Broadcasting Act 1961* banning party political broadcasts by Sinn Féin. Yet, the Supreme Court did not consider the Article in great detail in this case despite the fact that this was the first opportunity for them to do so. Article 40.6.1.i was further undermined by *Attorney General v Paperlink Ltd*⁷³ in 1983 which recognised a separate unenumerated right to communicate under Article 40.3.1. Costello J held that Article 40.6.1.i was confined to protection of convictions and opinions while the right to communicate applied to the communication of information. Thus, the right to freedom of expression was “unnecessarily partitioned”⁷⁴ and considerable inconsistency is apparent in subsequent free speech case law with some cases maintaining the separation between the right to express opinions and the right to communicate information and other cases seeking to re-assimilate the right to communicate within the borders of Article 40.6.1.i. More recent cases have tended to amalgamate the two elements of freedom of expression, in particular *Irish Times Ltd. v*

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

⁶⁸ *Report of the Constitutional Review Group* (Dublin, Stationary Office, 1996) at 268.

⁶⁹ *Joint Committee on the Constitution First Report: Article 40.6.1.i- Freedom of Expression* (Government Publications, 2008) at 75.

⁷⁰ Daly, “Strengthening Irish Democracy: A Proposal to Restore Free Speech to Article 40.6.1°(I) of the Constitution” (2009) 31(1) DULJ 228, 229.

⁷¹ *Ibid.*

⁷² [1982] 1IR 337.

⁷³ [1984] ILRM 373.

⁷⁴ Daly, “Strengthening Irish Democracy: A Proposal to Restore Free Speech to Article 40.6.1°(I) of the Constitution” (2009) 31(1) DULJ 228, 244.

Ireland,⁷⁵ where the Supreme Court held that Article 40.6.1.i applied to the communication of information as well as opinions. However, as *Paperlink* has not yet been overruled, an element of confusion surrounding the relationship between the two rights remains.

- 1.49 Over the last two decades, there has been an increase in litigation on freedom of expression in Ireland. However, a number of commentators have noted that many of these decisions refer more extensively to Article 10 ECHR rather than Article 40.6.1.i.⁷⁶ The cases of *Mahon v Post Publications Ltd.*⁷⁷ and *Mahon v Keena*⁷⁸ particularly exemplify this new approach. In fact, the Supreme Court decision in *Mahon v Keena* was decided exclusively on the basis of Article 10 with only a “single, fleeting mention”⁷⁹ made to Article 40.6.1.i. This approach can be explained by the incorporation of the ECHR into Irish law by the *European Convention on Human Rights Act 2003*, as well as the superior clarity of Article 10 compared to Article 40.6.1.i. The body of jurisprudence from the European Court of Human Rights has also been a valuable resource for the domestic courts to draw on, as traditionally the European Court has defended the right to freedom of expression forcefully. However, as discussed below, there has been a move by the Court in more recent times towards greater protection for the right to privacy, contained in Article 8 of the Convention.

(b) The Right to Privacy

- 1.50 Privacy is generally viewed as a multi-faceted right containing a number of related elements, with Henchy J describing the right in *Norris v Attorney General* as “a complex of rights, varying in nature, purpose and range, each necessarily a facet of the citizen’s core of individuality within the constitutional order” and that the aspects of the right to privacy would all appear to:

“fall within a secluded area of activity or non-activity which may be claimed as necessary for the expression of an individual personality, for purposes not always necessarily moral or commendable, but meriting recognition in circumstances which do not endanger considerations such as State security, public order or morality, or other essential components of the common good.”⁸⁰

- 1.51 Thus, the core of the right to privacy is frequently acknowledged to be the concept of intimacy, which includes certain details, activities, ideas or emotions that people generally do not want to share with others, except perhaps close family or friends, and includes the home and family life, correspondence and sexual relations.⁸¹ However, privacy also has other elements including autonomy and identity, which may be of particular relevance to

⁷⁵ [1998] 4 IR 343.

⁷⁶ See, in particular, Daly, *Strengthening Irish Democracy: A Proposal to Restore Free Speech to Article 40.6.1°(I) of the Constitution* (2009) 31(1) DULJ 228, 251-254; Delaney and Carolan, *The Right to Privacy* (Thomson Round Hall, 2008) at 168-169, where Delaney and Carolan state: “where freedom of expression is concerned, the courts seem to refer increasingly to the provisions of Art. 10 of the Convention and to conduct a balancing exercise based on the principles established in the case law of the European Court of Human Rights.”

⁷⁷ [2007] 2 ILRM 1.

⁷⁸ [2007] IEHC 348.

⁷⁹ See Daly, “Strengthening Irish Democracy: A Proposal to Restore Free Speech to Article 40.6.1°(I) of the Constitution” (2009) 31(1) DULJ 228, 251.

⁸⁰ [1984] IR 36 at 71.

⁸¹ McGonagle *Media Law* 2nd ed (Thomson Round Hall, 2003) at 156.

the internet context.⁸² Autonomy refers to the idea of keeping control of one's destiny, whilst identity relates to allowing a person to develop his/her own potential as an individual.⁸³

- 1.52 Privacy is recognised in the Constitution as one of the unenumerated rights stemming from Article 40.3.1. Although a right to marital privacy was recognised in *McGee v Attorney General*,⁸⁴ the general right to privacy did not receive recognition until *Norris v Attorney General*,⁸⁵ where it was unsuccessfully invoked. The first successful invocation of the right came in *Kennedy v Ireland*,⁸⁶ where the plaintiffs, who were journalists, complained that the tapping of their phones amounted to an infringement of their privacy rights. In *Kennedy*, the importance of the right to privacy within the Constitutional framework was firmly established, with Hamilton P describing privacy as "one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State".⁸⁷ However, as is the case with other constitutional rights, privacy is not an unqualified right and can be restricted by the constitutional rights of others as well as the requirements of the common good and public order and morality. Hamilton P also connected the right to privacy to the concepts of dignity and liberty and emphasised its importance in a democratic state:

"The nature of the right to privacy must be such as to ensure the dignity and freedom of an individual in the type of society envisaged by the Constitution, namely, a sovereign, independent and democratic society. The dignity and freedom of an individual in a democratic society cannot be ensured if his communications of a private nature, be they written or telephonic, are deliberately, consciously and unjustifiably intruded upon and interfered with."⁸⁸

- 1.53 In contrast to the right to freedom of expression which, as discussed above, remained dormant until the last couple of decades, the right to privacy has been litigated before the courts on numerous occasions since its recognition in *Kennedy* and stands as one of the most prominent unenumerated rights. The right to privacy also enjoys significant protection in international human rights instruments, including under Article 17 of the International Covenant on Civil and Political Rights and Article 8 of the ECHR.

(c) *The European Court of Human Rights: Balancing the Right to Privacy and the Right to Freedom of Expression*

- 1.54 The European Court of Human Rights (ECtHR) has a significant body of case law concerning the challenge of balancing the Article 8 right to private and family life against the right to freedom of expression in Article 10, in contrast to the Irish courts which have rarely considered this issue.

⁸² *Ibid.*

⁸³ *Ibid.*

⁸⁴ [1974] IR 284.

⁸⁵ [1984] IR 36.

⁸⁶ [1987] IR 587.

⁸⁷ *Ibid* at 593.

⁸⁸ *Ibid.*

- 1.55 Traditionally, the ECtHR robustly defended the right to freedom of expression, with the Court stating in *Handyside v United Kingdom* that “freedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and each individual’s self-fulfilment”.⁸⁹ The Court also made clear in this case that Article 10 extends not only to “‘information’ or ‘ideas’ that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population.”⁹⁰
- 1.56 However, more recent decisions by the ECtHR have taken a more circumscribed approach to freedom of expression in favour of upholding the right to privacy. This shift is exemplified by the Court’s decision in *Von Hannover v Germany*⁹¹ where the Court upheld the applicant’s claim that failure to provide a remedy for photographs taken in a public place without her consent constituted a breach of Article 8. The Court held that when balancing the right to privacy against freedom of expression the “decisive factor” lies “in the contribution that the published articles and photos make to a debate of general interest,” and no such contribution was made in this case as the relevant photos referred exclusively to the applicant’s private life.⁹² The trend towards greater privacy protection is also visible from the Grand Chamber decision in *Delfi v Estonia*⁹³ which is particularly notable because it relates to online freedom of expression.

(i) *Delfi v Estonia*

- 1.57 In *Delfi*, an online news portal was held liable for user generated comments on one of their articles, entitled “SLK Destroyed Planned Ice Road”.⁹⁴ Delfi had argued before the Estonian Courts that it was not a publisher of the comments, which were “manifestly unlawful”⁹⁵ in nature, and so should be able to avail of the hosting immunity granted under Article 14 of the eCommerce Directive. However, the Estonian Supreme Court held that Delfi was a publisher and therefore liable. The case before the ECtHR thus concerned whether the effect of the decision to recognise Delfi as a publisher was compatible with Article 10 of the Convention.
- 1.58 The ECtHR held that restriction on freedom of expression in this case (about which the parties were not in dispute) was prescribed by law and pursued the legitimate aim of protecting the reputation and rights of others. The central aspect of the Court’s analysis thus focused on the proportionality requirement, with the Court identifying four factors as relevant for its analysis: (a) the context of the comments; (b) the liability of the actual authors of the comments as an alternative to Delfi’s liability; (c) the measures applied by Delfi in order to prevent or remove defamatory comments and (d) the consequences of the domestic proceedings for Delfi.⁹⁶

⁸⁹ *Handyside v United Kingdom* (1979-1980) 1 EHRR 737 at paragraph 49.

⁹⁰ *Ibid.*

⁹¹ *Von Hannover v Germany* [2004] EMLR 379.

⁹² *Ibid* at paragraph 76.

⁹³ *Delfi v Estonia*, application no. 64659/09 (16 June 2015).

⁹⁴ SLK are a public limited company that provides a public ferry transport service. The article attracted 185 comments, 20 of which contained personal threats and offensive language directed against L, SLK’s sole or majority shareholder and member of the company’s supervisory board. See *Delfi v Estonia*, application no. 64659/09 (16 June 2015) at paragraphs 16-19.

⁹⁵ *Ibid* at paragraph 116.

⁹⁶ *Ibid* at paragraph 142.

- 1.59 In examining the context of the comments, the ECtHR attached significant weight to the nature of the Delfi site- that it is very large, professionally managed and run on a commercial basis which sought to attract a large number of comments (as the number of visits to the site depended on the number of comments and the more visits, the more revenue from advertising generated). The Court also noted that Delfi exercised a substantial degree of control over the comments, as once comments were posted, the authors could not edit or delete them. The Court therefore felt that that Delfi's involvement in making the comments public "went beyond that of a passive, purely technical service provider".⁹⁷ In considering the liability of the authors of the comments, the Court noted that while procedures do exist in Estonia to trace anonymous online authors, the Estonian Government had provided evidence that such procedures were unreliable, and Delfi also had not put in place procedures to trace authors.
- 1.60 The measures taken by Delfi to remove and prevent defamatory comments were also examined. These measures included a disclaimer on the site stating that Delfi was not responsible for comments posted, an automatic filtering system which deleted comments based on the use of certain words, a notice and take down procedure which could be initiated by users and a system whereby administrators could remove comments on their own initiative. The Court was critical of the failure of the automatic filtering system to remove some of the comments considering that many of them were clearly harmful and some contained hate speech.⁹⁸ More controversially, the Court criticised the notice and take down system despite the fact that the content was removed without delay on the same day that Delfi was notified by the victim. The Court stated:
- "the rights and interests of others and of society as a whole may entitle Contracting States to impose liability on Internet news portals, without contravening Article 10 of the Convention, if they fail to take measures to remove clearly unlawful comments without delay, *even without notice* from the alleged victim or from third parties".⁹⁹
- This places a considerable burden on internet intermediaries like Delfi that provide content but also allow user generated comments, as it requires them to monitor their sites to ensure that "clearly unlawful comments" are removed without delay.
- 1.61 Finally, the Court held that the effect of the proceedings on Delfi were not particularly onerous as they had only been fined €320 and the site had not declined in popularity since the proceedings were commenced. Thus, based on analysis of each of the four factors, the Court found no violation of Article 10.
- 1.62 *Delfi* was the first judgment of the ECtHR dealing with online media liability for user generated comments on a news website or media platform and so it is an important contribution to the Court's jurisprudence on online freedom of expression. However, in deciding that the Estonian courts were correct to hold Delfi liable for user generated comments, the ECtHR adopted a restrictive approach to freedom of expression on the internet which may have considerable implications for news websites and other media platforms which provide content and allow user comments. Although the Court attempted to confine its decision to the facts before it as much as possible and stressed that the

⁹⁷ *Ibid* at paragraph 146.

⁹⁸ *Ibid* at paragraph 156.

⁹⁹ *Ibid* at paragraph 159 (emphasis added).

decision does not apply to internet forums such as social media platforms, bulletin boards and blogs, but rather, only relates to large professionally managed online news portals run on a commercial basis which publish articles of their own and allow users to comment on them,¹⁰⁰ the case nevertheless has significant implications for freedom of expression online. According to Article 19, an organisation dedicated to defending freedom of expression and a third party intervener in the case, the decision may lead to sites applying an overly restrictive standard in relation to user comments or even encourage sites not to include a comments section in order to protect themselves from any potential liability.¹⁰¹

- 1.63 *Delfi* also creates “considerable tension” with the EU system on intermediary liability governed by the eCommerce Directive.¹⁰² As McCarthy notes, the case “falls foul” of the prohibition on general monitoring requirements contained in Article 15 of the eCommerce Directive as “[b]y requiring Delfi to detect defamatory comments *ex ante*, the ECHR imposed a monitoring duty of a general nature.”¹⁰³ Most significantly, the Court failed to appreciate the significance of the hosting immunity provisions and “the role of internet intermediaries as the gateway to the exercise of free expression.”¹⁰⁴ Thus by imposing greater obligations on internet news portals, the Court is forcing this type of internet intermediary to adopt a more conservative approach to user comments which negatively affects individual rights and may have implications for the open nature of the internet as a whole. However, as noted above,¹⁰⁵ the European Commission has indicated that the eCommerce Directive may undergo review with a view to possibly imposing greater responsibility on intermediaries for removing content. Thus, this “tension” between the two systems may be reduced in the future.
- 1.64 *Delfi* also further highlights the contrast between European and US approaches to freedom of speech. As *Delfi* illustrates, the trend in Europe appears to be a move away from strong freedom of expression guarantees towards a strengthened protection for the right to privacy. However, this is in contrast to the position in the US, where freedom of speech has traditionally enjoyed significant protection under the First Amendment. The First Amendment provides that “Congress shall make no law...abridging the freedom of speech” and this has been interpreted by the US Supreme Court as embodying a commitment to the principle that public discourse “should be uninhibited, robust and wide-open and that it may include vehement, caustic, and sometimes unpleasantly sharp speech”.¹⁰⁶ Thus, in general, free speech in the US is protected unless it is “likely to produce a clear and present danger of substantive evil”.¹⁰⁷ This standard also applies to

¹⁰⁰ *Ibid* at paragraph 117.

¹⁰¹ See European Court strikes serious blow to free speech online” *Article 19* 14 October 2013 available at <https://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online>

¹⁰² McCarthy “Is The Writing on the Wall for Online Service Providers? Liability For Hosting Defamatory User-Generated Content Under European and Irish Law” (2015) *Hibernian L.J.* 16 at 41.

¹⁰³ *Ibid* at 42.

¹⁰⁴ European Court strikes serious blow to free speech online” *Article 19* 14 October 2013 available at <https://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online>

¹⁰⁵ See paragraphs 1.36-1.37 above.

¹⁰⁶ *New York Times v Sullivan*, 376 US 254, 270 (1964).

¹⁰⁷ *Terminiello v Chicago*, 337 US 1, 3 (1949).

the internet as is illustrated by the case of *Yahoo! Inc. v LICRA*¹⁰⁸ which involved a dispute relating to the sale of Nazi paraphernalia on the US based Yahoo!.com where a link to this site was also offered on the French Yahoo! site. In France, as in many other European states, allowing Nazi paraphernalia for sale is a criminal offence and enjoys no protection from freedom of expression guarantees. However, in the US this activity, while offensive, nevertheless benefits from First Amendment protection. Thus, a US Court found that an order by a French Court for Yahoo! to take all necessary measures to make access to the link impossible within France violated the First Amendment and could not be enforced in the US.¹⁰⁹

- 1.65 Considering the extent to which Irish courts have relied on the jurisprudence generated by Article 10, *Delfi* is likely to have an impact on protection for freedom of expression in this jurisdiction, particularly in the context of internet communications. However, the ECtHR appears to have taken a step back from *Delfi* in a more recent case *Magyar Tartalomszolgáltatók Egyesülete (MTE) and Index.hu Zrt (Index) v Hungary*.¹¹⁰

(ii) ***MTE and Index v Hungary***

- 1.66 *Magyar Tartalomszolgáltatók Egyesülete (MTE) and Index.hu Zrt (Index) v Hungary* was the first post-*Delfi* case to consider the liability of online intermediaries. It also involved the issue of user comments, but in contrast to *Delfi*, a violation of Article 10 was found. The Court distinguished *Delfi* on two grounds in particular, firstly on the basis of the nature of the comments, stating that while the comments in the present case were offensive they did not amount to hate speech as in *Delfi*, and secondly on the basis of the economic interests of the intermediaries in both cases, with the Court noting that while the second applicant did have significant economic interests (as the applicant had in *Delfi*) the first applicant operated on a non-profit basis as it is the self-regulatory body of internet content providers in Hungary.¹¹¹
- 1.67 The Court then applied the criteria that it had identified in *Delfi* as relevant for determining whether the interference with Article 10 is justified and the applicants could be held liable for the comments, that is, the context of the comments, the measures applied by the applicants in order to prevent or remove defamatory comments, the liability of the actual authors of the comments as an alternative to the intermediary's liability and the consequences of the domestic proceedings for the applicants.¹¹² Of particular note in this analysis, was the Court's comments on the consequences of the domestic proceedings for the applicants, where it noted that while the applicants had only been required to pay a small sum in court fees and no damages, "the decisive question" in terms of the consequences for them was:

"the manner in which Internet portals such as theirs can be held liable for third-party comments. Such liability may have foreseeable negative consequences on the comment environment of an Internet portal, for example by impelling it to close the commenting

¹⁰⁸ *Yahoo! Inc v LICRA* 169 F Supp 2d. 1181 (N.D. Cal. 2001).

¹⁰⁹ 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).

¹¹⁰ *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, app. no. 22947/13 (2 February 2016).

¹¹¹ *Ibid*, paragraph 64.

¹¹² *Ibid*, paragraph 69.

space altogether. For the Court, these consequences may have, directly or indirectly, a chilling effect on the freedom of expression on the Internet.”¹¹³

This statement appears to highlight a great difference in the approach of the Court in this case compared to that taken in *Delfi*, where the effect on freedom of expression of holding internet intermediaries liable for comments was not considered strongly at all. Although the Court again attempted to distinguish *Delfi* by adding to the above that this could be “particularly detrimental for a non-commercial website such as the first applicant”,¹¹⁴ the second applicant is a commercial website and the result also applies to them.

- 1.68 The Court also offered greater support to notice and takedown in this case than in *Delfi* by noting that it could “function in many cases as an appropriate tool for balancing the rights and interests of all those involved”¹¹⁵ and that it could have been used by the company to protect its interests (the company had not sought removal of the comments from the applicants, instead it went directly to the courts). However, the Court did state, as held in *Delfi*, that where hate speech is involved then liability could be imposed on the intermediary for failure to remove the content without delay even without notice.¹¹⁶ It is also clear, from Judge Kuris’ concurring opinion, that the Court recognised that its decision in *MTE and Index* could be interpreted as a “step back from *Delfi*”,¹¹⁷ yet Judge Kuris disputes this noting the different facts in *Delfi* (the presence of hate speech) and instead states that *MTE* is “merely further evidence that the balance to be achieved in cases of this type is a very subtle one”.¹¹⁸
- 1.69 Thus, *MTE* suggests that rather than signalling a general approach of the ECtHR to the issue of liability for online intermediaries, *Delfi* may be confined to its particular facts with the decisive feature in the case being the presence of hate speech. However, it is clear that cases involving this issue are fact-dependent and that uncertainty regarding the position of the ECtHR on liability of online intermediaries will continue. Nevertheless, commentators have welcomed the decision in *MTE* viewing it as “a step in the right direction”¹¹⁹ after *Delfi* and as a “more nuanced decision that fits better with existing practice and law”.¹²⁰

(d) Achieving Balance

- 1.70 Thus, balancing the right to freedom of expression and the right to privacy is a challenging task, particularly in the digital and online context. Proposing heavy handed law based measures intended to provide a remedy for victims of harmful digital communications has the potential to interfere with freedom of expression unjustifiably, and impact on the open

¹¹³ *Ibid*, paragraph 86.

¹¹⁴ *Ibid*.

¹¹⁵ *Ibid*, paragraph 91.

¹¹⁶ *Ibid*.

¹¹⁷ *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, app. no. 22947/13 (2 February 2016), Concurring Opinion of Judge Küris, paragraph 4.

¹¹⁸ *Ibid*.

¹¹⁹ “Case Law, Strasbourg: Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary, Intermediary liability (again)” *Inforrm* 7 February 2016 available at <https://inforrm.wordpress.com/2016/02/07/case-law-strasbourg-magyar-tartalomszolgaltatok-egyesulete-and-index-hu-zrt-v-hungary-intermediary-liability-again-jonathan-mccully/>.

¹²⁰ “European Court of Human Rights Revisits Intermediary Liability” *TechnoLlama* 3 February 2016 available at <http://www.technollama.co.uk/european-court-of-human-rights-revisits-intermediary-liability>.

and democratic nature of information sharing online which is the internet's greatest strength. However, as later chapters of the Report illustrate, there are gaps in the law that need to be addressed.

- 1.71 The best approach may be to prioritise less coercive solutions such as policy and education based remedies as well as civil law solutions. However, it is important that criminal laws are in place to deter especially harmful behaviour and ensure that appropriate responses are available for the most serious cases. The next section will consider where the line ought to be drawn in terms of criminalising harmful digital communications.

(3) Proportionality and the Harm Principle

- 1.72 An important general principle that has been applied to internet regulation is that of proportionality, which requires the least intrusive means of regulation. This principle favours minimal criminalisation and a focus on civil law as well as policy and education based measures as the central means of addressing harmful digital communications. In this respect, this Report applies the harm principle to establish a framework to guide reform proposals within this project. This approach is similar to that taken by the Commission in its *Issues Paper on Regulatory Enforcement and Corporate Offences*, where it was emphasised that the criminal law should only be employed as a last resort as "the only justification for interference with a person's liberty is to prevent harm to others" and therefore, "only acts that are 'injurious to others' should attract punishment".¹²¹ Thus, only behaviour that causes serious harm should be criminalised and where possible, other means of controlling and regulating behaviour should be engaged. This principle also helps to satisfy other important goals within this area including attempting to strike a balance between the rights to freedom of expression and privacy (because heavy handed criminal measures risk unjustifiable interference with freedom of expression) and ensuring technology neutrality (because crafting specialised laws designed to deal with internet crimes risks over-criminalisation of online activity compared to offline activity).
- 1.73 The New Zealand Law Commission in its 2013 Briefing Paper *Harmful Digital Communications* outlines a three tier approach to regulating digital communications which favours user empowerment and self-regulation as the preferred methods of regulation, with the law only being employed where these are ineffective.¹²² In this model, the first tier relates to user empowerment and emphasises the importance of educating individuals as to their rights and responsibilities in relation to digital communications as a means of combating harmful behaviour. This idea is often referred to as "digital citizenship" and is viewed by many commentators as essential to ensuring a better online environment.¹²³ The second tier refers to self-regulation by internet intermediaries and typically involves terms of use agreements which most internet users agree to when they

¹²¹ *Issues Paper on Regulatory Enforcement and Corporate Offences* (LRC IP 8-2016) at pages 11-12.

¹²² Law Commission of New Zealand, Ministerial Briefing Paper *Harmful Digital Communications: The adequacy of the current sanctions and remedies* (2013) at paragraph 3.75.

¹²³ See generally, Keats Citron and Norton "Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age" (2011) 91 BUL Rev. 1435.

use the services of internet intermediaries such as Facebook, Google and YouTube.¹²⁴ On occasions where user empowerment and self-regulation may be incapable of safeguarding individuals' rights the final tier, which relates to the law, may have to be employed. Thus, as a general principle, legal solutions should be resorted to only where other responses are inadequate.

1.74 Therefore, a three level hierarchy of responses is recommended to effectively target harmful digital communications:

- **Education:** to create user empowerment and foster safe and positive digital citizenship;
- **Civil law and regulatory oversight:** where education and related responses are ineffective and the law needs to be employed, civil law should be favoured as it is less onerous than the criminal law;
- **Criminal law:** only the most serious harm should be subject to the criminal law.

1.75 This hierarchy approach is particularly important in the context of harmful digital communications because the ease by which individuals can post content online means that much internet communication is spontaneous and impulsive, and thus a vast amount of content is posted every day.

1.76 The ability of the internet to inspire impulsive behaviour is often referred to as "the online disinhibition effect"¹²⁵ which provides that individuals are more likely to "act out" online because of factors such as anonymity, minimisation of authority, invisibility (digital and online communications tend to be text based so the individual does not see the effect of their words on the other person) and the asynchronicity of online communications (people often do not interact with each other in real time).¹²⁶ According to Suler, anonymity is one of the principal factors which creates the online disinhibition effect because it allows people to separate their online selves from their offline selves creating a sense that behaviour which occurs online is not as "real" as that which takes place offline.¹²⁷ Thus, individuals may communicate online in a manner that they otherwise would not in the offline context. Another important consideration in the context of internet communications is the volume of communications which can be made owing to the speed and ease of publication which the internet facilitates.

1.77 A hierarchical approach is also necessary within this area because this type of harmful communication often involves children and young people who require a less coercive response because of their immaturity. The immaturity of young people may exacerbate the online disinhibition effect leading to a greater level of impulsive behaviour among young people compared to adults. These factors mean that it would be impossible, as well as undesirable, for all harmful digital communications to be dealt with by the criminal law or perhaps even the civil law, and that a threshold is therefore required before the law should be engaged.

¹²⁴ Law Commission of New Zealand, Ministerial Briefing Paper *Harmful Digital Communications: The adequacy of the current sanctions and remedies* (2012) at paragraph 3.12.

¹²⁵ The term "online disinhibition effect" was coined by John Suler. See Suler, "The Online Disinhibition Effect" (2004) 7(3) *CyberPsychology & Behaviour* 321.

¹²⁶ *Ibid.*

¹²⁷ *Ibid* at 322.

- 1.78 The Crown Prosecution Service (CPS) for England and Wales issued guidelines on prosecuting cases involving communications sent via social media, which offer useful guidance on the types of communications that ought to be criminalised and those which should not be.¹²⁸ According to the guidelines, the communications which should be prosecuted include those which may constitute credible threats of violence to the person or damage to property, communications which specifically target an individual or individuals and which may constitute harassment or stalking, controlling or coercive behaviour, so-called “revenge pornography” or which may constitute other offences such as blackmail.¹²⁹ Communications which may amount to a breach of a court order should also be prosecuted.¹³⁰ However, communications which are grossly offensive, indecent, obscene or false and which do not fall into the above categories require a “high threshold” and in many cases prosecution will not be in the public interest.¹³¹ This approach takes into account the context in which such communications take place and recognises that without a high threshold, a very large amount of cases could be prosecuted. The CPS notes that “banter, bad jokes and offensive comments are commonplace and often spontaneous” online and that a certain amount of “give and take” is required in this type of environment.¹³² The communication must therefore be more than just offensive, shocking, disturbing, rude or distasteful to warrant prosecution, as this type of comment is protected by the right to freedom of expression as found in Article 10 ECHR.¹³³
- 1.79 When assessing whether the public interest would require a prosecution the prosecutor is also required to consider whether the suspect has “swiftly taken action to remove the communication or expressed genuine remorse” or whether swift action has been taken by others including service providers to remove or block the communication. Whether the communication was intended for a wide audience or that this was an obvious consequence of the communication, and whether the intended audience included the victim, should also be taken into account.¹³⁴ Prosecution may be required however where a particular victim is targeted and there is clear intention to cause distress or anxiety. Whether the offence is repeated is also listed as an important consideration. Thus, the two defendants in the Caroline Criado-Perez case¹³⁵ were prosecuted because their situation satisfied a number of these requirements- both had sent several threatening messages under numerous Twitter accounts and had shown no signs of remorse. The CPS has also stated that the age and maturity of the suspects should be “given significant weight”.¹³⁶ In particular, the guidelines do not view prosecutions of children under 18 as

¹²⁸ Crown Prosecution Service, *Interim Revised CPS Guidelines on Prosecuting Social Media cases* (3 March 2016) available at

http://www.cps.gov.uk/consultations/social_media_consultation_2016.html/.

¹²⁹ *Ibid.*

¹³⁰ *Ibid.*

¹³¹ *Ibid.*

¹³² *Ibid.*

¹³³ *Ibid.*

¹³⁴ *Ibid.*

¹³⁵ This case is discussed further above at footnote 6.

¹³⁶ Crown Prosecution Service, *Interim Revised CPS Guidelines on Prosecuting Social Media cases* (3 March 2016) available at

http://www.cps.gov.uk/consultations/social_media_consultation_2016.html/.

being within the public interest.¹³⁷ Therefore, prosecutions for cyber-bullying amongst children and adolescents are likely to be rare.

- 1.80 Thus, communications which constitute serious threats of violence and those which directly target individuals, including behaviour which amounts to harassment, that is, persistent behaviour which seriously interferes with a person's peace and privacy or causes alarm, distress or harm, should be subject to the criminal law in most cases. However, communications which do not come within these categories require a high threshold before they should be criminalised if freedom of expression is to be safeguarded. Nonetheless, activity designed to reach a large audience and carried out with the intent to cause serious distress or harm by an adult offender, would appear to meet this threshold.

(4) "Harmful communications" and "cyberbullying"

- 1.81 In the wide literature on this area, the terms "bullying" and, in the online and digital environment "cyberbullying", are often used to describe the kind of behaviour at issue in this Report. While there is no single agreed definition of bullying or of cyberbullying,¹³⁸ the well-accepted definitions include the most serious form of harmful communications, such as: the intentional victim-shaming of individuals (overwhelmingly women), so-called "revenge porn"; intimidating and threatening messages, whether directed at private persons or public figures; harassment; stalking; and non-consensual taking and communication of intimate images (so-called "upskirting" and "down blousing"). Bullying and cyberbullying are also often defined to include harmful communications such as hurtful or embarrassing comments as well as non-verbal exclusion from groups ("freezing out").
- 1.82 In the context of this Report, the Commission has, in general, avoided using the term bullying or cyberbullying because of the very wide potential breadth of those terms. This is because (for the principled-based reasons discussed above), it is especially important in the context of proposals to reform the criminal law, as discussed in Chapter 2, that only behaviour which meets a clear threshold of serious harm should involve the imposition of criminal liability. For this reason, the Report uses the term "harmful communications" and, in the context of reform of the criminal law, this concerns communications that are abusive, threatening, offensive, false (untrue), invade another person's privacy with intent to cause serious harm, concern non-consensual communication of intimate images, or involve matters such as harassment or stalking. As noted, these fall within the accepted definitions of bullying and cyberbullying. However, it would not be appropriate or proportional to apply the criminal law to the other forms of behaviour that also fall within accepted definitions of bullying and cyberbullying, that is, hurtful or embarrassing comments or non-verbal exclusion from groups ("freezing out"). In this respect, the Commission considers that such behaviour should be addressed in the context of the

¹³⁷ *Ibid.*

¹³⁸ See, for example, *Cyberbullying Among Young People* (EU Parliament Policy Department for Citizen's Rights and Constitutional Affairs, September 2016). This was a research paper prepared for the EU Parliament's Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee). The research paper contains a helpful overview of legal and policy measures concerning cyberbullying at international level and in EU member states, with a specific focus on young people.

promotion of digital safety as part of the functions of the proposed Digital Safety Commissioner, discussed in Chapter 3, below. These forms of behaviour should not be ignored; rather it is a matter of the appropriate and proportionate manner in which they could suitably be addressed.

(5) Technology Neutrality

- 1.83 A final general principle that needs to be taken into account when considering potential law reform in the area of harmful digital communications is technology neutrality. Technology neutrality has been repeatedly acknowledged as an important guiding principle in ICT (information and communications technology) regulation. The concept was first referred to in EU legislative proposals in 1998,¹³⁹ and a year later it was provided for in the US *Framework for Global Electronic Commerce*.¹⁴⁰ The first EU Directive to refer to the principle was Framework Directive 2002/21, which requires Member States to “take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology”.¹⁴¹ Technology neutrality has since become a cornerstone of EU ICT policy, with references made to the principle in the Better Regulation Directive 2009/140/EC¹⁴² as well as the 2016 General Data Protection Regulation¹⁴³ and the 2016 Directive on Network and Information Security (NIS Directive).¹⁴⁴
- 1.84 Technology neutrality is regularly cited as a desirable goal for legislative and other regulatory proposals aimed at targeting harmful digital communications. However, some commentators have argued that the principle is not well understood and that it is often presented as a goal for ICT regulation without proper examination of what exactly technology neutrality requires.¹⁴⁵ In particular, the two main elements of technology neutrality, firstly that “the fundamental rules should be the same online as offline” and secondly, “legal rules should not favour or discriminate against a particular technology”,

¹³⁹ See Reed, “Taking Sides on Technology Neutrality” (2007) 4(3) SCRIPT-ed 264, at 264.

¹⁴⁰ *Framework for Electronic Commerce* (1997), principle 2 available at <http://clinton4.nara.gov/WH/New/Commerce/read.html>.

¹⁴¹ Directive 2002/21/EC of the European Parliament and the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), recital 18.

¹⁴² Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, recitals 34, 35, 38, 40 and 68.

¹⁴³ Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

¹⁴⁴ Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

¹⁴⁵ See, in particular, Reed, “Taking Sides on Technology Neutrality” (2007) 4(3) SCRIPT-ed 264; Koops “Should ICT Regulation be Technology-Neutral” 77 in Koops, Lips, Prins & Schellekens (eds) *Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, IT & Law Series Vol. 9 (The Hague: TMC Asser Press, 2006) at 77-108 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746.

- are ambiguous and capable of being interpreted in different ways.¹⁴⁶ The first element of technology neutrality, that the same rules apply online as well as offline, does not necessarily mean that identical rules apply in both settings. Instead, Reed argues that the focus should be on achieving equivalence between the two, which may require different rules online and offline but which would be aimed at realising the same effect.¹⁴⁷
- 1.85 In the legislative context, technology neutrality aims to achieve a number of different goals. The purpose of targeting the effects of behaviour rather than the means used to carry it out is to achieve equivalence between online and offline activity.¹⁴⁸ Technology neutrality also aims to promote the development of ICT through its second element, non-discrimination between technologies.¹⁴⁹ However, Koops argues that the most important goal of legislation that aims to be technology neutral is to ensure sustainability.¹⁵⁰ This is because there is a greater risk in relation to laws that target technology that technological change may soon make the law obsolete. This requirement would appear to demand that specific technologies are not referred to in the legislation/regulation, however, this may interfere with another fundamental legal principle: certainty. Thus, Koops emphasises that these two requirements have to be balanced and that legislation should not refer to specific technologies if doing so would reduce sustainability, but only where legal certainty is also provided for.¹⁵¹ Reed therefore suggests that technology specific approaches should not be entirely rejected and that there may be areas of ICT regulation where a technology specific approach might be required if sufficient certainty cannot be guaranteed by a technology neutral approach.¹⁵²
- 1.86 Thus, although technology neutrality does have significant benefits as a legislative approach within the ICT arena, a nuanced understanding of the term is required as well as a willingness to recognise situations where technology neutrality may not be desirable and specificity could prove more beneficial. With respect to harmful digital communications, technology neutrality should be adopted as a starting point. This is because one of the central aims of legislation within this area is to achieve equivalence between the offline and online contexts and currently, the online context, as illustrated in Chapters 2 and 3 of this Report, is not as well regulated as the offline one. However, technology neutrality should not be adopted to the detriment of certainty and in the case of certain behaviour, a technology specific approach might be called for.
- 1.87 The Commission applies these principles and considerations in its discussion of reform of the criminal law in Chapter 2, and in its discussion of the promotion of digital safety and civil law remedies in Chapter 3.

¹⁴⁶ Reed, "Taking Sides on Technology Neutrality" (2007) 4(3) SCRIPT-ed 264, at 266.

¹⁴⁷ *Ibid* at 267.

¹⁴⁸ Koops "Should ICT Regulation be Technology-Neutral" 77 in Koops, Lips, Prins & Schellekens (eds) *Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, IT & Law Series Vol. 9 (The Hague: TMC Asser Press, 2006) at 77-108 available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=918746, at 26.

¹⁴⁹ *Ibid*.

¹⁵⁰ *Ibid*.

¹⁵¹ *Ibid* at 27. Koops suggests that "[l]egislation should abstract away from concrete technologies to the extent that it is sufficiently sustainable and at the same time provides for legal certainty".

¹⁵² Reed, "Taking Sides on Technology Neutrality" (2007) 4(3) SCRIPT-ed 264, at 283-4.

CHAPTER 2 REFORM OF CRIMINAL LAW CONCERNING HARMFUL COMMUNICATIONS

A Introduction

- 2.01 This chapter of the Report discusses reform of the criminal law concerning harmful communications, including harmful digital communications.
- 2.02 The first matter discussed relates to reform of the harassment offence in section 10 of the *Non-Fatal Offences Against the Person Act 1997*. Although this offence already applies to harassment “by any means”, the chapter considers whether a specific reference to harassment by digital or online means is necessary to ensure that this form of harassment is more effectively captured by the offence. The Commission also examines whether harassment by means of indirect communication should be covered by the harassment offence.
- 2.03 The merits of introducing a specific stalking offence are then explored. Although the Commission considered this question previously in its *Report on Aspects of Domestic Violence*,¹ it nevertheless considers that further examination of this issue is required particularly in the context of online and digital stalking.
- 2.04 The chapter then addresses the need for offences designed to target once-off harmful communications. Section 10 of the *Non-Fatal Offences Against the Person Act 1997* is limited to persistent behaviour and thus does not cover a single act that seriously interferes with a person’s peace and privacy or causes him or her alarm, distress or harm. However, once-off activity can have very serious consequences, particularly in cases involving the non-consensual distribution of intimate images (so called “revenge porn”). This chapter therefore discusses the need for offences designed to target this type of activity and other related, but distinct, behaviour, sometimes referred to as “upskirting” and “down-blousing”.
- 2.05 The Commission then considers a number of important procedural issues. These are: protecting the privacy of persons affected by harmful communications; protective measures to deal with prosecutions of persons under 17 years; and time limits for summary prosecutions. The Commission also considers whether offences relating to harmful communications should have extra-territorial effect (important because much online and digital communication involves content held on servers outside the State). The chapter then addresses the penalties that should apply on conviction for offences relating to harmful communications.

¹ Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013).

- 2.06 The chapter ends with an analysis of the extent to which the law on hate crime overlaps with harmful communications.
- 2.07 As discussed below, the existing criminal law already addresses some of the harmful communications at issue in this Report. Not surprisingly, however, some gaps exist that require reform, notably where new forms of communication have been used in harmful ways that could not have been anticipated previously. The Commission has therefore concluded that the existing criminal law, together with the proposals intended to deal with the new forms of harmful communications, could usefully be consolidated into a single piece of legislation. This approach is reflected in Part 2 of the draft *Harmful Communications and Digital Safety Bill* in Appendix A of this Report.

B Reform of the offence of harassment

- 2.08 The first matter considered in this Chapter is whether section 10 of the *Non-Fatal Offences Against the Person Act 1997* fully captures the various forms of harassing behaviour conducted using digital or online means of communication, such as the internet and mobile phones.
- 2.09 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.”
- 2.10 Section 10 derives from a recommendation in the Commission’s 1994 *Report on Non-Fatal Offences Against the Person*² 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].”³
- 2.11 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 up to 7 years on conviction on

² Law Reform Commission *Report on Non-Fatal Offences Against the Person* (LRC 45-1994), paragraph 9.77.

³ 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.

indictment.⁴ As an 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.⁵ This ensures that the victim can gain relief in cases where imprisonment may not be appropriate.⁶ 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.⁷ 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.⁸

- 2.12 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*,⁹ 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.¹⁰ 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 10.¹¹ The Commission also recommended that the term “persistently” be retained rather than replaced with a “course of conduct” requirement as in some other jurisdictions.¹²

⁴ Section 10(6) of the *Non-Fatal Offences Against the Person Act 1997*: see the discussion of penalties at paragraph 2.235 below.

⁵ Section 10(3) of the *Non-Fatal Offences Against the Person Act 1997*.

⁶ Charleton, McDermott and Bolger, *Criminal Law* (Butterworths, 1999), paragraph 8.206.

⁷ Section 10(5) of the *Non-Fatal Offences Against the Person Act 1997*.

⁸ 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*.

⁹ Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013).

¹⁰ *Ibid*, paragraph 2.23.

¹¹ *Ibid*, paragraph 2.88.

¹² *Ibid*, paragraph 2.102.

In *Director of Public Prosecutions (O'Dowd) v Lynch*¹³ 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.

- 2.13 *Lynch* illustrates that persistence requires continuing behaviour and will usually involve more than one incident, but it can include a single incident provided it is prolonged, thereby meeting the test of continuity. However, the interpretation of the persistence requirement made in *Lynch* has yet to be considered by the Supreme Court or applied by the High Court in any subsequent cases.
- 2.14 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."¹⁴ 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."¹⁵ 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".¹⁶ Stalking is best understood as an aggravated form of harassment which is a wider offence that could encompass other behaviour not readily identifiable as stalking.¹⁷ The Commission adopted this view in its *Report on Aspects of Domestic Violence*, concluding that stalking is included as a type of

¹³ [2008] IEHC 183, [2010] 3 IR 434: see the more detailed discussion in Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.22ff.

¹⁴ Law Reform Commission, *Report on Non-Fatal Offences Against the Person* (LRC 45-1994), paragraph 9.77.

¹⁵ 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."

¹⁶ As quoted in MacEwan, "The new stalking offences in English Law: will they provide effective protection from cyberstalking" (2012) *Crim LR* 767, at 768.

¹⁷ Gillespie, "Cyberstalking and the law: a response to Neil MacEwan" (2013) *Crim LR* 38, at 39.

harassment under section 10.¹⁸ Cyber-stalking has been described as involving a relentless pursuit of the victim online often in combination with an offline attack.¹⁹ Just as stalking is commonly characterised as a sub-category of harassment, the Commission suggests that cyber-stalking that meets the test of persistence is best described as a form of cyber-harassment.

(1) Examples of harmful digital communications

2.15 The following are examples of harmful digital 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 media sites. 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.²⁰
- Targeting the victim's computing technology. This type of behaviour arose in the English case *R v Debnath*,²¹ 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*.²²
- Setting up harmful websites or fake profile pages on social media 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 actor Jennifer Lawrence, were posted online after their iCloud accounts had been hacked.²³ This clearly involved hacking but might not come within section 10 of the 1997 Act.

(2) Application of section 10 of the 1997 Act to harassment by digital or online means

2.16 Section 10 of the 1997 Act can be applied to many forms of harmful internet behaviour, including harassment by online or digital means, because section 10(1) provides that harassment may be carried out "*by any means* including by use of telephone" (emphasis

¹⁸ Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.92.

¹⁹ Jameson, "Cyberharassment: Striking a Balance between Free Speech and Privacy" (2008) 17 *Comm Law Conspectus* 231, at 236.

²⁰ 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>.

²¹ [2005] EWCA Crim 3472.

²² The 1991 Act is discussed at paragraph 2.90 below.

²³ "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>.

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” enables other forms of communication such as email, messages sent through a social media site or text messages to 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 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.

- 2.17 The cases outlined below come within section 10 of the 1997 Act because each involved a cyber-attack that continued over a prolonged period. They show that prosecutions have been brought pursuant to section 10 where there has been harassment by digital or online means, 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 digital or online means.²⁴

- 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.²⁵
- 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.²⁶ 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.²⁷

- 2.18 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

²⁴ The Commission noted this in its *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.94.

²⁵ This case is discussed in Shannon *Sixth Report of the Special Rapporteur on Child Protection* (Report Submitted to the Oireachtas, January 2013) at 95.

²⁶ “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>.

²⁷ “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>.

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.²⁸

- 2.19 These examples meet the persistence requirement in section 10 because they involved repeated acts over an extended period. These cases also illustrate that section 10 is capable of capturing many forms of harassment by digital or online means.²⁹

(3) Whether there should be a specific reference to harassment by digital or online means

- 2.20 In accordance with the harm principle, only the most serious behaviour should be subject to the criminal law. Harassment by means of digital or online communication is as serious as offline harassment and arguably, it can even be more harmful because of the particular characteristics of digital communications. Digital communications have the capacity to be instant, numerous, reach large even global audiences, be permanently available and are frequently anonymous in nature. Harassment by digital or online means can also have an inescapable quality as the victim can be targeted anytime and anywhere because of the ubiquity of portable internet connected devices such as smartphones. Thus, the potential for harassment by digital or online means to cause substantial harm is significant and it has being linked to serious psychological harm and even in extreme cases to suicide.
- 2.21 Section 10 of the 1997 Act already covers harassment by digital or online means as it applies to harassment “by any means” and it has been applied in certain online harassment cases as the examples discussed above demonstrate. However harassment by digital or online means is under-reported and under-prosecuted which suggests that this section is not effective in targeting this behaviour.
- 2.22 Studies conducted on cyber-bullying regularly find that individuals are reluctant to report such behaviour.³⁰ 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.³¹ Even where a child tells an adult about cyber-bullying or

²⁸ “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>.

²⁹ 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.

³⁰ 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.

³¹ See O'Higgins Norman “Report on Cyberbullying Research and Related Issues” Conference Paper, 1st National Cyberbullying Conference (1 September 2014) at 2. This Paper also notes that

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 harassment by digital or online means also creates challenges for both adult and child victims, who may believe that reporting the behaviour is futile because the perpetrator cannot be identified.³² 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.

- 2.23 In 2013, a number of representative groups in submissions to the Oireachtas Joint Committee on Transport and Communications believed that there was a need to clarify that existing law applied to harassment by digital or online means.³³

(a) Consultation responses

- 2.24 The majority of consultees were in favour of amending section 10 to include a specific reference to harassment by digital or online means. A number of respondents to the Issues Paper stated that they believed such an amendment could increase reporting of harassment by digital or online means and may deter such behaviour. Respondents also felt that such an amendment would offer clarity and “provide certainty to those tasked with interpreting the section”. It was also noted that such an amendment would emphasise the seriousness of harassment by digital or online means and the law's intolerance to it.
- 2.25 However, some of the consultees who were in support of this amendment also had certain reservations. One consultee emphasised that care must be taken to ensure that such a specific reference would not result in the disproportionate criminalisation of young people. This could be facilitated by providing guidance to law enforcement, which a number of consultees recommended should accompany the proposed amendment.
- 2.26 Consultees also emphasised that care would need to be taken with the wording of the specific reference to harassment by digital or online means. One consultee noted that, as the cases listed in the Issues Paper illustrated, the present section 10 has shown itself to be highly adaptable to a range of scenarios and any attempt to specify the means through which harassment could be carried out is “fraught with the risk that future technological developments will not be covered by any statutory wording”.
- 2.27 The main reason certain consultees did not support amending section 10 to include a specific reference to harassment by digital or online means is because they considered such an amendment unnecessary, as the section already applies to harassment “by any means”. These consultees instead advocated public engagement and education to ensure that the public is aware of the scope of section 10. A consultee also suggested that the

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.”

³² Srivastava and Boey “Online Bullying and Harassment: An Australian Perspective” (2012) 6 *Massaryk U J L & Tech* 299, at 313.

³³ 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.

real problem with section 10 lies not with the wording but with enforcement. This consultee remarked that “[w]e have heard from victims of online harassment who have reported the matter to the Gardaí and been told that there is simply nothing that can be done in respect of online harassment. This is simply not so and we recommend that this be clarified to Gardaí.”

- 2.28 At a 2015 Women’s Aid conference “Digital Abuse of Women: The Challenge of Online and Technology Abuse, Shaming and Stalking in Intimate Partner Relationships”³⁴ speakers highlighted the increasing role of digital and online technology in stalking/harassment cases. Margaret Martin, the Director of Women’s Aid, noted that digital technology had allowed “the volume to be turned up” on stalking/harassment, because such technology operates instantly thus increasing the intensity of the harassment. She also noted that 41% of domestic violence victims helped by Women’s Aid in the UK had been tracked or harassed through an electronic device. Digital technology is therefore a very significant tool for stalking/harassment and this should be reflected in the wording of a reformed harassment offence.

(b) Conclusion

- 2.29 The Commission considers that amending the harassment offence to include a specific reference to harassment by digital or online means would offer important clarification as to the scope of the offence, similar to the specific mention of harassment by telephone which is already included in section 10 of the 1997 Act. This clarification could lead to an increase in reporting of this type of harassment. Expressly identifying harassment by digital or online means in the legislation as a particular form of the wider offence of harassment would also underline society’s recognition of its seriousness and the need to prevent and punish it. However, educational measures aimed at the general public and the Gardaí are also necessary to increase public awareness of the capacity of the harassment offence to be used in cases involving harassment by digital or online means and to offer guidance to the Gardaí as to when the offence is applicable.
- 2.30 The reference in section 10 to “telephone” without any mention of other forms of electronic communication makes the section appear outdated. Thus, including a reference to harassment by digital or online communication would clarify and modernise the wording of the harassment offence. It would also correctly label the conduct that is covered by the offence and ensure that harassment by digital or online means is not a hidden form of harassment as section 10 of the 1997 Act currently suggests.
- 2.31 The Commission thus recommends that section 10 of the *Non-Fatal Offences Against the Person Act 1997* be repealed and replaced with a harassment offence which expressly applies to harassment by all forms of communication including through digital and online communications such as through a social media site or other internet medium. The Commission recommends that this amendment be made by including a definition of “communication” in the legislation which would extend to any form of communication including by letter, telephone (including SMS text message) or digital or online communication such as through a social media site or other internet medium. The

³⁴ Women’s Aid International Conference “Digital Abuse of Women: The Challenge of Online and Technology Abuse, Shaming and Stalking in Intimate Partner Relationships” 25 November 2015, Dublin City Council Civic Offices.

Commission has also concluded that the existing criminal law on harmful communications, together with the reforms proposed in this Report, should be consolidated into a single piece of legislation.

(4) Indirect harassment

- 2.32 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.³⁵
- 2.33 Indirect online harassment involves persistent harmful communications through email, social media sites or other digital or online means to third parties concerning a person but not directly communicated to the person. It would include, for example, situations where a defendant spreads harmful information whether true or false to the person's friends or family. It might also involve repeatedly posting content online to the public at large concerning a person.
- 2.34 There may be a gap in Irish law in relation to indirect harassment, a view that was shared by the then 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."³⁶ Comprehensively criminalising indirect harassment could be done by amending the harassment offence to include harassing communications with "any person" rather than just the target of the harassing behaviour. In the online context, this would clarify that it is a crime to post harassing communications on a publicly available website and to send digital communications to third parties which are harmful to the victim.

In the English case *R v Debnath*,³⁷ the defendant pleaded guilty to 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 online 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, and set up a website claiming that the complainant was gay.

- 2.35 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

³⁵ Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.21.

³⁶ Joint Committee on Transport and Communications *Report on Addressing the growth of Social Media and tackling Cyberbullying* (Government Publications, 2013) at 34.

³⁷ [2005] EWCA Crim 3472.

Debnath. Similarly, harmful messages posted on a private social media page such as on Facebook may also not be covered by section 10 if they do not involve direct communication with the subject.

2.36 Nonetheless, there have been two prosecutions under section 10 for indirect harassment type behaviour:

- 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.³⁸ The man received a four year suspended sentence.
- In 2015, a man pleaded guilty to three counts of harassment under section 10, one of which related to indirect harassment, whereby the accused set up a fake social media profile using a made-up woman's name but using pictures from the actual Facebook page of a woman he knew. These photos were interspersed with the sexual images of a similar looking woman taken from pornographic sites and the fake site, along with sexual communications, was then shared with over 1,000 men through social media. The woman only found about the fake site when a friend contacted her. The man was sentenced to six months imprisonment.³⁹

2.37 These cases suggest that there is a view that section 10 may extend to some situations where a person is exposed 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 online context posting abusive content on publicly accessible websites or social media profiles might amount to online harassment. However, both of these cases involved guilty pleas and so the law in this area has not been properly tested.

2.38 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.⁴⁰ 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.⁴¹ This is because, as defined in the English Act, "course of conduct" requires at

³⁸ 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>.

³⁹ See "Man jailed after falsely linking woman with online pornography" *Irish Times* 6 November 2015 available at <http://www.irishtimes.com/news/ireland/irish-news/man-jailed-after-falsely-linking-woman-with-online-pornography-1.2421444>.

⁴⁰ 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.

⁴¹ Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013) at paragraph 2.101.

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*⁴²).

(a) Indirect victim shaming (“revenge porn”) and section 10 of the 1997 Act

- 2.39 A particular form of indirect 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 referred to as “revenge porn”.⁴³ 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 celebrities illustrates the potential for such behaviour to be carried out on an industrial scale.⁴⁴

In the Canadian case *R v DeSilva*,⁴⁵ 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 voyeurism⁴⁶ for making and distributing the video and harassment in relation to the threats he made to the victim. Although the video was not widely 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.

- 2.40 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.⁴⁷ 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 social media page might possibly be prosecuted successfully under section 10 if the complainant had access to the page.

(b) Consultation responses

- 2.41 The majority of respondents to the Issues Paper were in favour of amending section 10 to provide for indirect harassment. One organisation outlined their experience with indirect harassment, stating that they had seen cases of revenge porn and cases where “graphic and disturbing lies have been spread on the internet about women by their ex-partners,

⁴² [2008] IEHC 183, [2010] 3 IR 434.

⁴³ 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>.

⁴⁴ “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>.

⁴⁵ 2011 ONCJ 133.

⁴⁶ The voyeurism aspect of the case is discussed at paragraph 2.122 below.

⁴⁷ As noted at paragraph 2.18 above, section 10 has been used in cases involving covert filming.

damaging their reputation, self-esteem and possibly their work opportunities.” They noted how difficult it was for such women to take effective action in these circumstances, as “when women report this type of cyber-harassment to the Gardaí they are told there is nothing they can do”. The organisation also suggested that defamation cases are too expensive and unlikely to be pursued by domestic violence victims in particular.

- 2.42 The young people who participated at the Commission’s consultative workshops in April 2106, facilitated by the Department of Children and Youth Affairs, expressed strong views on indirect behaviour. 100% of those participating felt that “revenge porn” should be illegal and 89% felt that the use of fake profiles to target individuals should be illegal.
- 2.43 A representative of the Office of the Director of Public Prosecutions speaking at the Commission’s Seminar in April 2015 indicated that the Office had experienced some challenges in prosecuting harassment cases involving indirect behaviour, such as where a page is set up on a social media site for the purposes of harassing a victim. The Office of the Director of Public Prosecutions thus supported amending section 10 to accommodate indirect harassment.
- 2.44 One consultee emphasised the importance of safeguards if this amendment were to be introduced, including, that there be no public interest element involved in such cases, that there is sufficient evidence that the behaviour was done expressly to intimidate and directed specifically at the person claiming to be a victim. This consultee highlighted the right of freedom of expression and the importance of not allowing such legislation “to stifle publishing of content online”, noting satirical profiles on social media sites as an example of the type of content that should not be captured by indirect harassment.
- 2.45 A number of social media companies who responded to the Issues Paper were not in favour of amending the harassment offence to provide for indirect harassment. One such company outlined a number of reasons for this opposition. Firstly, they suggested that extending the harassment offence to cover indirect harassment “would represent a fundamental change in the law of criminal harassment”. They noted that the offence of harassment has been defined by the Oireachtas and interpreted by the courts as requiring a direct nexus between perpetrator and victim and that amending section 10 to include indirect harassment “represents a significant change to this position”. Another consultee shared this view, emphasising that “any amendment of section 10 should respect the vital distinction between speech about another person and communication made to that person.”
- 2.46 Secondly, the social media company noted that the amendment could have unintended consequences, suggesting that depending on the wording, extending section 10 to cover indirect harassment could result in the criminalisation of gossip or spreading rumours offline and online about an individual and could “lead to a situation where an individual who engages in two or three similar conversations (online or off) finds themselves criminally liable for indirectly harassing the individual who was discussed in each of the conversations.” Although the social media company acknowledged that in practice much of this type of conduct is unlikely to be prosecuted, they nonetheless felt that there would be a high degree of prosecutorial discretion as to when indirect harassment would be charged and this could lead to uncertainty amongst the general public as to whether indirect communications are lawful or not.

- 2.47 However, section 10 requires that the harassing behaviour “seriously interferes with the other’s peace and privacy or causes alarm, distress or harm to the other”. The prosecutorial discretion under the section is therefore not as broad as the social media company claims. It is not sufficient for there simply to be an interference with peace and privacy, the interference must also be serious or cause “alarm, distress or harm” and it is unlikely that behaviour such as gossip or rumour spreading would meet this requirement.
- 2.48 Thirdly, the social media company suggested that criminalising indirect harassment could result in individuals becoming criminally liable for sharing lawful content. They warned that “without careful drafting and proper attention being paid to the need to protect lawful speech, social media comments about lawful matters and settled records of fact could be criminalised.”
- 2.49 Finally, the social media company noted the CPS’ Guidelines on social media communications⁴⁸ and the Scottish Crown Office and Procurator Fiscal Service’s Guidance on Cases Involving Communications sent via Social Media.⁴⁹ Both sets of Guidelines advise that a high degree of care needs to be taken in bringing prosecutions on the basis of online communications that do not breach court orders, contain threats or specifically target an individual in light of the need to safeguard the right to freedom of expression. In particular, the constuttee noted that the CPS Guidelines state that in the context of online misconduct, a harassment charge may be appropriate “where there is more than one incident, or the incident forms part of a course of conduct directed towards an individual.” They argued that this suggests that “the UK has retained the requirement of a nexus between the victim and the offender when bringing harassment cases, and has not adopted the approach of prosecuting in cases of “indirect” harassment”. Yet, this assessment ignores the *Debnath* case, discussed above,⁵⁰ where the defendant pleaded guilty to harassment (under section 2 of the English *Protection from Harassment Act 1997*) mainly conducted through indirect means. The defendant was also subjected to a restraining order under section 5 of the English Act which prohibited her from “contacting directly or *indirectly* the complainant his fiancée and others specified”.⁵¹ This case clearly suggests that indirect communications do come within the scope of the English Act.

(c) *Conclusion*

- 2.50 By expanding the harassment offence to include communications with a third person rather than just the target of the harassment, an important gap in the law of harassment would be filled.
- 2.51 Currently, indirect communications such as posting content on public websites or sending harmful communications to third parties connected to the victim do not appear to be

⁴⁸ Crown Prosecution Service, *Interim Revised CPS Guidelines on Prosecuting Social Media cases* (3 March 2016) available at http://www.cps.gov.uk/consultations/social_media_consultation_2016.html.

⁴⁹ Crown Office & Procurator Fiscal Service, *Guidance on cases involving Communications sent via Social Media* available at http://www.copfs.gov.uk/images/Documents/Prosecution_Policy_Guidance/Book_of_Regulations/Final%20version%2026%2011%2014.pdf.

⁵⁰ See paragraph 2.34 above.

⁵¹ *R v Debnath* [2005] EWCA Crim 3472 at paragraph 3 (emphasis added).

covered by section 10 in most cases. This has been confirmed during the consultative process leading to this Report. Although this Report also proposes an offence designed to deal with indirect victim-shaming behaviour (so-called “revenge porn”), which some consultees have suggested could obviate the need for a reference to indirect harassment, the expansion of the harassment offence to include indirect activity is nonetheless warranted because not all indirect behaviour is related to the victim-shaming behaviour. Moreover, in certain cases that type of behaviour may be part of a pattern of persistent behaviour where charging the perpetrator with harassment would be appropriate.

- 2.52 The Commission also believes that providing for indirect harassment would not constitute a fundamental change to the harassment offence because the direct nexus between the perpetrator and the victim would be retained. This is because while the indirect behaviour may appear to be directed at a third party, the behaviour would still need to be such that it can be proven that it harasses the victim. The behaviour must thus seriously interfere with the victim’s peace and privacy or cause him or her alarm, distress or harm as well as satisfy the requirement that a reasonable person would realise that the harassing acts would seriously interfere with the victim’s peace and privacy or cause the victim alarm, distress or harm. These elements of the proposed amended harassment offence would prevent prosecutions for behaviour such as gossiping or the sharing of lawful content.

2.53 **The Commission recommends that the legislation included in this Report on harmful communications should apply to all forms of communication, whether offline or online, analogue or digital, and therefore should include communication by letter, telephone (including SMS text message), camera, or digital or online communication such as through a social media site or other internet medium. The Commission also recommends that the existing criminal law on harmful communications, together with the reforms proposed in this Report, should be consolidated into a single piece of legislation.**

2.54 **The Commission recommends that section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be repealed, and replaced by an offence of harassment that is modelled on section 10 and that includes two additional provisions: (a) that the harassment offence should expressly apply to harassment by any means of communication, including through digital and online communications; and (b) that it should deal with indirect form of communications, such as setting up fake online social media profiles.**

C Specific Stalking Offence

- 2.55 The amendments to the harassment offence recommended by the Commission above will ensure that harassment by digital or online means is better accommodated than it is presently. However, the Commission also feels that consideration should be given as to whether a specific offence to target stalking, including cyber-stalking, should be introduced.
- 2.56 Although stalking is frequently described as a form of harassment (and as mentioned above, section 10 was described in the Oireachtas debates as expressly intended to deal with stalking⁵²) there is an argument that it is a distinct crime deserving of specific recognition. Ann Moulds, anti-stalking advocate and founder of Action Scotland Against

⁵² See paragraph 2.14.

Stalking, offers a useful description of how stalking is different and more serious than harassment:

“Somebody might harass another person because they are not happy with them or whatever, but that is slightly different from the intimate relationship that stalker has with his victim. There is an emotional relationship between two people, and it is an unequal relationship.”⁵³

- 2.57 The Suzy Lamplugh Trust, which runs the UK National Stalking Helpline, defines stalking as “repeated, unwanted contact that occurs as a result of fixation or obsession and causes the victim(s) to feel distressed or fearful”.⁵⁴ Thus, stalking is often seen as an “aggravated form of harassment”⁵⁵ because it involves an intense obsession or fixation on the part of the perpetrator which creates an unwanted intimacy between the stalker and victim. This type of intense fixation giving rise to a quasi-intimate relationship is not present in all cases of harassment. Thus, this quantifiable difference⁵⁶ between stalking and harassment inspired changes to both Scottish and English law (both discussed below) which were aimed at ensuring that the crime of stalking would be properly identified and more effectively investigated and prosecuted.
- 2.58 The Commission previously considered the question of whether a specific stalking offence was required in its 2013 *Report on Aspects of Domestic Violence*.⁵⁷ In that Report, the Commission concluded that the “offence of harassment is sufficiently broad in scope to encompass behaviour that is colloquially known as ‘stalking’”⁵⁸. In arriving at this conclusion, the Commission took into account the consultations it had with the Director of Public Prosecutions and the Gardaí which indicated that the majority of section 10 prosecutions were for stalking type behaviour,⁵⁹ as well as the experiences of other jurisdictions including England and Wales where the Commission noted that “the addition of a specific stalking offence has created a situation where the offence of harassment and the offence of stalking are made up of the same elements”⁶⁰. The Commission thus felt that introducing a specific stalking offence “would be unnecessarily complicating and would result in a duplication of the criminal law”⁶¹.
- 2.59 However, while the 2013 Report considered the question of whether a specific stalking offence may be required this was not a core element of that Report and thus the issue was dealt with relatively briefly. In particular, the substantial impact of digital technology on harassment and stalking was not examined in detail in the 2013 Report or taken specifically into account by the Commission when it recommended against introducing a stalking offence. Thus, the Commission has decided to consider again whether a specific

⁵³ See Scottish Parliament Justice Committee, *Justice Committee Official Report 23 March 2010*, Criminal Justice and Licensing Scotland Bill, col. 2809, available at <http://archive.scottish.parliament.uk/s3/committees/justice/or-10/ju10-1102.htm#Col2775>.

⁵⁴ *Out of Sight, Out of Mind: An investigation into the response to stalking* (Suzy Lamplugh Trust, 2016) at 6.

⁵⁵ See Independent Parliamentary Inquiry into Stalking Law Reform, *Main Findings and Recommendations* (Justice Unions’ Parliamentary Group, 2012) at 11.

⁵⁶ *Ibid* at 23- where it was noted that campaigners in Scotland viewed stalking as “quantifiably different from harassment in law”.

⁵⁷ Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013).

⁵⁸ *Ibid* at paragraph 2.90.

⁵⁹ *Ibid*.

⁶⁰ *Ibid* at paragraph 2.91.

⁶¹ *Ibid* at paragraph 2.92.

stalking offence should be introduced particularly as a means of ensuring that stalking by digital or online means is more effectively targeted. In this respect, the experiences of Scotland and England and Wales may offer some guidance.

(1) Scotland

- 2.60 Prior to 2010, no specific stalking or harassment offences existed in Scotland. Instead, such behaviour was generally prosecuted under a common law breach of the peace offence. However, after a 2009 case *Harris v HM Advocate*,⁶² held that that the breach of the peace offence required a public element, there was concern that some cases of stalking would not satisfy this and would be difficult to prosecute. According to Middlemiss, there was particular concern that stalking that occurs in private or in an isolated place, as in the *Harris* case would not be covered.⁶³ There was also a need to address digital or online activity including stalking that is carried out through social media sites, telephone, texting and e-mail.⁶⁴ Thus, the new offences were partially introduced to ensure that harassment/stalking by digital or online means could be effectively prosecuted.
- 2.61 The *Criminal Justice and Licensing (Scotland) Act 2010* includes an offence of threatening and abusive behaviour (section 38) and a stalking offence (section 39). Both of these offences are designed to target harassment and related behaviour. The offence of threatening and abusive behaviour acts as a statutory version of the breach of the peace offence which previously applied. The offence prohibits individuals from behaving in a threatening or abusive manner where that behaviour is likely to cause a reasonable person fear or alarm and he or she either intends by the behaviour to cause fear or alarm or is reckless as to whether the behaviour would cause fear or alarm.⁶⁵ The offence applies whether the behaviour in question amounts to a course of conduct or a single act.⁶⁶ Thus, this is quite a broad offence, designed to target both once-off acts and persistent activity with no specific examples of the behaviour the offence can capture included in its wording. When the *Criminal Justice and Licensing (Scotland) Bill* was being debated, it was suggested by a number of representatives that this general offence would be sufficient to capture all forms of harassment and stalking without the need for a separate stalking offence.⁶⁷ However, this view was ultimately rejected as the Scottish Parliament was persuaded of the benefits of including a specific stalking offence alongside this general offence.
- 2.62 At the committee stage, Ann Moulds emphasised the importance of a specific stalking offence as the abusive and threatening behaviour offence “is an open, catch-all offence. It

⁶² *Harris (Mark) v HM Advocate* [2009] HCJAC 80.

⁶³ Middlemiss, “Let the stalker beware? Analysis of the law of stalking in Scotland” *J.Crim. L.* 407 at 411-412.

⁶⁴ *Ibid.*

⁶⁵ Section 38(1) of the *Criminal Justice and Licensing (Scotland) Act 2010*.

⁶⁶ Section 38(3) of the *Criminal Justice and Licensing (Scotland) Act 2010*.

⁶⁷ See, in particular, Justice Committee 13 April 2010 Meeting, Criminal Justice and Licensing (Scotland) Bill available at <http://www.scottish.parliament.uk/parliamentarybusiness/report.aspx?r=5494&mode=html>.

does not identify the crime or tell anybody what law has been broken".⁶⁸ She stated that stalking is "a hidden crime" and that it would remain hidden, despite it being a serious crime if the general offence alone was introduced.⁶⁹ Members of the Scottish police also supported a specific offence as they felt it offered clarity for both the general public and law enforcement agencies.⁷⁰

- 2.63 Thus, section 39 of the *Criminal Justice and Licensing Scotland Act 2010* provides for an offence of stalking. This offence is committed when a person stalks another person by engaging in a course of conduct with the intention of causing fear or alarm, or when he or she knows or ought to have known that engaging in the course of conduct would cause the victim fear or alarm, and the course of conduct causes the victim to suffer fear or alarm.⁷¹ Defences are included for lawful behaviour, behaviour engaged in for the purpose of preventing or detecting crime or where the course of conduct was reasonable in the circumstances.⁷² The section also includes a definition of "conduct", with a detailed list of prohibited behaviour described:

"'conduct' means—

- (a) following B [the victim] or any other person,
- (b) contacting, or attempting to contact, B or any other person by any means,
- (c) publishing any statement or other material—
 - (i) relating or purporting to relate to B or to any other person,
 - (ii) purporting to originate from B or from any other person,
- (d) monitoring the use by B or by any other person of the internet, email or any other form of electronic communication,
- (e) entering any premises,
- (f) loitering in any place (whether public or private),
- (g) interfering with any property in the possession of B or of any other person,
- (h) giving anything to B or to any other person or leaving anything where it may be found by, given to or brought to the attention of B or any other person,
- (i) watching or spying on B or any other person,
- (j) acting in any other way that a reasonable person would expect would cause B to suffer fear or alarm,"⁷³

The stalking offence does not apply to once off activity as the section provides that a course of conduct "involves conduct on at least two occasions"⁷⁴.

- 2.64 A notable feature of the Scottish offences is that both the general offence and the stalking offence carry the same penalties: a maximum 5 years imprisonment or a fine or both on conviction on indictment and a 12 month maximum sentence or a fine or both on summary conviction. This is even though the stalking offence is more difficult to prove, as it

⁶⁸ See Scottish Parliament Justice Committee, *Justice Committee Official Report 23 March 2010*, Criminal Justice and Licensing Scotland Bill, col. 2805, available at <http://archive.scottish.parliament.uk/s3/committees/justice/or-10/ju10-1102.htm#Col2775>.

⁶⁹ *Ibid.*

⁷⁰ *Ibid.*

⁷¹ Section 39(1), (2) of the *Criminal Justice and Licensing (Scotland) Act 2010*.

⁷² Section 39(5) of the *Criminal Justice and Licensing (Scotland) Act 2010*.

⁷³ Section 39(6) of the *Criminal Justice and Licensing (Scotland) Act 2010*.

⁷⁴ *Ibid.*

requires a course of conduct and for the victim to have actually suffered fear or alarm⁷⁵ (and consequently, if the threshold of this offence is not met at trial then the accused can be convicted of the threatening and abusive behaviour offence instead⁷⁶). The aggravated nature of the stalking offence would thus presumably be reflected at the sentencing stage with stalking convictions likely to attract sentences nearer to the higher end of the scale, compared to convictions for threatening and abusive behaviour.

(2) England and Wales

- 2.65 In 2012, England and Wales introduced the *Protection of Freedoms Act 2012* which inserted two new stalking offences into the *Protection from Harassment Act 1997*. These offences were introduced because the *Protection from Harassment Act 1997* was viewed as being ineffective at targeting stalking, with one contributor to the House of Lords debate on the *Protection of Freedoms Act 2012* summing up the situation as follows: “[t]he current law is patently not working and the state is failing victims”⁷⁷. The main problem identified with the *Protection from Harassment Act 1997* was its breadth,⁷⁸ in particular, it “did not go far enough to identify and prosecute the types of behaviour that distinguish stalking from other, milder cases of harassment”⁷⁹. Thus, the 1997 Act was described as “no longer fit for purpose”⁸⁰ as cases of stalking and harassment continued to rise since the 1997 Act was passed, and dissatisfaction was expressed by stalking victims who felt that their cases had not been taken seriously by the criminal justice system.⁸¹
- 2.66 England was also influenced by the success of the Scottish stalking laws, with the *Independent Parliamentary Inquiry into Stalking Law Reform* noting, that while there had only been 70 prosecutions for stalking in the 10 year period before the *Criminal Justice and Licensing (Scotland) Act* was passed in 2010, there had been 150 prosecutions in the first four months of that Act being introduced in the Strathclyde region alone.⁸² In particular, the fact that the Scottish law names the crime of stalking and lists relevant stalking behaviours was persuasive in ensuring that the specific stalking offences were adopted.

⁷⁵ The section 38 offence can apply where the behaviour “is likely to cause a reasonable person fear or alarm” - section 38(1)(b) of the *Criminal Justice and Licensing (Scotland) Act 2010*.

⁷⁶ Section 39(8) and (9) of the *Criminal Justice and Licensing (Scotland) Act 2010* provide: “(8) Subsection (9) applies where, in the trial of a person (“the accused”) charged with the offence of stalking, the jury or, in summary proceedings, the court—

(a) is not satisfied that the accused committed the offence, but

(b) is satisfied that the accused committed an offence under section 38(1).

(9) The jury or, as the case may be, the court may acquit the accused of the charge and, instead, find the accused guilty of an offence under section 38(1).”

⁷⁷ House of Lords Debate on *Protection of Freedoms Act 2012* (6 December 2011), col. 650 available at <http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/111206-0001.htm#11120644000422>

⁷⁸ *Independent Parliamentary Inquiry into Stalking Law Reform, Main Findings and Recommendations* (Justice Unions’ Parliamentary Group, 2012) at 21.

⁷⁹ House of Lords Debate on *Protection of Freedoms Act 2012* (6 December 2011), col. 650 available at <http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/111206-0001.htm#11120644000422>

⁸⁰ *Independent Parliamentary Inquiry into Stalking Law Reform, Main Findings and Recommendations* (Justice Unions’ Parliamentary Group, 2012) at 21.

⁸¹ *Ibid* at 22.

⁸² *Independent Parliamentary Inquiry into Stalking Law Reform, Main Findings and Recommendations* (Justice Unions’ Parliamentary Group, 2012) at 24.

2.67 The *Protection of Freedoms Act 2012* inserted sections 2A (offence of stalking) and 4A (stalking involving fear of violence or serious alarm or distress) into the *Protection from Harassment Act 1997*. Under section 2A, a person is guilty of an offence if they pursue a course of conduct that amounts to stalking.⁸³ A person pursues a course of conduct amounting to stalking if the course of conduct amounts to harassment, the acts or omissions involved are associated with stalking and the person knows or ought to have known that the course of conduct amounts to harassment.⁸⁴ The section then lists “examples of acts or omissions which, in particular circumstances, are ones associated with stalking”:

- “(a) following a person,
- (b) contacting, or attempting to contact, a person by any means,
- (c) publishing any statement or other material—
 - (i) relating or purporting to relate to a person, or
 - (ii) purporting to originate from a person,
- (d) monitoring the use by a person of the internet, email or any other form of electronic communication,
- (e) loitering in any place (whether public or private),
- (f) interfering with any property in the possession of a person,
- (g) watching or spying on a person.”⁸⁵

This is a summary offence which carries maximum penalties of 51 weeks imprisonment or a fine not exceeding £5000.⁸⁶ This offence carries a greater maximum term of imprisonment than the general offence of harassment under section 2 of the *Protection from Harassment Act 1997* which has a 6 month maximum sentence.⁸⁷

2.68 The aggravated stalking offence under section 4A is committed where a defendant pursues a course of conduct which amounts to stalking and either causes another person to fear on at least two occasions that violence will be used against them, or causes another serious alarm or distress which has “a substantial adverse effect” on the other person’s usual day to day activities. It must also be established that the defendant knows or ought to know that his/her course of conduct will cause the other person fear or alarm or distress⁸⁸ based on whether a reasonable person with the same information as the defendant would think that the course of conduct would cause this⁸⁹. This offence carries a maximum penalty of 5 years imprisonment or a fine or both on conviction on indictment and 12 months or a fine or both on summary conviction.⁹⁰ These penalties are the same as those that apply to the general “putting people in fear of violence” offence under section 4 of the *Protection from Harassment Act 1997*.

2.69 It has been suggested that the main result of introducing the new stalking offences in England was “to simply set out that which was always implicit – stalking counts as

⁸³ Section 2A(1) of the *Protection from Harassment Act 1997*.

⁸⁴ Section 2A(2) of the *Protection from Harassment Act 1997*.

⁸⁵ Section 2A(3) of the *Protection from Harassment Act 1997*.

⁸⁶ Section 2A(4) of the *Protection from Harassment Act 1997*.

⁸⁷ Section 2(2) of the *Protection from Harassment Act 1997*.

⁸⁸ Section 4A(1) of the *Protection from Harassment Act 1997*.

⁸⁹ Section 4A(2), (3) of the *Protection from Harassment Act 1997*.

⁹⁰ Section 4A(5) of the *Protection from Harassment Act 1997*.

behaviour that can cause harassment”⁹¹. However, the offences seem to have had a significant practical impact with the number of charges brought under the *Protection from Harassment Act 1997* rising from 10,059 in 2012 to 13,348 in 2014.⁹²

(3) Northern Ireland

- 2.70 In Northern Ireland, stalking cases are currently prosecuted under the harassment offences in section 4 and section 6 of the *Protection from Harassment (Northern Ireland) Order 1997* (which broadly correspond to the harassment offences in the English and Welsh *Protection from Harassment Act 1997*). However, in response to a debate in the Northern Ireland Assembly in September 2016 on stalking, the Northern Ireland Justice Minister indicated that her Department would actively consider whether a specific stalking offence should be introduced, taking account of the experience in Scotland, England and Wales.⁹³

(4) Does Ireland need a specific stalking offence?

- 2.71 The experiences of Scotland and England and Wales suggest a number of advantages to introducing a specific stalking offence. Firstly, specifically naming stalking as an offence appears to have had a significant practical effect, with the number of prosecutions for stalking activity increasing in both Scotland and England and Wales since they introduced specific stalking offences.
- 2.72 Secondly, identifying stalking as a specific crime carries particular importance for victims of stalking because of the “hidden” nature of the crime as well as its more serious nature compared to harassment. This has been acknowledged by the English *Independent Parliamentary Inquiry into Stalking Reform* stating, that “[n]aming the crime appears to increase public protection from stalking and the confidence of victims”.⁹⁴ Thus, by specifically naming stalking in legislation, rather than including it within the broad-ranging offence of harassment, the different and more insidious character of the crime is underlined.
- 2.73 The Commission therefore recommends that a stalking offence, separate from the related offence of harassment, should be introduced. The Commission considers that the essential ingredients of the stalking offence should be the same as the proposed, amended, harassment offence, so that the offence would be committed where a person “stalks” another person by persistently following, watching, pestering or besetting another person or by persistently communicating by any means of communication with the other person or by persistently communicating with a third person by any means of communication about the other person.
- 2.74 For the purposes of this offence, a person would stalk another person where he or she, by his or her acts intentionally or recklessly, seriously interferes with the other person’s peace and privacy **and** causes alarm, distress or harm to the other person and his or her

⁹¹ Gowland, “Protection from Harassment Act 1997: The ‘New’ Stalking Offences” (2013) 77(5) J. Crim. L. 387, 398.

⁹² “Stalking offences up 33% across UK- police figures” *Reuters* 24 June 2015 available at <https://www.rt.com/uk/269455-stalking-harassment-offences-rise/>.

⁹³ Northern Ireland Assembly, Official Report (Hansard), Volume 115, No 1, 12 September 2016, available at <http://data.niassembly.gov.uk/HansardXml/plenary-12-09-2016.pdf>.

⁹⁴ Independent Parliamentary Inquiry into Stalking Law Reform, *Main Findings and Recommendations* (Justice Unions’ Parliamentary Group, 2012) at 28.

acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy **and** cause alarm, distress or harm to the other person. Thus, the stalking offence would differ from the harassment offence by requiring the intentional or reckless acts of the perpetrator to interfere seriously with the victim's peace and privacy and cause him or her alarm, distress or harm, as opposed to the harassment offence which makes these alternative requirements. This additional threshold that would need to be met for the stalking offence to be committed, as opposed to harassment, underlines stalking's status as an aggravated form of harassment.

- 2.75 The Commission recommends that the stalking offence carry the same penalties as the re-stated harassment offence, that is, on summary conviction a Class A fine and/or imprisonment for a term not exceeding 12 months and, on conviction on indictment, an unlimited fine and/or imprisonment not exceeding 7 years. While the Commission considers stalking to be an aggravated form of harassment, it does not feel that it is necessary to provide for a higher maximum sentence for stalking than is provided for harassment. The 7 year maximum sentence for harassment is considerable and is already greater than many jurisdictions, such as England and Wales where the maximum sentence for comparable offences is 5 years. Furthermore, the relevant aggravating factors in an individual case can suitably be taken into account at the sentencing stage.

- 2.76 **The Commission recommends that an offence of stalking separate from the related offence of harassment should be enacted. The Commission recommends that the essential ingredients of the stalking offence should be the same as the harassment offence, whereby the offence would be committed where a person "stalks" another person by persistently following, watching, pestering or besetting another person or by persistently communicating by any means of communication with the other person or by persistently communicating with a third person by any means of communication about the other person. However, the stalking offence would differ from the harassment offence by requiring the intentional or reckless acts of the perpetrator to interfere seriously with the victim's peace and privacy and cause him or her alarm, distress or harm, as opposed to the harassment offence which makes these alternative requirements.**

D Offences Designed to Target Once-off Harmful Digital Communications

- 2.77 As discussed above, section 10 of the *Non-Fatal Offences Against the Person Act 1997* is limited to persistent behaviour. The Commission recommended in its 2013 *Report on Aspects of Domestic Violence* that harassment should be confined to persistent behaviour,⁹⁵ as described in *Director of Public Prosecutions (O'Dowd) v Lynch*,⁹⁶ 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.⁹⁷
- 2.78 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

⁹⁵ Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraph 2.97.

⁹⁶ [2008] IEHC 183, [2010] 3 IR 434.

⁹⁷ Law Reform Commission, *Report on Aspects of Domestic Violence* (LRC 111-2013), paragraphs 2.93-2.94.

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 section of the Report 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.⁹⁸

- 2.79 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 media sites 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.⁹⁹
- 2.80 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.
- 2.81 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 digital communications.

(1) Other relevant criminal offences

- 2.82 Offences in the *Post Office (Amendment) Act 1951* (as amended in 2007), the *Non-Fatal Offences Against the Person Act 1997*, the *Criminal Damage Act 1991*, the *Child Trafficking and Pornography Act 1998* and the *Data Protection Acts 1988 and 2003* are capable of capturing some but not all forms of once-off harmful digital communications.

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

- 2.83 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—

⁹⁸ See Chapter 3.

⁹⁹ See O’Higgins Norman “Report on Cyberbullying Research and Related Issues” Conference Paper, 1st 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”.

- (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."

- 2.84 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.
- 2.85 Section 13 was introduced to "enable the Department [of Posts and Telegraphs] to deal adequately with telephone offences, e.g. nuisance calls, false ambulance calls, grossly offensive or annoying conduct on the telephone".¹⁰⁰ No similar offence existed under previous Post Office legislation. The section was amended in 2007 by the *Communications Regulation (Amendment) Act 2007*. This amendment clarified that the offence could apply to text messages, but the main purpose of the amendment was to increase the penalties that apply under the section.¹⁰¹ During the committee stage of the Bill, a Senator recommended that the offence be extended to electronic mail, as well as text message as proposed, as a means of targeting cyber-bullying.¹⁰² However, this proposal was rejected by the Minister for Communications, Marine and Natural Resources on the grounds that it would widen the offence "considerably" and "would not fit in with the remit of the Bill as originally introduced" as "the sole intent of the Bill is to address nuisance calls to the emergency services only".¹⁰³ Thus, the merit of extending the offence to cover electronic communications was not considered, as this type of amendment was not deemed suitable for the particular Bill under debate.
- 2.86 As noted above,¹⁰⁴ in 2014 the *Report of the Internet Content Governance Advisory Group* recommended that section 13 be amended to include "electronic communications" within the definition of measures dealing with the "sending of messages which are grossly

¹⁰⁰ See Vol. 126 *Dáil Éireann Debates*, 27 June 1951, Post Office (Amendment) Bill, 1951– Second Stage, comments by Minister for Posts and Telegraphs Erskine Childers available at <http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/takes/dail1951062700053?opendocument>.

¹⁰¹ Vol. 186 *Seanad Éireann Debates*, 20 February 2007, Communications Regulation (Amendment) Bill 2007 Committee Stage, comments by Minister for Communications, Marine and Natural Resources Noel Dempsey available at 186 <http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/DebatesWebPack.nsf/takes/seanad2007022000008?opendocument&highlight=communications%20regulation%20%28amendment%29%20act%202007>.

¹⁰² Vol. 186 *Seanad Éireann Debates*, 20 February 2007, Communications Regulation (Amendment) Bill 2007 Committee Stage, comments by Senator Michael McCarthy available at 186 <http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/DebatesWebPack.nsf/takes/seanad2007022000008?opendocument&highlight=communications%20regulation%20%28amendment%29%20act%202007>.

¹⁰³ Vol. 186 *Seanad Éireann Debates*, 20 February 2007, Communications Regulation (Amendment) Bill 2007 Committee Stage, comments by Minister for Communications, Marine and Natural Resources Noel Dempsey available at 186 <http://oireachtasdebates.oireachtas.ie/Debates%20Authoring/DebatesWebPack.nsf/takes/seanad2007022000008?opendocument&highlight=communications%20regulation%20%28amendment%29%20act%202007>.

¹⁰⁴ Chapter 1, paragraph 1.11.

offensive, indecent, obscene or menacing”.¹⁰⁵ In its Issues Paper, the Commission stated that it agreed with this proposed amendment.¹⁰⁶ However, upon further consideration, the Commission feels that a more comprehensive amendment to section 13 is required.

- 2.87 The Commission feels that simply inserting “electronic communications” into section 13(1)(a) would not be an appropriate response to the need for a criminal offence to target once-off harmful digital communications. Section 13 uses terminology which is out-dated and potentially vague and requires more extensive reformulation if it is to successfully apply to modern forms of communication. This is discussed further below, where vagueness and the principle of legality are considered in light of a decision of the Indian Supreme Court,¹⁰⁷ where an offence relating to sending harmful electronic communications, which contained expressions including “menacing” and “grossly offensive” was struck down as unconstitutional.
- 2.88 Locating the offence within post office legislation also appears unsuitable should it be expanded to include digital communications, which, as the Minister noted during the 2007 Act debate, would represent a considerable widening of the offence. However, while the Minister claimed that section 13 was designed to target nuisance calls to emergency services only, this does not appear to be the case based on the debates surrounding the 1951 Act, noted above, where a wider purpose behind the section was indicated. Nonetheless this should be clarified. It would thus be preferable to repeal section 13 and provide for a new offence in a dedicated harmful communications bill instead. This is considered further below.

(b) *Section 5 of the Non-Fatal Offences Against the Person Act 1997*

- 2.89 Section 5 of the *Non-Fatal Offences Against the Person Act 1997* provides for an offence of making a threat to kill or cause serious harm. This offence applies to threats “by any means”¹⁰⁸ and therefore would appear to extend to threats made online. This offence also applies to once-off threats as there is no persistence element included. In order to commit this offence, the perpetrator must make the threat “intending the other to believe it will be carried out”¹⁰⁹ this requirement ensures that only intentional threats are captured by this offence and so, for example, messages posted online which use threatening language but are made without this intention are not covered. This offence carries a maximum sentence of 12 months for a summary conviction and 10 years for a conviction on indictment.¹¹⁰

(c) *Criminal Damage Act 1991*

- 2.90 The *Criminal Damage Act 1991*¹¹¹ replaced 19th century legislation on criminal damage. It took account of advances in technology, so that it can be applied to digital or online

¹⁰⁵ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014) at page 45.

¹⁰⁶ Law Reform Commission *Issues Paper on Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying* (LRC IP 6-2014) at page 3.

¹⁰⁷ *Shreya Singhal v Union of India* (2015) Writ Petition (Criminal) No. 167 of 2012.

¹⁰⁸ Section 5(1) of the *Non-Fatal Offences Against the Person Act 1997*.

¹⁰⁹ *Ibid.*

¹¹⁰ Section 5(2) of the *Non-Fatal Offences Against the Person Act 1997*.

¹¹¹ 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.

communication where an individual's computing technology is targeted by unauthorised access or hacking of their email, social media or other type of internet-based account to send harmful messages or post harmful material. By contrast with the requirement for persistence in section 10 of the 1997 Act, the 1991 Act applies to once-off activity.

2.91 The 1991 Act extends to the deletion and modification of data.¹¹² 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."

2.92 "Damage" in relation to data is defined in section 1(1) of the 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.¹¹³ 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."¹¹⁴ 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.

2.93 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.

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.

¹¹² 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."

¹¹³ "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>.

¹¹⁴ 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>.

- 2.94 The 1991 Act also includes an offence, under section 5, of unauthorised accessing of data. This offence applies where a person without lawful excuse operates a computer-
- “(a) within the State with intent to access any data kept either within or outside the State, or
(b) outside the State with intent to access any data kept within the State,
shall, whether or not he accesses any data, be guilty of an offence.”

The offence is committed whether or not the person intended to access the relevant data. In the context of harmful digital communications, this offence may be relevant where content is hacked from an individual's devices or cloud services and posted publicly.

- 2.95 The *Criminal Justice (Offences Relating to Information Systems) Bill 2016* proposes to implement the 2013 EU Directive on Attacks Against Information Systems.¹¹⁵ The Bill proposes to amend the 1991 Act to remove all references to data and to introduce a number of new offences to replace the offences under the 1991 Act which relate to damage to data and unauthorised accessing of data.
- 2.96 Assuming the 2016 Bill is enacted, the offence under section 2 of the 1991 Act relating to damage to property including data will be replaced with an offence of “interference with data without lawful authority”.¹¹⁶ This offence will be committed where a person without lawful authority “intentionally deletes, damages, alters or suppresses, or renders inaccessible, or causes the deterioration of, data on an information system”. The hacking offence currently provided for under section 5 of the 1991 Act will be replaced by offences dealing with accessing an information system without lawful authority¹¹⁷ and interfering with the functioning of an information system by imputing data, transmitting, deleting, altering, suppressing or causing the deterioration of data or rendering data on the system inaccessible.¹¹⁸ The Bill also includes offences dealing with intercepting the transmission of data without lawful authority¹¹⁹ and using a computer programme or any device, password, unencryption key or code or access code to commit one of the other offences provided for in the Bill.¹²⁰
- 2.97 The 2016 Bill contains a provision on jurisdiction (discussed below¹²¹) which extends the offences to persons within the State who commit an offence in relation to an information system outside the State¹²² and persons outside the State who commit an offence in relation to an information system in the State.¹²³ The Bill also extends to Irish citizens, persons ordinarily resident in the State, a body corporate established under the law of the State and companies formed and registered or otherwise provided for under the *Companies Act 2014*, who commit an offence outside the State in relation to an

¹¹⁵ Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

¹¹⁶ Section 4 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

¹¹⁷ Section 2 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

¹¹⁸ Section 3 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

¹¹⁹ Section 5 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

¹²⁰ Section 6 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

¹²¹ See paragraph 2.230.

¹²² Section 10(1)(a) of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

¹²³ Section 10(1)(b) of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

information system outside the State where the act is also an offence under the law of the place where the act was committed.¹²⁴

(d) *Child Trafficking and Pornography Act 1998*

- 2.98 The distribution of intimate images of children (child pornography) online is a crime under section 5 of the *Child Trafficking and Pornography Act 1998*. Online distribution of child pornography is expressly included under the Act as the definition of child pornography extends to any visual or audio representation of a child (who is engaged in or depicted as being engaged in sexual activity or depicted as witnessing sexual activity or whose dominant characteristic is the depiction, for a sexual purpose, of the genital or anal region of a child or encourages or counsels any sexual activity with children or indicates or implies that a child is available to be used for the purpose of sexual exploitation) “irrespective of how or through what medium the representation, description or information has been produced, transmitted or conveyed”¹²⁵. There is no persistence requirement under section 5 of the 1998 Act and so the offence is capable of capturing once off uploads of intimate content where the person depicted is under 17 years.
- 2.99 Section 5 of the 1998 Act relates to the production, distribution, publication, import, export or sale of child pornography. Section 5(1) provides that an offence is committed by any person who-
- “(a) knowingly produces, distributes, prints or publishes any child pornography,
 - (b) knowingly imports, exports, sells or shows any child pornography,
 - (c) knowingly publishes or distributes any advertisement likely to be understood as conveying that the advertiser or any other person produces, distributes, prints, publishes, imports, exports, sells or shows any child pornography,
 - (d) encourages or knowingly causes or facilitates any activity mentioned in paragraph (a), (b) or (c), or
 - (e) knowingly possesses any child pornography for the purpose of distributing, publishing, exporting, selling or showing it”
- 2.100 A person found guilty of an offence under section 5 is liable on summary conviction to a fine not exceeding €2500 or to imprisonment for a term not exceeding 12 months or both and to a fine or to imprisonment for a term not exceeding 14 years or both on conviction on indictment.
- 2.101 A potentially problematic feature of the 1998 Act is that it makes no express provision for what might be described as self-produced child pornography,¹²⁶ whereby individuals under the age of 17 send intimate content to others under 17, frequently referred to as “sexting.” This type of behaviour has become more pervasive since the introduction of camera phones and particularly smartphones and thus is unlikely to have been contemplated when the 1998 Act was enacted. There is therefore no discretion in the 1998 Act to account for the age of the defendant, unlike the *Criminal Law (Sexual Offences) Act 2006*, which only allows proceedings for the offence of defilement of child

¹²⁴ Section 10(1)(c) of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

¹²⁵ Section 2(1) of the *Child Trafficking and Pornography Act 1998*.

¹²⁶ This term is used by Hallissey to describe sexting between children under the age of 17. See Hallissey, “The Constitutional Status of ‘Sexting’ and Self-Produced Child Pornography” (2012) 22(4) ICLJ 109.

under the age of 17 years to be taken by or with the consent of the DPP where the defendant is under the age of 17 years.¹²⁷ Thus, Hallissey notes the anomalous situation that currently stands whereby, if an underage couple engages in sexual activity they may not be breaking the law, if they come under one of the exceptions provided for in the 2006 Act, but if they film this activity then they are open to the full force of the criminal law.¹²⁸

- 2.102 The *Criminal Law (Sexual Offences) Bill 2015* proposes to make a number of amendments to the 1998 Act in order to implement the 2011 EU Directive on Combating Sexual Abuse and Sexual Exploitation of Children and Child Pornography¹²⁹. The 2015 Bill proposes to strengthen the law against child pornography significantly, particularly through making better provision for targeting the online distribution and means of acquiring such content. The Bill proposes to update the language used in section 5 of the 1998 Act by inserting “transmits” and “disseminates” after “distributes”.¹³⁰ The 2015 Bill also proposes to amend the offence of possession of child pornography under section 6 of the 1998 Act by providing that the offence would be committed if a person “acquires” child pornography as well as possesses such material or if a person “knowingly obtains access to child pornography by means of information and communication technology”.¹³¹
- 2.103 The 2015 Bill also proposes to introduce offences relating to the use of information and communication technology to facilitate the sexual exploitation of a child.¹³² The first offence would provide that a person who “by means of information and communication technology communicates with another person (including a child) for the purpose of facilitating the sexual exploitation¹³³ of a child by that person or any other person” is guilty of an offence and liable on conviction on indictment to a term of imprisonment not exceeding 14 years. The second offence relates to using information and communication technology to send sexually explicit material to a child. “Sexually explicit material” is defined as “any indecent or obscene images”¹³⁴. On summary conviction this offence would carry a maximum penalty of a term of imprisonment not exceeding 12 months; on conviction on indictment it would carry a maximum sentence of 5 years imprisonment.

¹²⁷ Section 3(9) of the *Criminal Law (Sexual Offences) Act 2006*.

¹²⁸ Hallissey, “The Constitutional Status of ‘Sexting’ and Self-Produced Child Pornography” (2012) 22(4) ICLJ 109, at 113.

¹²⁹ *Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA*.

¹³⁰ Section 12 of the *Criminal Law (Sexual Offences) Bill 2015*.

¹³¹ Section 14 of the *Criminal Law (Sexual Offences) Bill 2015*.

¹³² Section 8 of the *Criminal Law (Sexual Offences) Bill 2015*.

¹³³ “Sexual exploitation” is defined in section 2 of the Bill as meaning, in relation to a child, “(a) inviting, inducing or coercing the child to engage in prostitution or the production of child pornography,

(b) the prostitution of the child or the use of the child for the production of child pornography,

(c) the commission of an offence specified in the Schedule to the Act of 2001 against the child, causing another person to commit such an offence against the child, or inviting, inducing or coercing the child to commit such an offence against another person,

(d) inducing or coercing the child to engage or participate in any sexual, indecent or obscene act,

(e) inviting the child to engage or participate in any sexual, indecent or obscene act which, if done, would involve the commission of an offence against the child, or

(f) inviting, inducing or coercing the child to observe any sexual, indecent or obscene act, for the purpose of corrupting or depraving the child.”

¹³⁴ Section 8(4) of the *Criminal Law (Sexual Offences) Bill 2015*.

Significantly, the Bill provides that no proceedings shall be brought for these offences against children under the age of 17 except by or with the consent of the DPP.¹³⁵

- 2.104 The proposed offence of sending sexually explicit material to a child in the 2015 Bill could be applied in cases involving underage sexting instead of the distribution of child pornography offence under the 1998 Act. This offence would be more suitable for such cases as the requirement for the DPP to consent before such proceedings could be brought ought to ensure that cases involving teenagers of similar age consensually exchanging intimate images are not prosecuted. Charging this offence in the case of children under the age of 17 instead of the distribution of child pornography offence would also allow the child to avoid the stigma associated with child pornography offences which were clearly not intended to apply to self-generated content distributed by teenagers.

(e) *Data Protection Acts 1988 and 2003*

- 2.105 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 involve the implementation of a 1981 Council of Europe Convention¹³⁶ and a 1995 EU Directive on Data Protection¹³⁷ 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. The 2016 General Data Protection Regulation,¹³⁸ when it comes into force in May 2018, will replace the 1995 Directive and will ensure even greater harmonisation across EU member states in this area.
- 2.106 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. Yet, as noted by both the Oireachtas Committee on Transport and Communications and the 2014 *Report of 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.¹³⁹
- 2.107 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

¹³⁵ Section 8(3) of the *Criminal Law (Sexual Offences) Bill 2015*.

¹³⁶ Council of Europe, *Convention for the Protection of individuals with regard to Automatic Processing of Personal Data* (28 January 1981).

¹³⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

¹³⁸ Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The 2016 Regulation is discussed further in Chapter 3, at paragraphs 3.30-3.46.

¹³⁹ 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, Climate Action and Environment, 2014) at 41.

possession of the data controller”.¹⁴⁰ 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”¹⁴¹ and this definition includes social networking and other websites.¹⁴² 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.”¹⁴³ This is known as the “household exemption” and it will generally exclude personal data posted on private social networking pages.¹⁴⁴ 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.¹⁴⁵ The Article 29 Data Protection Working Party has 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 the household exemption does not apply and the user would be considered a data controller.¹⁴⁶ 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 1988 and 2003*.

- 2.108 For the *Data Protection Acts 1988 and 2003* to apply, the data controller must either be established in the State and the data in question processed in the context of that establishment¹⁴⁷ or in the case of data controllers not established in the State or in any

¹⁴⁰ Section 1 of the *Data Protection Act 1988*.

¹⁴¹ 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.”

¹⁴² See Article 29 Data Protection Working Party *Opinion 5/2009 on online social networking* 01189/09/EN WP 163 (June 2009) at 5.

¹⁴³ Section 1(4)(c) of the *Data Protection Act 1988*, implementing the “household exemption” in Article 3.2 of Directive 95/46/EC.

¹⁴⁴ Article 29 Data Protection Working Party *Opinion 5/2009 on online social networking* 01189/09/EN WP 163 (June 2009) at 5.

¹⁴⁵ 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 website 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.

¹⁴⁶ See Article 29 Data Protection Working Party *Opinion 5/2009 on online social networking* 01189/09/EN WP 163 (June 2009) at 6.

¹⁴⁷ 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—

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.”¹⁴⁸

- 2.109 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.¹⁴⁹ 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 Commissioner¹⁵⁰ who will attempt to settle the dispute by amicable resolution and will notify the individual if this is not possible.¹⁵¹ 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 time.¹⁵² 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.¹⁵³ It is an offence to fail or refuse to comply, without reasonable excuse, with an enforcement notice.¹⁵⁴ 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.¹⁵⁵ Where a person is convicted under the Acts, the

(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.”

¹⁴⁸ Section 1(3B)(a)(ii) of the *Data Protection Act 1988*.

¹⁴⁹ 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.”

¹⁵⁰ 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.

¹⁵¹ Section 10(1)(b)(ii) of the 1988 Act. This decision then may be appealed to the Circuit Court within 21 days.

¹⁵² Section 10(2) of the *Data Protection Act 1988*.

¹⁵³ 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.

¹⁵⁴ Section 10(9) of the *Data Protection Act 1988*.

¹⁵⁵ Section 31(1) of the *Data Protection Act 1988*.

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.¹⁵⁶

- 2.110 Therefore, while the *Post Office (Amendment) Act 1951*, the *Non-Fatal Offences Against the Person Act 1997*, the *Criminal Damage Act 1991*, the *Child Trafficking and Pornography Act 1998* and the *Data Protection Acts 1988 and 2003* cover some once-off harmful digital communications, none of these offences are capable of providing a comprehensive response to this type of behaviour. The Commission thus considers that new criminal offences are required. In this respect, it is instructive to look at how other jurisdictions have legislated for this type of activity.

(2) How once-off harmful digital communications are dealt with in other jurisdictions

- 2.111 A number of jurisdictions have introduced offences designed to target once-off harmful digital communications including New Zealand, Australia, Canada and England and Wales. The experiences of these states can offer guidance on how legislating for this issue can be approached.

(a) General offences designed to target once-off harmful digital communications

(i) New Zealand

- 2.112 In 2015, New Zealand introduced an offence of “causing harm by posting a digital communication” under section 22 of the *Harmful Digital Communications Act 2015*. This offence is designed to target harmful once-off digital communications. This offence is committed where a person posts a digital communication with the intention to cause harm to a victim and this action would cause harm to a reasonable person in the position of the victim and the posting causes harm to the victim.¹⁵⁷ The Act defines “harm” as “serious emotional distress”.¹⁵⁸
- 2.113 In assessing whether a post would cause harm the court may take into account any factors it considers relevant including the extremity of the language used, the age and characteristics of the victim, whether the communication was anonymous, whether it was repeated, the extent of circulation of the communication, whether it is true or false and the context in which the communication appeared.¹⁵⁹ The definition of “posts a digital communication” extends to the posting of intimate videos and images,¹⁶⁰ behaviour which

¹⁵⁶ Section 31(2) of the *Data Protection Act 1988*.

¹⁵⁷ Section 22(1) of the *Harmful Digital Communications Act 2015*.

¹⁵⁸ Section 4 of the *Harmful Digital Communications Act 2015*.

¹⁵⁹ Section 22(2) of the *Harmful Digital Communications Act 2015*.

¹⁶⁰ Section 4 of the *Harmful Digital Communications Act 2015* defines “posts a digital communication” as follows—

“(a) means transfers, sends, posts, publishes, disseminates, or otherwise communicates by means of a digital communication—

(i) any information, whether truthful or untruthful, about the victim;

or

(ii) an intimate visual recording of another individual; and

(b) includes an attempt to do anything referred to in paragraph (a)”

Section 4 of the Act also defines an “intimate visual recording” as follows—

“(a) means a visual recording (for example, a photograph, videotape, or digital image) that is made in any medium using any device with or without the knowledge or consent of the individual who is the subject of the recording,

and that is of—

some other jurisdictions, discussed below, have chosen to provide specific offences for. The offence carries a maximum sentence of 2 years imprisonment.¹⁶¹

- 2.114 This offence has been subjected to considerable criticism since the *Harmful Digital Communications Act 2015* was passed. Commentators argue that the offence is overbroad and vague, particularly the definition of harm and the factors which can be taken into account when assessing whether harm is caused.¹⁶² It has also been suggested that the offence has created a situation whereby behaviour which is legal offline is illegal online as the offence captures a very wide category of speech.¹⁶³ In this respect, one commentator highlighted that public interest speech such as exposing corruption online could be covered by the offence as well as parody and satire.¹⁶⁴ The offence has thus been described as a “threat to online free speech”.¹⁶⁵
- 2.115 However, the prosecutions taken under section 22 to date do not suggest that the offence is being used excessively or inappropriately. As of April 2016, the offence has been used to charge around 12 people since its introduction in July 2015.¹⁶⁶ The types of cases that have been prosecuted include a man who was jailed for 11 months for posting a “disturbing” video on Facebook aimed at a woman¹⁶⁷ and a number of cases involving so-called “revenge porn”.¹⁶⁸

(i) an individual who is in a place which, in the circumstances, would reasonably be expected to provide privacy, and the individual is—

(A) naked or has his or her genitals, pubic area, buttocks, or female breasts exposed, partially exposed, or clad solely in undergarments; or

(B) engaged in an intimate sexual activity; or

(C) engaged in showering, toileting, or other personal bodily activity that involves dressing or undressing; or

(ii) an individual’s naked or undergarment-clad genitals, pubic area, buttocks, or female breasts which is made—

(A) from beneath or under an individual’s clothing; or

(B) through an individual’s outer clothing in circumstances where it is unreasonable to do so; and

(b) includes an intimate visual recording that is made and transmitted in real time without retention or storage in—

(i) a physical form; or

(ii) an electronic form from which the recording is capable of being reproduced with or without the aid of any device or thing.”

¹⁶¹ Section 22(3) of the *Harmful Digital Communications Act 2015*. A body corporate which is convicted of this offence is liable to a fine not exceeding \$200,000 (£122,708).

¹⁶² See, for example, “New law poorly-drafted, vague, and could criminalise free speech” *Stuff.co.nz* 6 July 2015 available at <http://www.stuff.co.nz/the-press/opinion/69955436/new-law-poorly-drafted-vague-and-could-criminalise-free-speech>.

¹⁶³ *Ibid.*

¹⁶⁴ *Ibid.*

¹⁶⁵ “Cross-Examination: The Unintended Consequences of the Harmful Digital Communications Act” *Equal Justice Project* available at <http://equaljusticeproject.co.nz/2015/07/cross-examination-the-unintended-consequences-of-the-harmful-digital-communications-act/>.

¹⁶⁶ “Online bullying law showing teeth, but gap remains” *Stuff.co.nz* 22 April 2016 available at <http://www.stuff.co.nz/nelson-mail/opinion/79197653/online-bullying-law-showing-teeth-but-gap-remains>.

¹⁶⁷ “Kiwi man jailed for sending ‘disturbing’ Facebook video” *Stuff.co.nz* 20 April 2016 available at <http://www.stuff.co.nz/national/crime/79121013/Man-jailed-for-disturbing-Facebook-video>.

¹⁶⁸ See “Victim: revenge porn ‘devastating’” *New Zealand Herald* 20 April 2016 available at http://m.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11625636.

(ii) UK

- 2.116 In the UK, there are two offences capable of applying to once-off harmful online communications on a general basis: section 1 of the *Malicious Communications Act 1988*¹⁶⁹ and section 127 of the *Communications Act 2003*¹⁷⁰.
- 2.117 Section 1 of the *Malicious Communications Act 1988* provides for an offence of (a) sending a letter, electronic communication or article of any description which conveys a message which is indecent or grossly offensive, a threat or information which is false and known or believed to be false by the sender and (b) "sending an article or electronic communication which is, in whole or part of an indecent or grossly offensive nature".¹⁷¹ The offence carries a maximum sentence of 12 months on summary conviction and 2 years for conviction on indictment.¹⁷²
- 2.118 Under section 127 of the *Communications Act 2003*, a person who sends, by a public electronic communications network, a message or other matter that is grossly offensive, indecent, obscene or menacing or causes such a message or other matter to be sent is guilty of an offence.¹⁷³ The section also makes it an offence to send or cause to be sent false messages by means of a public electronic communications network or to persistently make use of a public electronic communications network for the purpose of causing annoyance, inconvenience or needless anxiety.¹⁷⁴ This is a summary offence and carries a maximum term of imprisonment of 6 months.¹⁷⁵ A message sent by a "public electronic communications network" has been held to include a message sent by Twitter¹⁷⁶ and to also extend to other communications sent via social media which are "accessible to all those who have access to the internet"¹⁷⁷
- 2.119 The Crown Prosecution Service's Guidelines on Social Media¹⁷⁸ offer guidance on the use of section 1 of the *Malicious Communications Act 1988* and section 127 of the *Communications Act 2003*. The Guidelines state that "grossly offensive, indecent, obscene or false communications" are "subject to a high threshold and in many cases a prosecution is unlikely to be in the public interest", however, credible threats, which the offences can also apply to, "should be prosecuted robustly".¹⁷⁹ This approach appears to have been influenced by the controversial *Chambers v DPP*¹⁸⁰ case where the decision to prosecute an individual under section 127 for sending a "tweet" which was intended to be

¹⁶⁹ This offence extends to England and Wales and Northern Ireland.

¹⁷⁰ This offence extends to England and Wales, Northern Ireland and Scotland.

¹⁷¹ Section 1(1) of the *Malicious Communications Act 1988*. This offence was amended to include electronic communications under section 43 of the *Criminal Justice and Police Act 2001*.

¹⁷² Section 1(4) of the *Malicious Communications Act 1988* (as amended by the *Criminal Justice and Courts Act 2015*). The offence carried a maximum penalty of six months imprisonment prior to the 2015 amendment.

¹⁷³ Section 127(1)(a) of the *Communications Act 2003*.

¹⁷⁴ Section 127(1)(b) of the *Communications Act 2003*.

¹⁷⁵ Section 127(3) of the *Communications Act 2003*.

¹⁷⁶ *Chambers v DPP* [2012] EWH2 2157.

¹⁷⁷ Crown Prosecution Service, *Interim Revised CPS Guidelines on Prosecuting Social Media cases* (3 March 2016) available at http://www.cps.gov.uk/consultations/social_media_consultation_2016.html. The CPS Guidelines were first published as interim guidelines in December 2012.

¹⁷⁸ *Ibid.*

¹⁷⁹ *Ibid.*

¹⁸⁰ [2012] EWHC 2157.

humorous and did not create “fear or apprehension in those to whom it is communicated”¹⁸¹ was extensively criticised.¹⁸²

- 2.120 Thus, the CPS Guidelines state that a prosecution under either section 1 of the *Malicious Communications Act 1988* or section 127 of the *Communications Act 2003* should only proceed where the prosecutor is satisfied that there is sufficient evidence that the communication in question is more than “offensive shocking or disturbing” or “satirical, iconoclastic or rude comment” or “the expression of unpopular or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it”.¹⁸³ However, once the communication meets this threshold, the prosecutor still has to consider whether it is in the public interest to prosecute. In this respect, key considerations include whether a specific person was targeted and whether there was an intention to cause distress or anxiety, whether the communication is repeated and the age and maturity of the suspect, with prosecutions of those under 18 “rarely likely to be in the public interest”.¹⁸⁴
- 2.121 Nevertheless, despite the presence of these Guidelines, it appears to remain difficult for prosecutors in the UK to strike the right balance between punishing wrongdoing and ensuring freedom of expression is safeguarded. While prosecutions under section 127 in the Nimmo and Sorley cases for the online abuse of feminist campaigner Caroline Criado Perez¹⁸⁵ were clearly justified given the volume of communications, the threatening nature of the communications and the fact that they targeted a specific individual, other cases such as that of Jake Newsome who posted a single offensive message on his Facebook page about the murdered school teacher Ann Maguire¹⁸⁶ are less clear-cut and potentially represent a threat to freedom of expression.

(b) Voyeurism and upskirting

- 2.122 As noted above, the Canadian case *R v DeSilva*¹⁸⁷ 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. 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.

¹⁸¹ *Ibid* at paragraph 30.

¹⁸² See, for example, “Twitter joke trial: Paul Chambers wins high court appeal against conviction” *The Guardian* 27 July 2012 available at <http://www.theguardian.com/law/2012/jul/27/twitter-joke-trial-high-court>; “England and Wales: Court overturns absurd conviction for Twitter joke” *Article 19* 27 July 2012 available at <https://www.article19.org/resources.php/resource/3394/en/england-and-wales:-court-overturns-absurd-conviction-for-twitter-joke>.

¹⁸³ Crown Prosecution Service, *Interim Revised CPS Guidelines on Prosecuting Social Media cases* (3 March 2016) available at http://www.cps.gov.uk/consultations/social_media_consultation_2016.html.

¹⁸⁴ *Ibid*.

¹⁸⁵ “Two jailed for Twitter abuse of feminist campaigner” *The Guardian* 24 January 2014 available at <http://www.theguardian.com/uk-news/2014/jan/24/two-jailed-twitter-abuse-feminist-campaigner>.

¹⁸⁶ “Is it right to jail someone for being offensive on Facebook and Twitter?” *The Guardian* 13 June 2014 available at <http://www.theguardian.com/law/2014/jun/13/jail-someone-for-being-offensive-twitter-facebook>.

¹⁸⁷ 2011 ONCJ 133: see paragraph 2.39 above.

Because of this, in some jurisdictions where voyeurism 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.¹⁸⁸ 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.¹⁸⁹ 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.

- 2.123 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 of section 41B) must not intentionally distribute that image.
- 2.124 The English voyeurism offence does not appear to cover "upskirting" because the definition of "private act" requires "the person's genitals, buttocks or breasts" "to be exposed or covered only in underwear"¹⁹⁰ and upskirting images are usually taken where a person is dressed. Thus, upskirting has instead been prosecuted under the common law offence of outraging public decency.¹⁹¹ However, it has been suggested that this offence is unsuitable as the "fundamental mischief" involved in upskirting "is not creating disgusting sights in public but infringing the dignity of individuals".¹⁹² Gillespie thus

¹⁸⁸ 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.

¹⁸⁹ *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.

¹⁹⁰ Section 68(1) of the *Sexual Offences Act 2003*.

¹⁹¹ See for example *R v Hamilton* [2007] EWCA Crim 2062, [2008] 2 W.L.R. 107; Prosecuting upskirting under the common law offence of outraging public decency has also been discussed by the Law Commission of England and Wales. See Law Commission of England and Wales, *Simplification of Criminal Law: Public Nuisance and Outraging Public Decency* (Law Com No. 358, 2015).

¹⁹² Law Commission of England and Wales, *Simplification of Criminal Law: Public Nuisance and Outraging Public Decency* (Law Com No. 358, 2015) at paragraph 3.109.

suggests that it would be preferable to expand the English voyeurism offence to include “upskirting”,¹⁹³ similar to the case in New Zealand, where offences relating to making intimate visual recordings specifically cover “upskirting”.¹⁹⁴ The New Zealand legislation also applies to the distribution of intimate visual recordings¹⁹⁵ like the Victorian Act discussed above, which again is not covered by the English offence.

- 2.125 The Commission has concluded that the absence of an offence designed to target voyeurism and “upskirting” is a significant gap in the law. This is because where intimate images are taken without consent in a public place, the victim of such activity nonetheless retains a reasonable expectation of privacy, and should be entitled to the same protection as other victims of non-consensual distribution of intimate images. The Commission thus proposes that the criminal law concerning harmful communications should also accommodate “upskirting” and “downblousing” behaviour. This is considered further below.

(c) *Distribution of intimate images offences*

- 2.126 A number of jurisdictions have introduced specific offences designed to target the distribution of intimate images, including the Australian state of Victoria, Canada, England and Wales and Scotland.

(i) *Victoria*

- 2.127 In Victoria, the *Crimes Amendment (Sexual Offences and Other Matters) Act 2014* amended the *Summary Offences Act 1966* to introduce offences relating to the distribution of intimate images in broader circumstances than in the particular context of “upskirting”. The first offence relates to the distribution of an intimate image¹⁹⁶ and is committed where a person “intentionally distributes an intimate image of another person (B) to a person other than B” and “the distribution of the image is contrary to community standards of acceptable conduct”.¹⁹⁷ The Act defines “community standards of acceptable conduct” as including standards of conduct having regard to the following-

- “(a) the nature and content of the image;
- (b) the circumstances in which the image was captured;
- (c) the circumstances in which the image was distributed;

¹⁹³ Gillespie, “‘Up-skirts’ and ‘down blouses’: voyeurism and the law” (2008) *Crim. L.R.* 370 at 382.

¹⁹⁴ Sections 216G-N of the New Zealand *Crimes Act 1961* (as amended by the *Crimes (Intimate Covert Filming) Amendment Act 2006*). Section 216G defines “intimate visual recording” to include recordings of:

“a person’s naked or undergarment-clad genitals, pubic area, buttocks or female breasts which is made:

- (i) from beneath or under a person’s clothing; or
- (ii) through a person’s outer clothing in circumstances where it is unreasonable to do so.”

¹⁹⁵ Sections 216J (prohibition on publishing, importing, exporting or selling intimate visual recording) of the New Zealand *Crimes Act 1961*.

¹⁹⁶ Section 40 of the *Summary Offences Act 1966* (as inserted by the *Crimes Amendment (Sexual Offences and Other Matters) Act 2014*) defines an “intimate image” as:

“a moving or still image that depicts—

- (a) a person engaged in sexual activity; or
- (b) a person in a manner or context that is sexual; or
- (c) the genital or anal region of a person or, in the case of a female, the breasts.”

¹⁹⁷ Section 41 DA of the *Summary Offences Act 1966* (as inserted by the *Crimes Amendment (Sexual Offences and Other Matters) Act 2014*).

- (d) the age, intellectual capacity, vulnerability or other relevant circumstances of a person depicted in the image;
- (e) the degree to which the distribution of the image affects the privacy of a person depicted in the image.”¹⁹⁸

The offence does not apply where B is not a minor and “had expressly or impliedly consented, or could reasonably be considered to have expressly or impliedly consented to the distribution of the image and the manner in which the image was distributed”. The offence carries a maximum sentence of 2 years.

- 2.128 The *Crimes Amendment (Sexual Offences and Other Matters) Act 2014* also inserts an offence of threatening to distribute an intimate image,¹⁹⁹ which has a maximum penalty of one year’s imprisonment. The Canadian and English Acts discussed below do not include a comparable offence, but Scotland enacted a similar offence in its *Abusive Behaviour and Sexual Harm (Scotland) Act 2016*.²⁰⁰ The threat to disclose intimate images could cause almost as significant an amount of distress as disclosure itself, because the speed and ease by which disclosure can be carried out online and its instantly devastating impact mean that the victim is constantly in fear of this occurrence. Thus, there is considerable merit to introducing an offence covering threats of disclosure alongside a distribution of an intimate image offence.

(ii) Canada

- 2.129 The *Protecting Canadians from Online Crime Act 2014* entered into force in March 2015. This Act was introduced partly in response to two very high profile Canadian cases involving teenagers who committed suicide following the release of intimate images.²⁰¹ The Act inserts an offence into section 162.1 of the *Canadian Criminal Code*, which provides that any person who “knowingly publishes, distributes, transmits, sells, makes

¹⁹⁸ Section 40 of the *Summary Offences Act 1966* (as inserted by the *Crimes Amendment (Sexual Offences and Other Matters) Act 2014*).

¹⁹⁹ Section 41 DB of the *Summary Offences Act 1966* (as inserted by the *Crimes Amendment (Sexual Offences and Other Matters) Act 2014*) -

“(1) A person (A) commits an offence if—

(a) A makes a threat to another person (B) to distribute an intimate image of B or of another person (C); and

(b) the distribution of the image would be contrary to community standards of acceptable conduct; and

(c) A intends that B will believe, or believes that B will probably believe, that A will carry out the threat.”

²⁰⁰ The *Abusive Behaviour and Sexual Harm (Scotland) Act 2016* includes an offence under section 2 of “Disclosing, or threatening to disclose, an intimate photograph or film”.

²⁰¹ In 2012, 15 year old Amanda Todd committed suicide after she had been blackmailed into exposing her breasts via webcam. See “Man charged in Netherlands in Amanda Todd suicide case” *BBC News* 18 April 2014 available at <http://www.bbc.co.uk/news/world-europe-27076991>; In 2013, 17 year old Rehtaeh Parsons attempted suicide (and later had her life support machine turned off) after photos were distributed online of a gang rape incident in which she was the victim. See “Rehtaeh Parsons suicide: two charged over photos in cyberbullying case” *The Guardian* 9 August 2013 available at <http://www.theguardian.com/society/2013/aug/09/rehtaeh-parsons-suicide-charged-photos>.

available or advertises an intimate image”²⁰² of another person knowing the person depicted in the image did not consent, or being reckless as to this, is guilty of an offence.

- 2.130 The Act includes a defence, whereby no offence will be committed if the “conduct that forms the subject-matter of the charge serves the public good and does not extend beyond what serves the public good”.²⁰³ For the purposes of this defence, it is a question of law whether the conduct serves the public good and whether there is evidence of this, but it is a question of fact whether the conduct does or does not extend beyond what serves the public good and the motives of the accused are irrelevant in this assessment.²⁰⁴ It is notable that the Canadian offence includes a more substantial maximum penalty of 5 years imprisonment²⁰⁵ compared to the maximum 2 years imprisonment under the Victorian and English offences. The Scottish offence, discussed below, also carries a maximum penalty of 5 years imprisonment.²⁰⁶

(iii) *England and Wales*

- 2.131 In 2015, the England and Wales introduced an offence of “disclosing sexual photographs and films with intent to cause distress” designed to target victim-shaming behaviour (so-called “revenge porn”). This offence is contained in section 33 of the *Criminal Justice and Courts Act 2015* which provides:

“(1) It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made-

- (a) without the consent of an individual who appears in the photograph or film, and
- (b) with the intention of causing that individual distress.

(2) But it is not an offence under this section for the person to disclose the photograph or film to the individual mentioned in subsection 1(a) and (b).”

A number of defences are also included relating to disclosure for the purposes of preventing, detecting or investigating crime,²⁰⁷ disclosure in the course of, or with the view to, the publication of journalistic material where the individual believed this disclosure was or would be in the public interest²⁰⁸ and disclosure where the individual reasonably believed that the material had been previously disclosed for reward.²⁰⁹

- 2.132 In order for the offence to be committed, specific intent to have disclosed the content to cause distress must be proven, as intention to cause distress is not to be taken as being “a

²⁰² Intimate images are defined, under section 162.1(2), 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.”

²⁰³ Section 162.1(3) of the *Canadian Criminal Code*.

²⁰⁴ Section 162.1(4) of the *Canadian Criminal Code*.

²⁰⁵ Section 162.1(1)(b) of the *Canadian Criminal Code*.

²⁰⁶ Section 2(7) of the *Abusive Behaviour and Sexual Harm (Scotland) Act 2016*.

²⁰⁷ Section 33(3) of the *Criminal Justice and Courts Act 2015*.

²⁰⁸ Section 33(4) of the *Criminal Justice and Courts Act 2015*.

²⁰⁹ Section 33(5) of the *Criminal Justice and Courts Act 2015*.

- natural and probable consequence of the disclosure”.²¹⁰ There is no similar requirement in the Canadian and Victorian offences. Thus, individuals and perhaps young people in particular, who disclose this type of content without appreciating the consequences of their behaviour and not intending to cause the victim of the disclosure distress, may be able to escape liability under the English offence. The English offence carries a maximum penalty of 2 years imprisonment or fine or both on conviction on indictment and a maximum penalty of 12 months imprisonment or fine or both for summary conviction.²¹¹
- 2.133 Unlike the Canadian and Victorian offences which apply to “intimate images” the English offence applies to private sexual photographs or films.²¹² However, these terms are defined similarly in each of the Acts. While the Canadian definition of intimate images contains a reasonable expectation of privacy requirement that is not found in the English and Victorian offences, a similar assessment may nevertheless be required under these two offences, as the Victorian offence requires the degree to which the distribution affected the privacy of the person depicted in the image to be taken into account under the “community standards of acceptable conduct” requirement and the English offence requires that the image or film be private, which is defined as something that is not of a kind ordinarily seen in public.
- 2.134 The Victorian, Canadian, English and Scottish (discussed below) offences are all technology neutral and extend equally to offline as well as online disclosure. In the English offence, this is clear from the definition of “discloses”, which is defined in the Act as occurring when a person “by any means” “gives or shows” the material to another person or “makes it available to the person”.²¹³
- 2.135 It is worth noting that the introduction of a specific distribution of intimate images offence has led to an increase in reporting of this type of activity in England and Wales, with over 1,200 cases reported since the law came into effect in April 2015 compared to 149 cases during the two and half years to September 2014.²¹⁴ However, only 11% of reported offences resulted in the alleged perpetrator being charged and in 61% of cases no action was taken against the alleged perpetrator, mainly because of a lack of evidence or because the victim withdrew support.²¹⁵
- 2.136 It has also been suggested that the UK police are struggling to apply the new law correctly, particularly when to charge other offences such as harassment or child

²¹⁰ Section 33(8) of the *Criminal Justice and Courts Act 2015*.

²¹¹ Section 33(9) of the *Criminal Justice and Courts Act 2015*.

²¹² Section 35(3) of the *Criminal Justice and Courts Act 2015*, provides—
“A photograph or film is “sexual” if—

(a) it shows all or part of an individual’s exposed genitals or pubic area,

(b) it shows something that a reasonable person would consider to be sexual because of its nature, or

(c) its content, taken as a whole, is such that a reasonable person would consider it to be sexual.”

²¹³ Section 34(2) of the *Criminal Justice and Courts Act 2015*.

²¹⁴ “Revenge porn: Hundreds of images of children shared on Facebook and Instagram”, *The Independent* 24 January 2016 available at <http://www.independent.co.uk/news/uk/home-news/revenge-porn-hundreds-of-images-of-children-shared-on-facebook-and-instagram-a6830736.html>.

²¹⁵ “Revenge pornography victims as young as 11, investigation finds” *BBC News* 27 April 2016 available at <http://www.bbc.co.uk/news/uk-england-36054273>.

pornography instead of the disclosing sexual images offence.²¹⁶ This has been highlighted by a May 2016 case where a man received a caution for one offence under section 33 of the *Criminal Justice and Courts Act 2015* and three offences of sending a grossly offensive, indecent, obscene or menacing message, despite the fact that he targeted four women and a fifteen year old girl by posting images of them on pornography sites without their consent. Commentators have suggested that the man should have been charged with harassment given the persistent nature of his behaviour and that merely cautioning him was too lenient a response, particularly given that the intimate image offence related to the fifteen year old girl.²¹⁷

- 2.137 The section 33 offence has also been criticised because victims of the offence are not granted privacy when making a complaint when appearing in court.²¹⁸ This may discourage victims from coming forward as it creates a risk that the name and details of the victim could be reported in the press, which could draw greater attention to the images in question and lead to them being shared more widely.²¹⁹

An offence of disclosing private sexual photographs and films with intent to cause distress has also been enacted in Northern Ireland under section 51 of the *Justice Act (Northern Ireland) 2016*. This offence uses the same wording as the offence under section 33 of the *Criminal Justice and Courts Act 2015*; however the maximum sentence on summary conviction is only 6 months under the Northern Ireland offence compared to 12 months under section 33.

(d) Scotland

- 2.138 The *Abusive Behaviour and Sexual Harm (Scotland) Act 2016* was passed in April 2016 and introduced an offence of “disclosing or threatening to disclose an intimate photograph or film”. A person commits this offence if they disclose or threaten to disclose a photograph or film which shows, or appears to show, another person in an intimate situation and the person intends to cause, or is reckless as to whether the other person will be caused, fear, alarm or distress. The photograph or film must not have been disclosed to the public or by the person depicted in the image or with that person’s consent.²²⁰ Although this offence is similar to the offence introduced in England and

²¹⁶ “Police reaction to revenge porn is playing into predators’ hands” *The Guardian* 10 May 2016 available at <http://www.theguardian.com/commentisfree/2016/may/10/police-revenge-porn-cautions-sexual-predators>.

²¹⁷ “Police decision to caution man after uploading revenge porn pictures of 15 year old girl sparks outrage” *The Independent* 9 May 2016 available at <http://www.independent.co.uk/news/uk/crime/police-decision-to-caution-man-after-uploading-revenge-porn-pictures-of-15-year-old-sparks-outrage-a7019971.html>.

²¹⁸ “Call for ‘revenge porn’ victims to be kept anonymous” *BBC News* 15 December 2015 available at <http://www.bbc.co.uk/news/magazine-35042309>.

²¹⁹ *Ibid.*

²²⁰ Section 2(1) of the *Abusive Behaviour and Sexual Harm (Scotland) Act 2016*:

“A person (“A”) commits an offence if—

(a) A discloses, or threatens to disclose, a photograph or film which shows, or appears to show, another person (“B”) in an intimate situation,

(b) by doing so, A intends to cause B fear, alarm or distress or A is reckless as to whether B will be caused fear, alarm or distress, and

Wales, it has a number of features which make it a more comprehensive response to the harm caused by the non-consensual distribution of intimate images.

- 2.139 Firstly, the Scottish offence includes a broader mental element and thus applies not only to cases where the perpetrator intends to cause the victim fear, alarm or distress, but also where the perpetrator is reckless as to this. The mental element also applies to intention to cause or being reckless as to whether the victim will be caused “fear” and “alarm” as well as “distress” and so is wider than the English offence which only applies to intention to cause distress.
- 2.140 As noted above, the Scottish offence also applies to threats to disclose intimate photographs and films. This is an important extension of the offence of distributing intimate images as the threat to disclose an intimate image can be used to control and blackmail the person depicted in the image and thus has the potential to cause as significant distress as the disclosure itself.
- 2.141 Finally, the definitions of “intimate situation”, “film” and “photograph” include a wider range of intimate images than the equivalent definitions in the English legislation. Firstly, the definition of “intimate situation” applies not only to images where the “genitals, buttocks or breasts” are exposed but also where they are “covered only with underwear”.²²¹ This ensures that images depicting individuals dressed only in underwear are covered by the offence including “upskirting” or “downblousing” images, which are usually taken when the person is clothed and wearing underwear. The Scottish offence also applies to photo-shopped images, that is, where part of a person’s image, usually his or her face, is superimposed on to an image of the intimate parts (nude, or partially nude) of another person’s body. The Scottish offence includes such images by providing that the “film” and “photograph” are to be defined to include an image in any form “whether or not the image has been altered in any way”.²²² The English offence also applies to photographs or films which have been altered,²²³ however, section 35(5)(b) provides that a photograph is not private and sexual if “it is only private or sexual by virtue of the alteration”, whereas the Scottish law contains no such limitation.

(e) Conclusion

- 2.142 The general offences that apply to once off online activity in New Zealand and the UK have the advantage of being broad in scope and covering a wide range of communications. However, the breadth of these offences also creates freedom of expression concerns, as the dividing line between communications which are offensive but nevertheless should be permitted (as the right to freedom of expression extends to the protection of offensive speech²²⁴), and those which ought to be criminalised, can be difficult to discern. Thus, any

(c) the photograph or film has not previously been disclosed to the public at large, or any section of the public, by B or with B’s consent.”

²²¹ Section 3(1) of the *Abusive Behaviour and Sexual Harm (Scotland) Act 2016*:

“(1) For the purposes of section 2, a person is in an “intimate situation” if—

(a) the person is engaging or participating in, or present during, an act which—

(i) a reasonable person would consider to be a sexual act, and

(ii) is not of a kind ordinarily done in public, or

(b) the person’s genitals, buttocks or breasts are exposed or covered only with underwear.”

²²² Section 3(2) of the *Abusive Behaviour and Sexual Harm (Scotland) Act 2016*.

²²³ Section 34(5) of the *Criminal Justice and Courts Act 2015*.

²²⁴ See *Handyside v United Kingdom* (1979-1980) 1 EHRR 737.

general offence designed to target once-off activity needs to be drafted with enough specificity to ensure that the right to freedom of expression is safeguarded. The importance of drafting offences which are not overly broad and therefore vulnerable to being found unconstitutional on grounds of vagueness is discussed further below.

- 2.143 The offences introduced in Victoria, Canada, England and Wales and Scotland to target the distribution of intimate images are more specific and apply to behaviour which is clearly deserving of criminalisation. Thus, freedom of expression concerns are less likely to arise in this context. The greater specificity present in these offences also means that they are unlikely to offend the principle of legality. Specific offences targeting the distribution of intimate images also have the advantage of offering explicit recognition to the harm caused by this particularly serious form of online abuse.

(3) Vagueness

- 2.144 When proposing new criminal offences, it is vital to ensure that they fulfil the requirements of the doctrine of legality. Legality requires that criminal offences be clearly defined, that criminal statutes be interpreted strictly and in favour of the accused, that such statutes be promulgated, made reasonably accessible to the public and not be retroactively applied.²²⁵ The vagueness doctrine has been described as the “operational arm” of the legality principle and allows the courts to strike down as unconstitutional offences which are not sufficiently certain.²²⁶
- 2.145 As the criticisms of the New Zealand offence discussed above highlight, vagueness is a particular issue in relation to digital communication offences as these offences are often drafted using subjective terminology which is not clearly defined. The New Zealand offence could be challenged on these grounds and a similar offence introduced in India in 2008 has already been struck down by the Indian Supreme Court on this basis in the case *Shreya Singhal v Union of India*.²²⁷ However, before examining this case in greater detail, it is necessary to look further at the recognition for the principle of legality in Irish law.

(a) *The Principle of Legality and Irish law*

- 2.146 Constitutional recognition for the principle of legality can be found in a number of provisions, in particular, Article 15.5 which prohibits retroactive law making, Article 25 which requires laws to be promulgated by the President, Article 38.1 which requires that no person be tried save in due course of the law and Article 40.4.1 which protects personal liberty. Article 40.1 (equality before the law), Article 15.2.1 (exclusive legislative power vested in the Oireachtas) and Article 40.3 (personal rights) are also relevant to legality.
- 2.147 The leading case on vagueness in this jurisdiction is *King v Attorney General*,²²⁸ where the offence related to loitering with intent contained in section 4 of the *Vagrancy Act 1824* was struck down as unconstitutional. To be convicted of this offence all that was required was for the accused person to be a “suspected person or a reputed thief” frequenting or loitering in one of the places listed in the Act. In striking down the section, Henchy J (delivering the leading judgment in the Supreme Court) stated:

²²⁵ O'Malley, “Common Law Crimes and The Principle of Legality” (1989) 7 ILT 243, at 246.

²²⁶ *Ibid.*

²²⁷ *Shreya Singhal v Union of India* (2015) Writ Petition (Criminal) No. 167 of 2012.

²²⁸ [1981] IR 233.

“In my opinion, the ingredients of the offence and the mode by which its commission may be proved are so arbitrary, so vague, so difficult to rebut, so related to rumour or ill-repute or past conduct, so ambiguous in failing to distinguish between apparent and real behaviour of a criminal nature, so prone to make a man’s lawful occasions become unlawful and criminal by the breadth and arbitrariness of the discretion that is vested in both the prosecutor and the judge, so indiscriminately contrived to mark as criminal conduct committed by one person in certain circumstances when the same conduct, when engaged in by another person in similar circumstances, would be free of the taint of criminality, so out of keeping with the basic concept inherent in our legal system that a man may walk abroad in the secure knowledge that he will not be singled out from his fellow-citizens and branded and punished as a criminal unless it has been established beyond reasonable doubt that he has deviated from a clearly prescribed standard of conduct, and generally so singularly at variance with both the explicit and implicit characteristics and limitations of the criminal law as to the onus of proof and mode of proof, that it is not so much a question of ruling unconstitutional the type of offence we are now considering as identifying the particular constitutional provisions with which such an offence is at variance.”²²⁹

- 2.148 This passage was quoted in *Dokie v DPP*²³⁰ where section 12 of the *Immigration Act 2004* was declared unconstitutional on grounds of vagueness. Section 12 provided “every non-national” to produce a valid passport or equivalent document or registration certification “unless he or she gives a satisfactory explanation of the circumstances which prevent him or her from so doing”²³¹. Contravention of the section constituted an offence. The Court stated that the failure to define “satisfactory explanation” gave rise to vagueness and uncertainty and that the section had considerable potential for arbitrariness in its application by any individual member of An Garda Síochána.²³² Section 12 was found to lack “the clarity necessary to legitimately create a criminal offence”.²³³
- 2.149 In *Douglas v DPP*,²³⁴ the plaintiff had been charged under section 18 of the *Criminal Law (Amendment) Act 1935* with the offences of causing scandal and injuring the morals of the community. In his judgment, Hogan J discussed the vagueness doctrine at length. He emphasised that although legal certainty was a fundamental principle of the criminal law, “absolute precision is not possible” and that “one may therefore have perfectly general laws which can be adapted to new sets of facts within certain defined parameters, provided that the laws themselves articulate clear and objective standards”.²³⁵ Thus, some degree of vagueness is inevitable and a certain amount of flexibility is necessary in the law to enable it to keep pace with changing circumstances.²³⁶
- 2.150 According to the standards set down in *King* and *Dokie*, Hogan J held that the two offences relating to public scandal and injuring the morals of the community were “totally unclear”, as the terms had no defined legal meaning. The offences were “hopelessly vague and

²²⁹ *Ibid* at 257.

²³⁰ [2011] 1 IR 805.

²³¹ Section 12(1) of the *Immigration Act 2004*.

²³² *Ibid* at 818.

²³³ *Ibid* at 819.

²³⁴ [2013] IEHC 343.

²³⁵ *Ibid* at paragraph 26.

²³⁶ *Ibid*.

subjective in character and they intrinsically lend themselves to arbitrary and inconsistent application”.²³⁷ The relevant provisions were therefore “manifestly unconstitutional”.²³⁸ Hogan J adopted a similar approach in *McInerney v DPP*²³⁹ where the “offending modesty” offence contained in section 18 was also struck down for vagueness.

- 2.151 However, a number of more recent decisions appear to signal a slight retreat from the approach taken in *Douglas* and *McInerney* and reflect a more cautious approach to the vagueness doctrine. In *Cox v DPP*²⁴⁰ the offence of “wilfully, openly, lewdly and obscenely” exposure of the “person” with “intent to insult any female” contained in section 4 of the *Vagrancy Act 1824* was challenged on grounds of vagueness. However, McDermott J concluded that *Douglas* and *McInerney* were “entirely distinguishable”²⁴¹ as the terms at issue in this case, including “lewdly and obscenely”, “aptly and clearly qualify the circumstances which attract criminal liability”²⁴² in contrast to the impugned phrases in *Douglas* and *McInerney*.
- 2.152 In *McNamee v DPP*,²⁴³ Humphreys J referred to the surge in vagueness challenges as a “cottage industry”²⁴⁴ and proceeded to voice concern over what he perceived as the “war on vagueness”²⁴⁵. He emphasised that many of the “fundamental concepts on which the criminal law rests are of necessity general and undefined”²⁴⁶ and that to try and attain “extreme specificity” is “at best to simply chase an illusion and at worst, to create huge omissions and anomalies that simply do not arise with the use of more general phrases”²⁴⁷. He also noted that complete specificity “can only be pandered to, not satisfied” as the meaning of words depends on other words and “so on ad infinitum”²⁴⁸. Humphreys J felt that *Douglas* and *McInerney* were exceptional cases dealing with “extremely vague offences reflecting the social mores of 80 years ago” and that they are thus “outlying decisions in a system of criminal justice that is necessarily predicated on general concepts” and furthermore, the fact that a “concept is general does not make it unconstitutionally or unfairly vague”²⁴⁹.
- 2.153 *King, Dokie* and *Douglas* establish that criminal offences must not be vague with the potential to give rise to arbitrary application by members of the Gardaí, prosecutors and judges. Certainty in criminal offences is important to ensure a number of personal rights are upheld, but the key value the legality doctrine protects is the right to personal liberty.²⁵⁰ Where the criminal law is clear and certain, individuals are capable of regulating their conduct to suit its terms. However, vague laws generate uncertainty which may constrain individuals and negatively impact personal liberty. Although *Cox* and

²³⁷ *Ibid* at paragraph 57.

²³⁸ *Ibid* at paragraph 65.

²³⁹ *McInerney v DPP* [2014] IEHC 181.

²⁴⁰ *Cox v DPP* [2015] IEHC 642.

²⁴¹ *Ibid* at paragraph 34.

²⁴² *Ibid* at paragraph 39.

²⁴³ *McNamee v DPP* [2016] IEHC 286.

²⁴⁴ *Ibid* at paragraph 8.

²⁴⁵ *Ibid* at paragraph 12.

²⁴⁶ *Ibid* at paragraph 10.

²⁴⁷ *Ibid* at paragraph 11.

²⁴⁸ *Ibid* at paragraph 13.

²⁴⁹ *Ibid* at paragraph 14.

²⁵⁰ See O'Malley “Common Law Crimes and The Principle of Legality” (1989) 7 ILT 243, at 246.

McNamee underline that absolute precision is impossible and undesirable, criminal offences nonetheless need to contain clear and objective standards. While there are fundamental criminal law concepts which are by necessity only capable of being defined in general terms, this does not mean that all criminal offences should be drafted broadly and that specific definitions of terms which do lend themselves to precision should not be included where it would be desirable to do so.

(b) *Vagueness and digital communications offences*

2.154 As discussed above, the internet has given rise to harmful behaviours which might not be currently covered by the criminal law. This is an issue worldwide with many states responding by introducing new criminal offences to target novel forms of harmful digital communication. Thus, in 2008, India introduced an offence of “sending offensive messages through communication services etc”. However, on 24 March 2015, the Indian Supreme Court in *Shreya Singhal v Union of India*²⁵¹ struck down this offence on a number of grounds including on grounds of vagueness.

2.155 The offence of sending offensive messages through communication service etc” was provided for in section 66A of the *Information Technology Act 2000*.²⁵²

“Any person who sends, by means of a computer resource or a communication device:

(a) any information that is grossly offensive or has menacing character, or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device, or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or mislead the addressee or recipient about the origin of such messages,

shall be punishable with imprisonment for a term which may extend to three years and with fine”

2.156 The Indian Supreme Court cited a number of cases from the US Supreme Court on vagueness along with the leading domestic cases on the issue. Based on the standards articulated in this jurisprudence, the Court concluded that the expressions used in section 66A were “completely open-ended and undefined”.²⁵³ The Court noted that no specific definitions had been provided for any of the expressions used in the section nor did the section state that words and expressions used in the Penal Code would apply to the Act. The Court considered that every expression used in the section was “nebulous in meaning” and subjective, as “what may be offensive to one may not be offensive to another” and what may cause “annoyance and inconvenience to one may not cause annoyance and inconvenience to another”.²⁵⁴ The Court thus felt that there was “no demarcating line” conveyed in any of the expressions used and this rendered the section “unconstitutionally vague”.²⁵⁵

²⁵¹ *Shreya Singhal v Union of India* (2015) Writ Petition (Criminal) No. 167 of 2012.

²⁵² Section 66A was inserted by section 32 of the *Information Technology (Amendment) Act 2008*.

²⁵³ *Shreya Singhal v Union of India* (2015) Writ Petition (Criminal) No. 167 of 2012 at paragraph 69.

²⁵⁴ *Ibid* at paragraph 76.

²⁵⁵ *Ibid*.

- 2.157 The Court also discussed two UK cases, *DPP v Collins*²⁵⁶ and *Chambers v DPP*,²⁵⁷ involving section 127 of the *Communications Act 2003*. Section 127 and section 66A have a shared genealogy, as they both originate from the same UK offence.²⁵⁸ The Indian Supreme Court noted how in both *Collins* and *Chambers*, the lower courts and the appellate courts reached different conclusions, with the dismissal of the charge in *Collins* being reversed on appeal by the House of Lords and the conviction in *Chambers* being overturned by the High Court. The Supreme Court thus stated that the fact that “judicially trained minds” came to “diametrically opposite conclusions on the same set of facts” highlighted that terms such as “grossly offensive” and “menacing” “are so vague that there is no manageable standard by which a person can be said to have committed an offence or not to have committed an offence”.²⁵⁹ The Court concluded that similarly, section 66A contained “absolutely no manageable standard”²⁶⁰ by which to charge a person for an offence and so was unconstitutionally vague.
- 2.158 Although *Singhal* was only the judgment of a two judge bench and a substantial part of the judgment was concerned with examining whether section 66A satisfied the requirements of the Indian constitution, the case is nonetheless of some persuasive value. The *Singhal* case is significant because section 66A closely resembles section 13 of the *Post Office (Amendment) Act 1951* which also relates to sending grossly offensive, obscene, indecent or menacing communications, except that section 13 as it currently stands does not apply to internet communications. Nonetheless, the *Singhal* case could thus cast doubt on the certainty of this offence as well as any other potential offences designed to deal with harmful communications. *Singhal* illustrates the difficulty with offences which use imprecise terms such as “grossly offensive” and “menacing”. Frequently, these terms are not defined in the relevant legislation and so it is left to the courts and those prosecuting these offences to determine the appropriate standard. The variation between the courts in the *Collins* and *Chambers* cases demonstrates the breadth of discretion available to those interpreting such offences and the potential for them to give rise to inconsistent results.
- 2.159 Certain jurisdictions have also introduced civil measures designed to target harmful digital communications which have also been struck down for vagueness. In *Crouch v Snell*,²⁶¹ the Nova Scotian Supreme Court struck down the *Cyber-safety Act 2013* on grounds that it unjustifiably interfered with the rights to freedom of expression and liberty under the Canadian Charter. This Act allowed protection orders to be granted where a subject had engaged in cyber-bullying and “there are reasonable grounds to believe that the respondent will engage in cyberbullying of the subject in the future”²⁶². In particular, the Court held that the definition of cyber-bullying in the Act was overbroad. The Act defined cyber-bullying as follows:

²⁵⁶ (2006) 1 WLR 2223.

²⁵⁷ [2012] EWHC 2157.

²⁵⁸ Section 10(2)(a) of the UK *Post Office (Amendment) Act 1935*, which has been replaced a number of times over the years. The Indian Supreme Court discusses this at footnote 1 of the judgment.

²⁵⁹ *Shreya Singhal v Union of India* (2015) Writ Petition (Criminal) No. 167 of 2012 at paragraph 82.

²⁶⁰ *Ibid.*

²⁶¹ *Crouch v Snell*, 2015 NSSC 340.

²⁶² *Cyber-safety Act 2013*, section 8(b).

“‘cyberbullying’ means any electronic communication through the use of technology including, without limiting the generality of the foregoing, computers, other electronic devices, social networks, text messaging, instant messaging, websites and electronic mail, typically repeated or with continuing effect, that is intended or ought reasonably be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person’s health, emotional well-being, self-esteem or reputation, and includes assisting or encouraging such communication in any way.”²⁶³

- 2.160 The Court held that the Act and this definition in particular amounted to a “colossal failure”²⁶⁴ because of the extent to which it interfered with freedom of expression. The Court found that the Act restricts both public and private communications, provides for no defences and did not require proof of harm. Procedural safeguards such as automatic review of protection orders by a Court and the respondent’s right to request a hearing, were also held to “do nothing to address the fact that the definition of cyberbullying is far too broad, even if a requirement of malice was read in”.²⁶⁵ The Court also concluded that the requirement that “there be reasonable grounds to believe the respondent will engage in cyberbullying in the future” was impermissibly vague as the Act provided no guidance on what kinds of evidence and considerations should be taken into account when making this assessment.²⁶⁶ Certain features under the Act were also held to be arbitrary; in particular, the Act allowed protection orders to be granted *ex parte* and did not limit *ex parte* applications to those cases where the respondent’s identity is not known or easily identifiable.²⁶⁷
- 2.161 The Nova Scotian Act illustrates the difficulty in introducing efficient and robust measures designed to target the wide spectrum of behaviour that can amount to cyber-bullying while maintaining a balance between the right to privacy (including associated rights such as dignity and the right to reputation) and the rights to freedom of expression and liberty. Thus, both the Nova Scotian and Indian examples highlight the challenges of ensuring certainty when legislating for harmful digital communications and the need for legislation to contain expressions capable of clear definition in order to not to fall foul of the vagueness doctrine.

(4) Specific offences to target once-off harmful digital communications

(a) *The offence proposed in the Issues Paper*

- 2.162 The Issues Paper asked whether an interference with a person’s privacy carried out using cyber technology involving 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 rather than the civil law and are more likely to alter their behaviour to avoid its

²⁶³ *Cyber-safety Act 2013*, section 3(1)(b).

²⁶⁴ *Crouch v Snell*, 2015 NSSC 340 at paragraph 165.

²⁶⁵ *Ibid.*

²⁶⁶ *Ibid* at paragraphs 136-137.

²⁶⁷ *Ibid*, paragraphs 155-158.

more serious consequences compared to the civil law. Once-off incidents conducted through digital or online 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.

2.163 Two examples illustrate the type of material in question:

- In 2013, a teenage girl was filmed performing a sex act at a concert. This video was posted on a number of social media sites and subsequently went viral. No charges were brought in this case as the girl made no complaint to the Gardaí.²⁶⁸
- 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 prosecution²⁶⁹

2.164 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*.²⁷⁰ 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.²⁷¹

2.165 The second case would not be an offence under the 1951 Act, were it to be amended to include internet communications, as the content was not “grossly offensive, indecent, obscene or menacing” – it was embarrassing. However, the subject could have attempted to rely on the *Data Protection Acts 1988 and 2003*. The video constitutes personal data under the Acts and the individual who uploaded the video would most likely not have been able to rely on the household exemption given the large audience to whom the video was posted.²⁷² Thus, the subject could have sought removal of the video based on the fact that it was personal data which had not been processed fairly or used for “specified, explicit and legitimate purposes”.²⁷³ Had the data controller failed to take action, the subject could then have made a complaint to the Office of the Data Protection Commissioner who would have sought to resolve the matter amicably before issuing an enforcement notice requiring removal if this did not work.

2.166 The Issues Paper asked whether an offence should be introduced to target serious breaches of privacy that have the capacity to interfere to such a degree with a person’s privacy and reputation that civil remedies alone are an inadequate response and there is no public interest in having the information published. The Issues Paper noted that it would be necessary to ensure in any such offence that the law strike a proper balance

²⁶⁸ “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>.

²⁶⁹ 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/>.

²⁷⁰ Section 5 (producing, distributing etc., child pornography) of the *Child Trafficking and Pornography Act 1998*.

²⁷¹ See paragraphs 2.83-2.88 above.

²⁷² See paragraph 2.107 above.

²⁷³ Section 2(1)(c)(i) of the *Data Protection Act 1988*.

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.

- 2.167 The Issues Paper noted that 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.
- 2.168 Where the seriousness threshold was not met, the Issues Paper emphasised that civil law remedies would remain available for interferences with privacy.²⁷⁴ So, cases such as *Von Hannover v Germany*,²⁷⁵ where 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, would not be covered by the offence. Instead, such cases could lead to a civil remedy as the Court held the plaintiff was entitled to in *Von Hannover*. Thus, individuals would not face prosecution for disseminating content online that, while embarrassing, was not seriously damaging to the victims' reputation or privacy.
- 2.169 The Issues Paper also suggested that if such an offence were to be created, then 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.

²⁷⁴ See Chapter 3.

²⁷⁵ *Von Hannover v Germany* [2004] EMLR 379.

In *Herrity v Associated Newspapers (Ireland) Ltd*,²⁷⁶ 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.

2.170 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. The Issues Paper noted that similarly, an offence designed to target once-off posting of harmful content 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.

2.171 Thus, the Issues Paper proposed that 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.

2.172 The Issues Paper also included a table to illustrate the comparison that may be made between section 10 and the offence proposed in the Issues Paper:

Section 10 of the <i>Non-Fatal Offences Against the Person Act 1997</i>	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

²⁷⁶ *Herrity v Associated Newspapers (Ireland) Ltd* [2009] 1 IR 316. This case is discussed further at paragraph 3.28 below.

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

(b) Consultation responses

- 2.173 The majority of consultees favoured introducing a new offence of a single serious interference with personal privacy. Consultees agreed that the capacity of the internet to replicate content across numerous platforms means that the consequences of a single interference with privacy can be just as devastating as persistent behaviour because the victim is at risk of being constantly re-victimised. 72% of the young people who attended the Commission's consultation in partnership with the Department of Children and Youth Affairs felt that cyber-bullying, even on a once-off basis, should be illegal. Young people emphasised that even a single post of harmful content online "can change somebody's life forever. It's worldwide, can escalate and is there forever". 100% of the participants at the consultation also believed that revenge porn, including on a once-off basis, should be illegal.
- 2.174 However, many consultees disagreed with the offence as formulated in the Issues Paper. A number of consultees believed that the offence should be technology neutral. As one consultee noted, the criminal law has traditionally, but not always, looked to the actions of the defendant and their impact on the victim rather than the tools used to commit the crime. They advocated the same approach here observing, that "invasions of privacy can be devastating for the victim whether they take place online or offline". Thus, this consultee stated that "adopting a technology neutral approach allows law enforcement agencies to focus on the substance of the alleged interference with privacy rather than being fixated on whether or not "cyber technology" was used to commit the wrong" and that "an unhelpful precedent" could be set by treating similar behaviour differently simply because the method used is different. Adopting a technology neutral approach would also be in line with the offences introduced in some of the other jurisdictions discussed above.
- 2.175 Some respondents to the Issues Paper questioned the need for a new offence if section 13 of the *Post Office (Amendment) Act 1951* were amended to include internet communications as recommended in the *Report of the Internet Content Governance Advisory Group*.
- 2.176 Other consultees favoured introducing an offence confined to the publication and distribution of intimate images similar to the Victorian, Canadian, English and Scottish offences discussed above. As one consultee noted in this respect, "due to the severity of the interference with privacy and dignity involved in posting intimate and sexual images online without the consent of the person(s) shown... a separate offence should be created prohibiting this type of conduct, even if it is only a single instance" A number of speakers at the Public Seminar also supported introducing a specific offence to target the

publication and distribution of intimate images rather than the more general offence proposed in the Issues Paper.

- 2.177 Section 10 of *the Non-Fatal Offences Against the Person Act 1997* is limited to persistent behaviour and thus does not cover a single act that seriously interferes with a person's peace and privacy or causes him or her alarm, distress or harm. This gap has become particularly apparent since the advance of digital communication, as the internet enables instant communication to large audiences, often on an anonymous basis. These features of digital communication mean that even a single communication has the capacity to interfere seriously with a person's peace and privacy or cause alarm, distress or harm, particularly as digital or online communications are also difficult to erase completely. Thus, as digital communications are permanent or at least, very difficult to remove, they have a persistent quality similar to the multiple acts which are required for the offence of harassment to be committed and the criminal law arguably should recognise this.
- 2.178 Although a number of other offences can be applied to some forms of harmful once-off digital communications, including the *Post Office (Amendment) Act 1951*, the *Data Protection Acts 1988 and 2003* and the *Criminal Damage Act 1991*, no offence is capable of applying comprehensively and gaps are clearly present in relation to certain behaviour, such as the distribution of intimate images of adults where this is not carried out persistently.
- 2.179 A number of jurisdictions have introduced offences to target harmful once-off digital communications. However, while New Zealand introduced a general offence, most other jurisdictions have opted for specific offences designed to target the distribution of intimate images. This particular crime has been identified as an especially serious form of harmful digital communication which is not covered by Irish legislation unless it satisfies the persistence requirement in section 10. A significant number of consultees also favoured introducing an offence to target this behaviour as opposed to the general offence proposed in the Issues Paper. Many consultees felt that the offence formulated in the Issues Paper was too broad and thus it risks falling foul of the vagueness doctrine. The experiences in India and Nova Scotia highlight the challenges of introducing measures designed to target digital communications while safeguarding freedom of expression and ensuring the doctrine of legality is respected.
- 2.180 Therefore, while most consultees supported introducing an offence to target once-off harmful digital communications, many felt the offence as presented in the Issues Paper was too broad and advocated targeted offences instead. Consultees agreed that the publication and distribution of intimate images, particularly online, constitutes a serious interference with the right to privacy that should be criminalised. Furthermore, a clear gap exists in our criminal law in relation to this behaviour when it is not carried out persistently.

(c) *Offence of distributing a threatening false, indecent or obscene message*

- 2.181 As noted above, section 13 of *the Post Office (Amendment) Act 1951* is outdated, and while the Internet Content Governance Advisory Group recommended that it be amended to include internet communications, the Commission considers that more significant reform of this offence is required. A modernised version of section 13 should extend to digital communications but also use clearer terms than those currently found in the section, some of which are potentially vague.

- 2.182 Thus, the Commission recommends that section 13 be repealed and replaced with a new offence designed to apply to all forms of communication including messages distributed online through social media, and that this should include not only messages to a person but also about a person. This new offence would be committed where a person intentionally or recklessly for the purpose of causing alarm, distress or harm, by any means of communication distributes or publishes a threatening, false, indecent or obscene message to or about another person or distributes or publishes such a message persistently. This is broadly based on the factors in section 13 of the 1951 Act, but the wording has been aligned with the “harm” test in section 10 of the *Non-Fatal Offences Against the Person Act 1997*.
- 2.183 The new offence of distributing a threatening, false, indecent or obscene message reflects section 13 of the 1951 Act in that one act is sufficient for the offence to be committed. The offence also reflects section 13 of the 1951 Act by being capable of applying to persistent acts, and can thus be compared with the restated harassment offence and the new stalking offence.
- 2.184 This new offence thus amends the wording of section 13 by omitting the word “grossly offensive” and replacing “menacing” with “threatening” as these terms (“grossly offensive” and “menacing”) could be vulnerable to constitutional challenge on grounds of vagueness. The Commission considers that the other terms used in the offence are also sufficiently clear. A constitutional challenge to the phrase “gross indecency” was rejected in *PP v DPP*,²⁷⁷ in which the High Court (Moriarty J) stated that the term “is neither susceptible to nor requires a discursive definition” and that “the inherent problems of formulating a precise and comprehensive definition of gross indecency, taking into account changes in social attitudes and the multiplicity of situations of potential relevance that could arise, are such that it was not incumbent upon legislatures to devise such a definition.”²⁷⁸ At the time of writing (September 2016), this decision is under appeal. A suggestion that “obscene” was a constitutionally vague term was also rejected in *Cox v DPP*, discussed above.²⁷⁹
- 2.185 The Commission considers that the penalties for this offence should be the same as currently apply under section 10 of the 1997 Act: on summary conviction a Class A fine and/or a maximum of 12 months imprisonment; and on conviction on indictment, an unlimited fine and/or a maximum of 7 years imprisonment.
- 2.186 Section 13 of the 1951 Act includes a provision whereby on conviction of an offence under the section, “the court may in addition to any other penalty imposed for the offence, order any apparatus, equipment or other thing used in the course of committing the offence to be forfeited to the State.”²⁸⁰ The Commission has concluded that provision for such forfeiture should apply to all harmful communications offences included in the Report.

2.187 The Commission recommends that section 13 of the *Post Office (Amendment) Act 1951* be repealed and replaced with an offence of distributing a threatening, false,

²⁷⁷ *PP v DPP*, High Court, October 2015.

²⁷⁸ *Ibid*, paragraph 38.

²⁷⁹ *Cox v DPP* [2015] IEHC 642; see paragraph 2.152.

²⁸⁰ Section 13(4) of the *Post Office (Amendment) Act 1951*.

indecent or obscene message by any means of communication and with the intent to cause alarm, distress or harm or being reckless as to this.

- 2.188 The Commission recommends that the provision for forfeiture of any apparatus, equipment or other thing under section 13 of the *Post Office (Amendment) Act 1951* should apply to all harmful communications offences included in the Report.

(d) *Distribution of intimate images offences*

- 2.189 While the offence of distributing a threatening, false, grossly indecent or obscene message would extend to most harmful once-off digital communications, the Commission nonetheless considers that specific offences designed to target the distribution of intimate images are required. In this respect, there are two different situations which may necessitate separate responses.

(i) *Distribution of intimate image without consent, or threatening to do so, with intent to cause harm*

- 2.190 Firstly, there are cases involving disclosure of intimate images with the intention of causing distress. These are the so-called “revenge porn” cases where an individual posts or otherwise distributes intimate content such as photos or videos with the intention of causing the victim harm. This is very serious behaviour which certain jurisdictions, notably England and Wales, have specifically legislated against. The Commission considers that an offence should also be introduced in Ireland to respond to such behaviour.

- 2.191 Thus, the Commission recommends that an offence be introduced to target the distribution or publication, by any means, of an intimate image without the consent of the person depicted in the image. This offence should also extend to threats to publish or distribute an intimate image. This offence would be committed where by publishing or distributing the intimate image or threatening to do so, the perpetrator intentionally or recklessly seriously interferes with that person’s peace or privacy or causes alarm distress or harm to the person depicted in the image and a reasonable person would realise that the publication or distribution of the image would seriously interfere with the peace and privacy of the person depicted in the image or cause them alarm, distress or harm. Thus, the essential ingredients of the offence would mirror those presently found in section 10 of the *Non-Fatal Offences Against the Person Act 1997* except that this offence would not require persistence and could involve a once-off act.

- 2.192 The Commission recommends that the penalties for this offence be the same as those for harassment: (a) on summary conviction a Class A fine (a fine of up to €5,000) and/or up to 12 months imprisonment for a term not exceeding; and (b) on conviction on indictment an unlimited fine and/or to up to 7 years imprisonment.

(ii) *Taking or distributing an intimate image without consent*

- 2.193 However, not all cases of intimate image distribution involve intention to cause distress. Sometimes, such content is shared spontaneously or without considering the impact on the victim, especially in the case of young people, or is re-distributed by third parties. These cases may not be capable of being prosecuted under the offence recommended above because the intent to cause alarm, distress or harm element may not be present.

- 2.194 The Commission therefore recommends that a separate offence be introduced to target the non-consensual taking and distribution of intimate images, by any means of communication, without intent to cause alarm, distress or harm. This offence is aimed at behaviour that falls short of the intentional, egregious, activity associated with the shaming offence sometimes referred to as “revenge porn” that would be dealt with through the offence involving the distribution of intimate images without consent or threatening to do so with the intent to cause harm. The offence of taking or distributing an intimate image without consent may, in some respects, be thought of as being associated with the behaviour known as “sexting” but it differs in a fundamental way in that it is committed only where the intimate image is taken without consent. It remains a separate question, which is outside the scope of the criminal law, as to whether it is appropriate or suitable for persons, whether young persons or adults, to distribute intimate images. Applying the principle of proportionality discussed in Chapter 1, above, this might more appropriately be considered in the non-criminal context of the guidance that could be developed to promote positive digital citizenship, under the auspices of the proposed Digital Safety Commissioner, which the Commission discusses in Chapter 3, below.
- 2.195 Similar to the offence relating to the distribution of intimate images with intent to cause harm, the offence of taking or distributing an intimate image without consent would share some of the ingredients of the harassment offence under section 10 of the 1997 Act, namely, that the accused by his or her acts seriously interferes with the other person’s peace and privacy or causes alarm, distress or harm to the other person. However, the offence of taking or distributing an intimate image without consent would differ in an important respect from harassment by not requiring that the accused has acted either intentionally or recklessly: the offence would be committed simply by the taking, distributing or publishing of an intimate image without consent. It is therefore a strict liability offence, and for this reason the Commission proposes that it be a summary offence only, with maximum penalties of a Class A fine and/or up to 6 months imprisonment. The offence would also differ from harassment by not requiring persistence.

(iii) Consent

- 2.196 A key element of both of the intimate images offences is that the taking, distribution or publication of the intimate image is done without the consent of the victim. The Commission considers that a definition of consent should be set out for the purposes of the intimate images offences.
- 2.197 The primary purpose of the intimate image distribution offences included in this Report is to protect against harmful interferences with privacy and therefore these offences are not sexual offences as such. However, because these offences involve issues of great intimacy the general concept of consent that applies in sexual offences should apply to them.
- 2.198 In its 1988 *Report on Rape and Allied Offences*, the Commission recommended that “consent” be defined in legislation and that it mean “a consent freely and voluntarily given” and, that consent is “not freely and voluntarily given if it is obtained by force, threat,

intimidation, deception or fraudulent means”.²⁸¹ This type of definition of consent, based around the concepts of freedom and choice, was adopted in section 74 of the English *Sexual Offences Act 2003* and Article 3 of the *Sexual Offences (Northern Ireland) Order 2008*. These provisions are worded identically and provide that a person consents “if he agrees by choice, and has the freedom and capacity to make that choice.”²⁸² This approach to consent was also followed by the Commission in its *Report on Sexual Offences and Capacity to Consent*.²⁸³

- 2.199 The Commission thus recommends that the definition of consent applicable to the offence of distributing an intimate image without consent with intent to cause harm and the offence of taking or distributing an intimate image without consent should be that a person agrees by choice and that the person has the freedom and capacity to make that choice.

(iv) Definition of “intimate image”

- 2.200 The Commission recommends adopting a definition of “intimate image” based on the definition of “intimate image” inserted into the *Canadian Criminal Code* under the *Protecting Canadians from Online Crime Act 2014*.²⁸⁴ This definition would apply to visual recordings made by any means including a photographic, film or video recording in which the person depicted is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in sexual activity.
- 2.201 However, the Commission proposes that images depicting a person’s genital or anal region, or in the case of a female, her breasts, where the genital or anal region or breasts are covered by underwear, should also be included in the definition of “intimate image” as this would ensure that “upskirting” and “downblousing” images, which do not involve nudity, are covered.
- 2.202 The Commission also recommends that photo-shopped images, where part of a person’s image, usually his or her face, is superimposed on the intimate parts (nude, or partially nude) of another person’s body, should also be covered by intimate image offences. Therefore, the definition of intimate image included in the Report applies to a photographic, film or video recording “whether or not the image of the person has been altered in any way”. This wording is derived from the definitions of “film” and “photograph” in the *Abusive Behaviour and Sexual Harm (Scotland) Act 2016*.
- 2.203 The visual recording would also have to be made in circumstances that gave rise to a reasonable expectation of privacy at the time of the recording and where this reasonable expectation of privacy is retained at the time the image is communicated. However, the circumstances that gave rise to a reasonable expectation of privacy at the time of the recording can include that the recording was made when the person was in a public place. Extending the reasonable expectation of privacy requirement to public places again ensures that voyeuristic intimate images taken in public are captured.

²⁸¹ Law Reform Commission, *Report on Rape and Allied Offences* (LRC 24-1988) at paragraph 17.

²⁸² For further discussion of the law of consent in Ireland and in other countries see Law Reform Commission, *Report on Sexual Offences and Capacity to Consent* (LRC 109-2013) at paragraphs 2.04-2.22.

²⁸³ Law Reform Commission, *Report on Sexual Offences and Capacity to Consent* (LRC 109-2013).

²⁸⁴ Section 162.1(2) of the *Canadian Criminal Code*.

- 2.204 The Commission recommends the enactment of an indictable offence of distributing an intimate image without the consent of the person depicted in the image, or threatening to do so, and with the intent to cause alarm, distress or harm or being reckless as to this.
- 2.205 The Commission recommends the enactment of a summary, strict liability offence of taking or distributing an intimate image of another person without the other person's consent.
- 2.206 The Commission recommends that the definition of "consent" applicable to the intimate images offences should be that a person agrees by choice and that the person has the freedom and capacity to make that choice.
- 2.207 The Commission recommends "intimate image" should be defined as a visual recording of a person made by any means including a photographic, film or video recording: (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, and (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 image is communicated.
- 2.208 The Commission recommends that the definition of "intimate image" should also include what has been described as "upskirting" and "downblousing", that is, an image of the person's genital or anal region or in the case of a female of her breasts, whether the genital or anal region or, as the case may be, the breasts were covered by underwear or were bare.
- 2.209 The Commission recommends that the definition of "intimate image" should include "photo-shopping," that is, where part of a person's image, usually his or her face, is superimposed on to an image of the intimate parts (nude, or partially nude) of another person's body, so that the definition should apply to a photographic, film or video recording, whether or not the image of the person has been altered in any way.

E Procedural Issues and Harmful Digital Communications

- 2.210 The Commission now turns to address a number of procedural issues that arise in the context of the harmful communication offences at issue in this Report: protecting the privacy of persons affected by harmful communications; protective measures to deal with prosecutions of persons under 17; and time limits for summary prosecutions.

(1) Protection for privacy of person to whom offence relates

- 2.211 As noted above,²⁸⁵ section 33 of the *Criminal Justice and Courts Act 2015*, which deals with the victim shaming offence, so called "revenge porn", has been criticised for not providing victims of the offence with protection of their privacy when appearing in court. The Commission considers this to be a significant problem, because the publicity generated by court proceedings clearly has the potential to discourage victims from reporting such offences for fear of drawing more attention to the intimate images.

²⁸⁵ See paragraph 2.137.

- 2.212 Therefore, the Commission recommends that in any prosecution for a harmful communications offence provided for in the Report, the privacy of the person to whom the offence is alleged to have been committed should be protected. Allowing the privacy of the person to whom the relevant offence relates to be protected may encourage greater reporting of such offences, particularly the offences related to the distribution of intimate images where fear, shame and humiliation may prevent victims from coming forward.²⁸⁶ Protecting the privacy of victims of intimate image offences would also help in reducing the likelihood of such content going viral and therefore would reduce the harm caused to victims.²⁸⁷
- 2.213 The Commission recommends that the privacy protection should, in general, mirror the reporting restrictions that protect the privacy of a person in existing legislation. These restrictions should be broadly modelled on section 7 of the *Criminal Law (Rape) Act 1981* (as amended) which relates to anonymity for complainants and provides that, in general, no matter likely to lead members of the public to identify any person as a person in relation to whom the offence is alleged to have been committed shall be published in a publication available to the public or broadcast, except as authorised by a direction given under the section. As in section 7 of the 1981 Act, the Commission recommends that the accused should be able to apply to court for a direction to have the reporting restrictions removed and that the court must give such a direction if satisfied (a) that the direction is required for the purpose of inducing persons to come forward who are likely to be needed as witnesses at the trial, and (b) that the conduct of the applicant's defence at the trial is likely to be adversely affected if the direction is not given.
- 2.214 However, the Commission also considers that provision should be made for waiver of the ban on reporting by the person to whom the offence relates. This is not provided for in the 1981 Act, and allowing such a waiver reflects the Commission's view that while the harmful communication offences discussed in this Report often involve intimate matters, including intimate images, they are not, as such, sexual offences.

2.215 The Commission recommends that in any prosecution for a harmful communications offence provided for in the Report, the privacy of the person to whom the offence relates should be protected, broadly by analogy with comparable provisions as to reporting restrictions in existing legislation (including their modification or removal), as well as providing for waiver by the person to whom the offence relates.

(2) Consent of Director of Public Prosecutions in prosecution of person under 17

- 2.216 In accordance with the proportionality principle discussed in Chapter 1, the Commission considers that it would not be consistent with that principle, and it would be highly undesirable, to apply the criminal law to children and young persons under the age of 17 years in the way that the criminal law applies to adults. This is especially the case in the context of the communications at issue in this Report, where some online and digital behaviour of children and young people may arise from their inherent immaturity and

²⁸⁶ Prof. Clare McGlynn, Centre for Gender Equal Media, Briefing on *Anonymity for Complainants of Image-Based Sexual Abuse: focus on harms to victims, not motives of perpetrators* (July 2016) at 2 available at <https://claremcglynn.files.wordpress.com/2016/07/mcglynn-anonymity-revenge-porn-11-july-2016.pdf>.

²⁸⁷ *Ibid* at 2.

where there may be little or no intention to cause serious harm or distress. As also discussed in Chapter 1, it is vital that suitable preventative responses, such as education and empowerment, form a key aspect of national policy to deal with harmful communications by children and young people, including through the promotion of good digital citizenship under the auspices of the proposed Digital Safety Commissioner, discussed in Chapter 3, below. Nonetheless, where appropriate, the criminal law should be applied to persons under the age of 17. In this respect, it is important to note that the *Children Act 2001*, as amended, provides that, in general, the criminal justice process should be seen as a last resort for children and young persons, and only after other responses, such as the diversion programmes provided for in the 2001 Act, have been applied.

- 2.217 This project has not involved a detailed analysis of the suitability or otherwise of the diversion arrangements in the 2001 Act to the harmful communications offences dealt with in this Report. It is sufficient to note, however, that this would require consideration by all the relevant State agencies of their suitability at an operational level, including relevant constitutional and international standards that are relevant.²⁸⁸ The Commission considers that, since this project has not involved a detailed review of the 2001 Act, it should confine itself to recommending that no prosecution for the harmful communications offences discussed in the Report should be brought against persons under the age of 17 years except by or with the consent of the Director of Public Prosecutions. This reflects the position in the *Criminal Law (Sexual Offences) Bill 2015*, discussed above, where the offences relating to use of information and communications technology to facilitate the sexual exploitation of a child or to send sexually explicit material to a child cannot be prosecuted without the consent of the DPP where the defendant is under the age of 17 years. Again, as noted above, while the harmful communication offences in this Report are not, as such, sexual offences, the Commission considers that the protection in the 2015 Bill is also suitable for these offences bearing in mind the sensitive and intimate issues that often arise in them. In addition, the Commission is conscious that any decision to prosecute, or not to prosecute, will have been made by the DPP against the general background of the operational development and consideration of suitable diversion arrangements under the 2001 Act for the offences discussed in this Report.

2.218 The Commission recommends that no prosecution for the harmful communications offences discussed in the Report should be brought against persons under the age of 17 years except by or with the consent of the Director of Public Prosecutions.

(3) Time limits for summary prosecutions

- 2.219 The Commission has considered whether the general 6 month time limit for prosecuting summarily, provided for in section 10(4) of the *Petty Sessions (Ireland) Act 1851*, should be extended for harmful communications offences. The Oireachtas has enacted many specific exceptions to the general 6 month time limit. This includes a number of 2 year time limits for summary prosecutions: see for example section 22(2) of the *Animal*

²⁸⁸ For a critique of the diversion arrangements in the 2001 Act by reference to relevant constitutional and international standards, see Kilkelly, "Policing, Young People, Diversion and Accountability in Ireland" (2011) 55(2) *Crime Law and Social Change* 133-151.

Remedies Act 1993, section 32(3) of the *Employment Permits Act 2006*, section 76 of the *Consumer Protection Act 2007* and section 4 of the *Competition and Consumer Protection Act 2014*. A 3 year time limit for summary prosecutions is provided for in section 55 of the *Central Bank (Supervision and Enforcement) Act 2013* and in section 867 of the *Companies Act 2014*.

- 2.220 Frequently, cases involving harmful digital communications require evidence to be obtained from websites with servers located outside the jurisdiction. Such content can only be obtained through the use of the Mutual Legal Assistance Treaty procedure²⁸⁹ which the Commission understands from its consultative process can take up to 18 months to be completed. This is a significant problem in summary proceedings because the 6 month time limit will have expired before the relevant content has been received. Thus, extending this time limit for harmful communications offences would ensure that summary prosecutions for such offences will not be prevented by a restrictive time limit. The Commission has concluded that a 2 year time limit would be suitable in this respect. No specific time limit applies to prosecutions on indictment.

2.221 The Commission recommends that the general 6 month time limit for prosecuting summarily, provided for in section 10(4) of the *Petty Sessions Ireland Act 1851*, should be extended to 2 years for the harmful communications offences in the Report.

F Jurisdictional Issues and Harmful Communications: Extra-territorial Effect

- 2.222 The Commission turns to consider the extent to which harmful digital communications offences should have extra-territorial effect.²⁹⁰ The internet is not confined to “a single geographical area nor is it neatly divisible along territorial boundaries into distinct local networks.”²⁹¹ People may be subject to harmful communications from perpetrators, or through sites, located outside the State and, conversely, perpetrators based in the State may post harmful communications to or concerning individuals based outside it. 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.²⁹²
- 2.223 The general principle is that criminal jurisdiction is territorial, meaning that it is limited to offences committed within the territory of the State regardless of the nationality or domicile of the accused person.²⁹³ Murder and manslaughter are an exception to this general rule, with section 9 of the *Offences Against the Person Act 1861* (as amended by

²⁸⁹ This procedure is provided for under the *Criminal Justice (Mutual Assistance) Act 2008* which implements a number of international agreements between the State and other states relating to mutual assistance in criminal matters.

²⁹⁰ Similar considerations arise in the context of civil remedies, which are discussed in Chapter 3.

²⁹¹ Biswas “Criminal liability for cyber defamation: jurisdictional challenges and related issues from Indian jurisprudence” (2013) CLTR 121, at 125.

²⁹² 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 2.254 below.

²⁹³ Charleton, McDermott and Bolger, *Criminal Law* (Butterworths, 1999), paragraph 1.175.

the *Criminal Law Act 1997*) providing that Irish courts have jurisdiction over murder and manslaughter committed outside of Ireland where the accused is an Irish citizen. Article 29.8 of the Constitution also provides that the State may legislate with extra-territorial effect, which must be done expressly.

- 2.224 The majority of respondents to the Issues Paper felt that section 10 of the 1997 Act should be amended to have extra-territorial effect. Consultees emphasised the worldwide nature of the internet, suggesting that the location of an individual at the time of an incidence of harassment should not negate the protections which could be afforded to a victim.
- 2.225 However, many of the consultees were doubtful whether an amendment to the harassment offence to provide for extra-territorial effect would be effective in practice. A number of internet intermediaries noted the “disparate views” on what constitutes free speech in different jurisdictions and the difficulties extra-territoriality would present for them in “navigating these conflicting legal rules”. One internet intermediary suggested that if section 10 were to be amended to have extra-territorial effect then the “relevant connecting factors have to be laid down in a very clear fashion so that one can easily work out whether or not Irish law applies”, to ensure clarity and enable intermediaries to assess whether or not a particular piece of reported content could fall within the scope of the offence.
- 2.226 One consultee felt that the amendment would be “without meaningful purpose” as it would be difficult to ensure that the defendant is present for trial. They stated that extradition would be “inappropriate” in such cases as most online harassment cases will be tried summarily, and that the only alternative to extradition is trial in absentia, which aside from the human rights concerns it raises, would be meaningless without the ability to impose sanctions.
- 2.227 Therefore, if the harmful communications offences discussed in this Report were provided with extra-territorial effect, it would be essential that there be a connection to the State before jurisdiction could be exercised so that the State would be in a position to take action on the basis that it had a real interest.
- 2.228 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*²⁹⁴ an offence of criminal damage to data²⁹⁵ 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 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

²⁹⁴ 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.”

²⁹⁵ The offences under the 1991 Act are discussed at paragraphs 2.90-2.97 above.

pornography),²⁹⁶ he or she can be prosecuted in the State for such a scheduled or specified offence.²⁹⁷

- 2.229 The *Criminal Justice (Offences Relating to Information Systems) Bill 2016*, which proposes to implement the 2013 EU Directive on Attacks on Information Systems,²⁹⁸ and which therefore deals with offences comparable to those under consideration in this Report, includes a provision on extra-territoriality which may provide a helpful model for extra-territorial jurisdiction in the context of harmful communications. Under section 10 of this Bill, which proposes to implement the extra-territorial requirements in Article 12 of the 2013 Directive, jurisdiction is extended for offences under the Bill to persons within the State who commit an offence in relation to an information system outside the State²⁹⁹ and persons outside the State who commit an offence in relation to an information system in the State.³⁰⁰ The 2016 Bill also extends to Irish citizens, persons ordinarily resident in the State, a body corporate established under the law of the State and companies formed and registered or otherwise provided for under the *Companies Act 2014*, who commit an offence outside the State in relation to an information system outside the State where the act is also an offence under the law of the place where the act was committed.³⁰¹
- 2.230 It may be argued that, in the specific context of harmful internet behaviour, the extension of harmful communications offences 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. On the other hand, if an analogy is made with the *Sexual Offences (Jurisdiction) Act 1996*, it may well be that some scheduled sexual offences in the 1996 Act are not offences when committed in some other states. In both instances, therefore, a problem may only arise if the accused remains and an extradition (or European Arrest Warrant) request is made (which may be refused if the requested State does not have a similar offence and operates a rule of specialty).
- 2.231 Thus, in the context of the offences dealt with in this Report extra-territorial jurisdiction should be limited to these situations:
- where a harmful communications offence is committed by a person in the State in relation to a means of communication that is located outside the State,
 - where a harmful communications offence is committed by a person outside the State in relation to a means of communication located in the State or
 - where a harmful communications offence is committed by a person outside the State if the person is an Irish citizen, a person ordinarily resident in the State, an undertaking established under the law of the State, a company formed and registered under the *Companies Act 2014* or an existing company within the meaning of the

²⁹⁶ 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*.

²⁹⁷ Section 2(1) of the *Sexual Offences (Jurisdiction) Act 1996*.

²⁹⁸ Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

²⁹⁹ Section 10(1)(a) of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

³⁰⁰ Section 10(1)(b) of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

³⁰¹ Section 10(1)(c) of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

Companies Act 2014 and the offence is an offence under the law of the place where the act was committed.

- 2.232 It is undesirable that crimes be created which are not prosecutable in practice and the Commission does not wish to propose one. Therefore the harmful communications offences discussed in this Report should have extra-territorial effect but only in the three instances listed above.

- 2.233 **The Commission recommends that extra-territorial effect should apply to the harmful communication offences in the Report:**
- where a harmful communications offence is committed by a person in the State in relation to a means of communication located outside the State,
 - where a harmful communications offence is committed by a person outside the State in relation to a means of communication located in the State or
 - where a harmful communications offence is committed by a person outside the State if the person is an Irish citizen, a person ordinarily resident in the State, an undertaking established under the law of the State, a company formed and registered under the *Companies Act 2014* or an existing company within the meaning of the *Companies Act 2014* and the offence is an offence under the law of the place where the act was committed.

G Penalties on conviction for offences

- 2.234 In the Issues Paper, the Commission sought views on the appropriate maximum sentences that should apply to offences relating to harmful digital communications.
- 2.235 This issue arose in part against the background of some high-profile prosecutions in England in connection with internet “trolling”, which had involved the offence of sending communications with intent to cause distress or anxiety under the *Malicious Communications Act 1988*. At the time, this offence carries a maximum sentence of 6 months on conviction on indictment. In the aftermath of these prosecutions, this was increased under section 32 of the UK *Criminal Justice and Courts Act 2015* to 2 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 5 years.
- 2.236 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.³⁰² This recommendation was supported by the Department of Justice in its 2014 Strategic Review of Penal Policy.³⁰³ 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

³⁰² Law Reform Commission *Report on Mandatory Sentences* (LRC 108-2013) at paragraph 4.237.

³⁰³ *Strategic Review of Penal Policy Final Report* (Department of Justice and Equality, 2014) at 98.

constrain the ability of the courts to punish offenders on an individualised basis.³⁰⁴ Low level offenders are also disproportionately affected by presumptive minimum sentencing.³⁰⁵

- 2.237 The table below sets out the penalties under the current legislative provisions that apply to offences related to harmful digital communications.

Offence	Section	Penalties
<i>S. 10 Non-Fatal Offences Against the Person Act 1997</i>	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.
<i>S. 13(1) Post Office (Amendment) Act 1951, as amended by Communications Regulation (Amendment) Act 2007</i>	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.
<i>Ss. 2(1) and 5 Criminal Damage Act 1991</i>	s. 2(5) s. 5(1)	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

³⁰⁴ The Commission recommended that these regimes be repealed. See Law Reform Commission *Report on Mandatory Sentences* (LRC 108-2013), paragraph 4.238.

³⁰⁵ *Ibid*, paragraph 4.226.

		<p>both.</p> <p>Summary conviction: Class D fine (fine not exceeding €1000) or imprisonment for a term not exceeding 3 months or both</p>
S. 10(9) <i>Data Protection Act 1988</i> , as amended by <i>Data Protection (Amendment) Act 2003</i>	s. 31	<p>Summary conviction: Class B fine (fine not exceeding €4,000).</p> <p>Conviction on indictment: fine not exceeding €100,000.</p>
S. 2 <i>Prohibition of Incitement to Hatred Act 1989</i>	s. 6	<p>Summary conviction: Class C fine (fine not exceeding €2,500) or imprisonment for a term not exceeding 6 months, or both.</p> <p>Conviction on indictment: fine not exceeding €25,400 or imprisonment for a term not exceeding 2 years, or both.</p>
S. 6 <i>Criminal Justice (Public Order) Act 1994</i>	s. 6(2)	<p>Summary conviction: Class D fine (fine not exceeding €1000) or imprisonment for a term not exceeding 3 months, or both.</p>

- 2.238 Although there have been a limited number of prosecutions for harmful digital communications offences, a preference for suspended sentences and fines rather than custodial sentences can nonetheless be observed. Thus, in cases involving convictions for harassment involving digital or online means 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.³⁰⁶ 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.³⁰⁷ The man was sentenced to six months 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 €600.³⁰⁸
- In a 2014 case, a man pleaded guilty under section 10 after posting explicit items on a website about the victim.³⁰⁹ 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.

- 2.239 The majority of consultees considered that the penalties under section 10 of the 1997 Act are sufficient. However, it was suggested that certain factors should be treated as aggravating factors when sentencing under section 10 including whether the victim is a vulnerable person, a child under 18 or a person of mental disability and the extent to which content is disseminated online.
- 2.240 However, while most consultees considered the penalties under section 10 adequate, penalties applying to certain other offences were highlighted as being potentially inadequate. In particular, the lack of any prison sentence under the *Data Protection Acts 1988 and 2003* was noted, which consultees argued may not reflect the seriousness of the offence. It was also suggested that the hacking offence under section 5 of the *Criminal Damage Act 1991* should be made an indictable offence. However, should the *Criminal Justice (Offences Relating to Information Systems) Bill 2016* be enacted, section 5 of the 1991 Act will be replaced with indictable offences, which would carry up to 5 years imprisonment on conviction on indictment.³¹⁰

³⁰⁶ This case is discussed in Shannon *Sixth Report of the Special Rapporteur on Child Protection* (Report submitted to the Oireachtas, January 2013) at 95.

³⁰⁷ “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>.

³⁰⁸ “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

³⁰⁹ “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>.

³¹⁰ Section 8 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016* provides that offences under sections 2, 4, 5 and 6 of the Bill would carry maximum sentences of 5 years for conviction on indictment while the offence under section 3 (interference with information system

- 2.241 Consultees expressed concern over the use of suspended sentences in this area, with one consultee remarking that suspended sentences may appear “inappropriate to victims who have had their privacy invaded, reputation destroyed or safety and wellbeing put at risk”.
- 2.242 The Commission considers that the maximum penalties for the harassment offence under section 10 of the *Non-Fatal Offences Against the Person Act 1997* are sufficient and provide a suitable upper level for penalties that should apply for other intent based harmful communications offences. The Commission therefore recommends that intent based offences discussed in this Report should carry maximum penalties of a Class A fine (fine not exceeding €5,000) or imprisonment for a term not exceeding 12 months or both on summary conviction and a fine or imprisonment for a term not exceeding 7 years or both on conviction on indictment. These penalties reflect the Commission’s view that a once-off act can have as serious consequences as persistent behaviour, particularly in the online context, and so the relevant maximum penalties for all three of these offences should be the same.
- 2.243 The Commission recommends that the offence of taking or distributing an intimate image without consent should be a summary offence only, with maximum penalties of a Class A fine and/or 6 months imprisonment.

2.244 **The Commission recommends, because the maximum penalties for the harassment offence in section 10 of the *Non-Fatal Offences Against the Person Act 1997* are sufficient and provide a suitable upper level for penalties, these penalties should apply to all comparable indictable harmful communications offences provided for in the Report. The Commission also recommends that the offence of taking or distributing an intimate image without consent should be a summary offence only, with maximum penalties on conviction of a Class A fine and/or 6 months imprisonment.**

H Hate Crime and Harmful Digital Communications

- 2.245 This project has also involved exploring the extent to which the current law on hate crime intersects or overlaps with harmful digital communications. 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 sections of society and make verbal attacks on an instantaneous basis to wide audiences.³¹¹
- 2.246 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.”³¹² Incitement includes publication, broadcast and preparation of materials. The 1989 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

without lawful authority) would carry a maximum sentence of 10 years for conviction on indictment.

³¹¹ Whine “Cyberhate, anti-semitism and counter legislation” (2006) Comms L 124, at 124.

³¹² Section 1(1) of the *Prohibition of Incitement to Hatred Act 1989*.

residence.”³¹³ 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”.³¹⁴ 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 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.³¹⁵ Some of those who joined also contributed further abusive material to the page.

- 2.247 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.
- 2.248 A number of respondents to the Issues Paper questioned whether the 1989 Act is adequate to deal with online hate speech. One consultee noted that the legislation was not designed to deal with the internet and could not have envisaged “a situation in which every individual has the ability to publish and broadcast to mass audiences”. Another consultee queried whether “static images, such as photographs, ‘memes’ or pictures” are covered by section 2 of the 1989 Act, as “these do not amount to a ‘recording of visual images’”, and while the interpretation section of the 1989 Act defines ‘written material’ as ‘any sign or visual representation’, they felt that this matter required clarification.
- 2.249 Other legislation may be used to prosecute online hate speech but only to a very limited extent. 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 “menacing” messages, but this only extends to the telephone and text and does not include digital or online communications.
- 2.250 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

³¹³ Section 2 of the *Prohibition of Incitement to Hatred Act 1989* 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.”

³¹⁴ See Cummisky, “Facebooked: Anti-Social Networking and the Law” 105(9) *Law Society Gazette*, November 2011 at 16.

³¹⁵ *Ibid* at 17.

prosecuted under section 4(1) of the *Public Order Act 1986*,³¹⁶ which is broadly similar to section 6 of the 1994 Act:

In *R v Stacey*,³¹⁷ the accused published, while drunk, an offensive tweet mocking the footballer Fabrice Muamba after he collapsed during a football match. 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.³¹⁸ The accused was convicted under section 4(1)(a) of the *Public Order Act 1986* and sentenced to 56 days imprisonment.

However, the definition of “public place” in the 1994 Act does not appear to extend to the internet as it is limited to physical places.³¹⁹ The English Act is not confined in this way, as it does not include a definition for “public place”.

- 2.251 Section 10 of the *Non-Fatal Offences Against the Person Act 1997* may be 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.
- 2.252 Ireland intends to ratify the Council of Europe Convention on Cybercrime,³²⁰ and has been encouraged to ratify the Additional Protocol to the Convention concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.³²¹ 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 response to propaganda of racist and xenophobic nature committed through computer systems.

³¹⁶ 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.”

³¹⁷ *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>.

³¹⁸ *Ibid* at paragraph 8 of the judgment.

³¹⁹ Section 3 of the *Criminal Justice (Public Order) Act 1994* provides: “In this Part, except where the context otherwise requires- [...]

public place includes:

- (a) any highway,
- (b) any outdoor area to which at the material time members of the public have or are permitted to have access, whether as of right or as a trespasser or otherwise, and which is used for public recreational purposes,
- (c) any cemetery or churchyard,
- (d) any premises or other place to which at the material time members of the public have or are permitted to have access, whether as of right or by express or implied permission, or whether on payment or otherwise, and
- (e) any train, vessel or vehicle used for the carriage of persons for reward.”

³²⁰ Council of Europe Convention on Cybercrime (23 November 2001). Ireland signed this Convention on 28 February 2002. The Government Legislation Programme, Summer Session 2016, states that work on a Bill to implement the Convention is underway.

³²¹ 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).

- 2.253 In 2008 the EU adopted a Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law,³²² 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 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.³²³ 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.³²⁴ 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.³²⁵ 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.³²⁶ In this respect, the EU Commission's Report notes that the 1989 Act does not extend to such cases.³²⁷ It also points out that, in accordance with the Lisbon Treaty, infringement proceedings may be taken against EU Member States for failure fully to implement the Framework Decision from 1 December 2014.³²⁸ The effect of this is that the State will implement the Framework Decision at some time.
- 2.254 The Commission considers that reform of online hate speech laws needs to be undertaken as part of an overarching reform of hate crime, as the problems with Ireland's hate crime laws extend beyond the potential difficulty with applying them in the online setting. Firstly, the 1989 Act, which is the principal Act within this area, is ineffective, with only a

³²² 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.

³²³ *Ibid*, article 1(1).

³²⁴ *Ibid*, article 9(2).

³²⁵ 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.

³²⁶ 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."

³²⁷ 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.

³²⁸ The European Commission's 2014 report states, 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."

limited number of convictions secured under it.³²⁹ This is because the offences under the Act are very difficult to prove, particularly the stirring up hatred offence under section 2. Secondly, while progress is underway to implement the Cybercrime Convention, action still needs to be taken to implement the 2008 Framework Decision as well as ratify the Protocol to the Cybercrime Convention.

- 2.255 In this respect, it is clear that comprehensive reform of hate crime legislation is in progress and the Commission considers that such an approach would be preferable to efforts designed to address online hate speech only. This view was shared by many of the respondents to the Issues Paper. Because this type of wide-ranging reform is outside the scope of this project, the Commission recommends that online hate speech should be addressed as part of the general reform of hate crime law.

2.256 The Commission recommends that hate speech should be addressed as part of the general reform of hate crime law, which falls outside the scope of this Report.

³²⁹ See Schweppe, Haynes and Carr, *A Life Free From Fear: Legislating for Hate Crime in Ireland: An NGO Perspective* (2014) at 12.

CHAPTER 3 DIGITAL SAFETY, TAKEDOWN PROCEDURE AND CIVIL LAW

A Introduction

- 3.01 This chapter considers the second major element of this project, the need for an oversight system to promote digital safety and to provide for efficient take down procedures for harmful digital communications, as well as related civil law matters.
- 3.02 In accordance with the harm principle discussed in Chapter 1, the criminal law should only be employed as a last resort, to target the most serious behaviour for which other responses are unsuitable. The criminal law is not an appropriate response to some harmful digital communications for a number of reasons, including that a substantial amount of such activity is carried out by young people, as well as by adults behaving impulsively and without intending to cause harm. The civil law, including an oversight system to promote digital safety and efficient take down procedures, may thus be more suitable, particularly for less serious cases involving harmful digital communications. The civil law may also provide more effective remedies in some cases, as victims of such behaviour frequently attach greater priority to removal of the harmful content rather than punishing the perpetrator. The current law provides for some civil remedies, but as discussed further below, these may not be either readily accessible or effective in many cases.
- 3.03 However, before examining the existing civil law remedies, it is necessary to explore to what extent existing non-statutory arrangements put in place by internet intermediaries, such as social media platforms, are effective to deal with harmful digital communications. In this respect, the ability of social media platforms to offer remedies without the need for court-based processes to be engaged is of particular relevance, because a considerable amount of harmful digital communications are posted using these platforms.

B Non-statutory Arrangements on Social Media Sites

- 3.04 Under current non-statutory, self-regulated, arrangements, individuals can report harmful content to social media sites and request that it be removed. All the prominent social media companies have content and conduct policies and standards which outline their approaches to different categories of harmful content, including hate speech, sexual violence and exploitation, serious threats, harassment and related activity, creating fake profiles, posting private information without consent and content that would promote self-harm. Not all of these categories appear to be treated in the same way, with removal more likely in the case of some types of content rather than others.

(1) Content and conduct policies of social media companies**(a) Hate speech**

- 3.05 All of the content and conduct policies of the leading social media companies state that they do not tolerate hate speech on their platforms. In its Community Standards, Facebook states that it “removes hate speech which includes content that directly attacks people based on their race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender or gender identity or serious disabilities or diseases”.¹ Google+ notes that the balance between protecting freedom of expression and safeguarding users against hate speech is a delicate one but “if the primary purpose is to attack a protected group, the content crosses the line” and will be removed.²
- 3.06 In May 2016, Facebook, Twitter, YouTube and Microsoft agreed with the European Commission a *Code of Conduct on Countering Illegal Hate Speech Online*.³ This code of conduct includes a number of public commitments, including that the four companies are to have clear and effective processes in place to review notifications regarding illegal online hate speech with dedicated teams to review notifications. The companies agreed to review the majority of requests in less than 24 hours. The code also provides for commitments by the companies to educate and raise awareness among their users of the types of content not permitted on their platforms and to provide information on procedures for submitting notices. The code also includes provisions on cooperation, between the companies and civil society organisations as well as between themselves and other platforms, to facilitate reporting of online hate speech and to share best practices on how to respond, including further developing effective counter speech campaigns. The European Commission and the companies agreed to assess the commitments in the code on a regular basis and to report to the High Group on Combating Racism, Xenophobia and all forms of intolerance by the end of 2016.
- 3.07 This code of conduct was adopted as a response to the terrorist attacks in Paris in 2015 and Brussels in 2016, and may ensure that policies on online hate speech by social media platforms, particularly those that agreed to the code (but perhaps also more widely) will be subjected to greater scrutiny.

(b) Sexual violence and exploitation

- 3.08 Content that threatens or promotes sexual violence or exploitation is prohibited on social media sites. Facebook’s Community Standards provide that this category includes “sexual exploitation of minors and sexual assault” as well as photographs or incidents of sexual violence and “images shared in revenge or without permission from the people in the images”.⁴ Facebook provides a definition of sexual exploitation which includes “any sexual content involving minors” as well as threats to share intimate images, solicitation of sexual material and offers of sexual services. The Community Standards also provide that

¹ Facebook, *Community Standards* available at <https://en-gb.facebook.com/communitystandards/#>.

² Google+, *User Content and Conduct Policy*, Policies for Google+, Hangouts and Photos available at <https://www.google.com/intl/en-US/+/policy/content.html>.

³ European Commission, *Code of Conduct on Countering Illegal Hate Speech Online* (2016) available at http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

⁴ Facebook, *Community Standards* available at <https://en-gb.facebook.com/communitystandards>.

where appropriate such content may be referred to law enforcement.⁵ Twitter's Rules refer to a "child sexual exploitation policy" with intimate photos or videos involving adults dealt with under its private information policy.⁶ The child sexual exploitation policy is phrased in particularly strong terms, with Twitter stating that it does not tolerate such content on its site and that when it is made aware of child exploitation content they will remove such content without further notice and report to the National Center for Missing & Exploited Children ("NCMEC")⁷. Accounts which promote or contain updates to child sexual exploitation material are permanently suspended. Google+ provides for a similar policy on child sexual exploitation which is described separately to its policy on sexually exploitative material involving adults.⁸ However, Instagram, like Facebook, puts both types of content together, with its Community Guidelines stating that "zero tolerance" will be exercised in relation to "sharing sexual content involving minors or threatening to post intimate images of others".⁹

- 3.09 Although sexually exploitative material involving minors has always been treated with the utmost seriousness on the major social media sites, it has only been in more recent times that sexually exploitative material involving adults, particularly "revenge porn", has attracted a similarly strong response. Thus, it was not until 2015 that several social media companies including Facebook, Twitter and Google explicitly banned "revenge porn" from their sites owing to growing pressure on them to take action against this type of material.¹⁰

(c) *Serious threats*

- 3.10 Serious credible threats are not tolerated on social media sites and will be removed where such threats represent a "genuine risk of physical harm or amount to direct threats to public safety"¹¹. In determining whether a threat is credible, Facebook states that it takes into account factors such as the person's physical location or public visibility.¹²

(d) *Harassment and related activity*

- 3.11 Harassment and bullying are not permitted on the major social media sites. Facebook states that it will remove content "that appears to purposefully target private individuals with the intention of degrading or shaming them".¹³ This includes, but is not limited to "pages that identify and shame private individuals, images altered to degrade private individuals, photos or videos of physical bullying posted to shame the victim, sharing personal information to blackmail or harass people and repeatedly targeting other people with unwanted friend requests or messages." Instagram's Community Guidelines state

⁵ *Ibid.*

⁶ Twitter, *The Twitter Rules* available at <https://support.twitter.com/articles/18311>.

⁷ Although the National Center for Missing & Exploited Children is a US based NGO, it operates a global network in partnership with the International Centre for Missing & Exploited Children. See <http://www.missingkids.org/GMCN>.

⁸ Google+, *User Content and Conduct Policy*, Policies for Google+, Hangouts and Photos available at <https://www.google.com/intl/en-US/+/policy/content.html>.

⁹ Instagram, *Community Guidelines* available at <https://help.instagram.com/477434105621119/>.

¹⁰ See "Why did it take so long to ban revenge porn?" *Fusion* 29 June 2015 available at <http://fusion.net/story/157734/revenge-porn-bans-were-long-time-coming/>.

¹¹ Facebook, *Community Standards* available at <https://en-gb.facebook.com/communitystandards/#>.

¹² *Ibid.*

¹³ *Ibid.*

that content will be removed that “targets private individuals to degrade or shame them” or where it amounts to personal information meant to harass or blackmail.¹⁴ Repeated unwanted messages are also not permitted. Twitter states that users “may not incite or engage in the targeted abuse or harassment of others”.¹⁵ Among the factors that may be considered when evaluating whether behaviour amounts to harassment include: “if the primary purpose of the account is to harass or send abusive messages to others; if the reported behaviour is one-sided or includes threats; if the reported account is inciting others to harass another account; and if the reported account is sending harassing messages to an account from multiple accounts”.¹⁶ Google+ also does not allow harassment or bullying and states that users engaged in such activity may be permanently banned in addition to the content being removed, and that “[i]n emergency situations, we may escalate imminent threats of serious harm to law enforcement”.¹⁷ Snapchat¹⁸ and Ask.fm¹⁹ also explicitly ban bullying and harassment under their terms of service.

- 3.12 A number of social media sites made changes to their bullying and harassment policies in 2015. Twitter announced new tools to allow users to flag and report abuse more easily as well as unveiling a new filter which will prevent users from seeing abusive messages in April 2015.²⁰ Facebook and Instagram improved their Community Standards pages in 2015, setting out in greater detail the type of content that is not permitted on their sites.²¹ In 2015, Ask.fm established a Safety Advisory Board²² and a Safety Centre (which offers information to users about staying safe online)²³ as part of the plan by its parent company Ask.com, which acquired Ask.fm in August 2014, to enhance safety and reduce bullying on the service. These changes may have been in response to negative publicity linking social media sites to harmful digital communications and the recognition that, unless such companies are shown to be doing something to combat this problem, their user numbers could decline.

(e) *Fake profiles, private information and other prohibited content*

- 3.13 All social media sites include policies on posting private information such as addresses and bank details and policies on impersonation, which prohibit users from setting up fake profiles to mislead or confuse other users. Content that promotes self-harm is also explicitly prohibited on all social media platforms.

¹⁴ Instagram, *Community Guidelines* available at <https://help.instagram.com/477434105621119/>.

¹⁵ Twitter, *The Twitter Rules* available at <https://support.twitter.com/articles/18311>.

¹⁶ *Ibid.*

¹⁷ Google+, *User Content and Conduct Policy*, Policies for Google+, Hangouts and Photos available at <https://www.google.com/intl/en-US/+/policy/content.html>.

¹⁸ Snapchat, *Community Guidelines* available at <https://support.snapchat.com/a/guidelines>.

¹⁹ Ask.fm, *Terms* available at <http://about.ask.fm/legal/en/terms.html>.

²⁰ See “The Top Social Media Platforms’ Efforts To Control Cyber-Harassment” *Socially Aware* 31 August 2015 available at <http://www.sociallyawareblog.com/2015/08/31/the-top-social-media-platforms-efforts-to-control-cyber-harassment/>.

²¹ *Ibid.*

²² Ask.fm, “Askfm Forms First Ever Safety Advisory Board” Press Release 15 January 2015 available at <http://about.ask.fm/ask-fm-forms-first-ever-safety-advisory-board/>.

²³ Ask.fm, “Askfm Launches New Safety Center” Press Release 9 February 2015 available at <http://about.ask.fm/ask-fm-launches-new-safety-center/>.

(2) Reporting Harmful Content and Takedown in practice

- 3.14 The prominent social media platforms include tools for reporting content which violates their content and conduct policies as well as privacy controls which can limit the audience of the content posted by the user.
- 3.15 Reporting is done via reporting buttons/links displayed on user profiles or beside the content posted. Thus, these reporting buttons are prominent and easily accessible to the user. Reports are then reviewed by trained teams and content that violates the terms of the site's content and conduct policy will be removed. Users can also block other users on these sites or hide the content posted by other users. Sites such as Facebook also include social reporting functions which enable users to report content which they may not like, but which does not breach the content and conduct policy of the relevant site, to the user responsible for the posting.
- 3.16 Social media sites enable users to control the audience of the content they post. Thus, users are given the option of allowing all internet users access to their profile and/or any content posted or to limit full profile access and postings to "friends" or other smaller audiences selected by the user. The default setting for users on Facebook and Snapchat is to allow access only to friends of the user. In contrast, Twitter and Instagram are default public platforms whereby all content posted is visible to all internet users, not just account holders of the platforms, unless the user changes their privacy settings to only permit access to more limited audiences.
- 3.17 It is difficult to assess the efficacy of social media companies' content and conduct policies and reporting and removal procedures as such companies do not publish information on how many people they employ to investigate reports of abuse, the amount and types of reports they receive or the level of satisfaction of those who complain.²⁴ Thus, no accurate statistics are available. In consultation meetings held with the Commission, members of the Gardaí have indicated that social media platforms are very quick to respond to reports of child pornography on their services as well as serious threats to life and safety. A representative from the Office of the Data Protection Commissioner felt from his experience of dealing with the large internet intermediaries that they are thorough when it comes to removing content as they are aware of the consequences of not responding to complaints.
- 3.18 At the Commission's consultation in April 2016, facilitated by the Department of Children and Youth Affairs, young people were asked whether they "had any experience of getting something taken down from the internet". Very few of the participants had personal experience of this, but the general view expressed was that it was very difficult to get content removed from the internet and that social media platforms should make this easier. Young people felt that the reporting systems on the major social media sites were not effective and that these platforms should make it easier to report and remove content from the internet. In relation to fake profiles or accounts, participants felt that social media sites should take greater responsibility in relation this type of activity by making it

²⁴ "Top tech firms urged to step up online abuse fightback" *The Guardian* 11 April 2016 available at <https://www.theguardian.com/technology/2016/apr/11/facebook-twitter-google-urged-to-step-up-online-abuse-fightback>.

more difficult to set up such accounts and taking action to prevent users from setting up another fake account once one is shut down.

- 3.19 The Commission also understands from its consultative meetings with the social media sector that response times to complaints about harmful communications have improved between 2014 and 2016, reflecting the increased application of technology and people to this issue. Response times will vary according to the complexity of the complaint, and the more serious types of reports will receive a priority response. For example, a report relating to an immediate threat to a person's safety such as a suicide threat would be likely to receive an immediate response regardless of the time the report was made, whereas a complaint relating to something complex such as financial fraud could take 24 hours or longer for a response.
- 3.20 As noted in Chapter 1, one of the reasons why obtaining takedown is difficult is because internet intermediaries enjoy immunity under the terms of the 2000 eCommerce Directive and the requirements for notice and takedown under the Directive are unclear. However, as discussed in Chapter 1, this Directive is expected to be reviewed shortly²⁵ and so intermediaries including social media companies may be required to take a more active role in monitoring and reviewing content in the future.
- 3.21 Before considering any alternative mechanisms, the Commission first discusses existing civil remedies for harmful digital communications and then explores possible reforms, including statutory arrangements that have been introduced in New Zealand and Australia.

C Reform of Civil Remedies for Harmful Digital Communications

(1) Existing civil remedies

(a) *Defamation Act 2009*

- 3.22 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".

- 3.23 As the 2009 Act provides that a defamatory statement can be published by any means, it applies to publication through the digital or online 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*,²⁶ 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

²⁵ See Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions "A Digital Single Market Strategy for Europe" (May 2015) at paragraph 3.3.2, and the discussion of the eCommerce Directive in Chapter 1, above.

²⁶ [2012] IEHC 42.

ordering the termination of the website upon which the material was posted. A *Norwich Pharmacal* order²⁷ was also granted.

- 3.24 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”²⁸ 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*²⁹ illustrates:

In *McKeogh v Doe* 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.”³⁰ 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. 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.

- 3.25 McKeogh also underlines the potentially great cost of civil proceedings, with the plaintiff reportedly facing a legal bill of over €1,000,000.³¹
- 3.26 Another difficulty with injunctions in the context of digital 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*³² 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

²⁷ *Norwich Pharmacal* orders are discussed at paragraph 3.100 below.

²⁸ *Tansey v Gill* [2012] IEHC 42 at paragraph 25.

²⁹ *McKeogh v Doe* [2012] IEHC 95.

³⁰ “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>.

³¹ “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>.

³² [2010] IEHC 48.

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.

- 3.27 A number of consultees discussed the problems with take down orders, suggesting that the absence of an adequate and expeditious take down procedure is a significant issue. One consultee highlighted that while many websites will comply readily with takedown orders, others are very reluctant. This consultee also commented on worldwide take down versus national takedown of harmful content, stating that some websites suggest that if a victim avails of their policies and if take down ensues (which is not guaranteed), then the takedown will be on a worldwide basis. However, if a victim uses or needs a court order for take down, the websites may take the negotiating approach that only local national take down will be achieved. The consultee described this as “on one hand an intimidation to victims; on another it is a suggestion that corporate policies, some of which may be contained on a website (and in any event which may be changed at will), stand in greater importance than legal courts orders.”

(b) *Civil remedy for breach of a constitutional right*

- 3.28 A number of recent cases have highlighted the remedies available to plaintiffs based on breach of a constitutional right by another person.³³ Such a cause of action could be particularly beneficial in the context of harmful digital communications 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*³⁴:

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.

- 3.29 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. An example of this might be the case mentioned above of the humiliating video of a teenage girl making drunken remarks,³⁵ as the video was uploaded without her consent and no public interest element was involved.

³³ *Sullivan v Boylan (No. 2)* [2013] IEHC 104; *Herrity v Associated Newspapers (Ireland) Ltd* [2009] 1 IR 316.

³⁴ *Herrity v Associated Newspapers (Ireland) Ltd* [2009] 1 IR 316.

³⁵ 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/>.

(c) Data Protection Acts 1988 and 2003

- 3.30 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.³⁶ 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,³⁷ but this remedy is very difficult to obtain as actual injury or damage must be proven before compensation is awarded.³⁸ However, the 2016 General Data Protection Regulation provides for damages for “moral damage”³⁹ or distress as other jurisdictions, notably the UK following the decision in *Google Inc. v Vidal Hall and others*,⁴⁰ already do.
- 3.31 As discussed in Chapter 2,⁴¹ the *Data Protection Acts 1988 and 2003* 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”⁴² which generally excludes personal or recreational internet activity such as posting on social networking websites. However, in *Lindqvist, Bodil, Criminal Proceedings against*,⁴³ the Court of Justice of the European Union (CJEU) held that the household exemption did not apply where an individual posted content online which was accessible to an “indefinite number of people”.⁴⁴ Thus, an individual may assume the responsibilities of a data controller where they post content about another person on a publicly available website or a social networking page which is accessible to a large number of people.

(i) Right to Protection of Personal Data and the Right to Privacy

- 3.32 The data protection regime offers significant protection for the right to privacy. The 1995 Directive⁴⁵ which forms the basis for the 2003 Act which substantially amended the 1988 Act, emphasises that the goal of the EU Data Protection system is to safeguard the fundamental freedoms of individuals and in particular, the right to privacy.⁴⁶ This goal of the Directive is clearly articulated by the CJEU in its seminal *Google Spain* judgment, where the Court stated that the Directive “seeks to ensure a high level of protection of the

³⁶ The *Data Protection Acts* are also discussed at paragraphs 2.105-2.110 above.

³⁷ Section 7 of the *Data Protection Acts 1988*.

³⁸ See *Michael Collins v FBD Insurance PLC* [2013] IEHC 137.

³⁹ See Recitals 75, 83 and 85 and Article 82 of *Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.

⁴⁰ [2015] EWCA Civ 311.

⁴¹ Chapter 2, paragraph 2.107.

⁴² Section 1(4)(c) of the *Data Protection Act 1988*, implementing the “household exemption” in Article 3.2 of Directive 95/46/EC.

⁴³ *Criminal Proceedings against Lindqvist and Bodil* (C-101/01) [2004] ECR I 12971.

⁴⁴ *Ibid.*, at paragraph 47.

⁴⁵ Directive 95/46/EC, which will be repealed and replaced in 2018 by Regulation (EU) 2016/679, the 2016 General Data Protection Regulation (GDPR).

⁴⁶ *Ibid.* See, in particular, Recital 2 of the 1995 Directive:

“Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy...”

fundamental rights and freedoms of natural persons, in particular their right to privacy, with respect to the processing of personal data.”⁴⁷

- 3.33 The right to the protection of personal data is also recognised as a specific right under Article 8 of the EU Charter of Fundamental Rights. Article 8 provides that:

- “1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.”

The presence of this specific right to protection of personal data in the Charter underlines the importance the EU attaches to data protection. The close relationship between protection of personal data and the right to privacy is reflected in the case law of the CJEU where the right to protection of data contained in Article 8 is frequently read in light of the right to privacy found in Article 7 of the Charter. Thus, in *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources and Ors* the CJEU stated that “the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is especially important for the right to respect for private life enshrined in Article 7 of the Charter”.⁴⁸

(ii) **Case law of the Court of Justice of the European Union on Data Protection**

- 3.34 *Digital Rights Ireland* was one of a series of cases from 2014 and 2015 that illustrate the significance and considerable reach of the EU Data Protection regime. In this case, the Data Retention Directive⁴⁹ was struck down as incompatible with Articles 7 and 8 of the Charter by the CJEU. The Court emphasised that because of the fundamental nature of the right to protection of personal data, “clear and precise rules governing the scope and application of the measure in question”⁵⁰ are required as well as “minimum safeguards” so that persons “have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data”⁵¹.
- 3.35 This case was followed by *Google Spain SL and Google Inc v Agencia Espanola de Protection de Datos*⁵² where the Court established that a right to be forgotten existed

⁴⁷ Case C-131/12, *Google Spain SL and Google Inc v Agencia Espanola de Protection de Datos* (judgment of 13 May 2014), paragraph 66.

⁴⁸ *Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and others; Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others* (judgment of 8 April 2014) at paragraph 53.

⁴⁹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

⁵⁰ *Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and others; Kärntner Landesregierung (C-594/12), Michael Seitlinger, Christof Tschohl and others* (judgment of 8 April 2014), paragraph 54.

⁵¹ *Ibid.*

⁵² Case C-131/12, *Google Spain SL and Google Inc v Agencia Espanola de Protection de Datos* (judgment of 13 May 2014).

under the Directive.⁵³ In this case, Mr Costeja González no longer wanted links to a newspaper article from 1998, which mentioned a real-estate auction organised following attachment proceedings for the recovery of social security debts owed by him, to be displayed in search results for his name. The Court upheld this request and also stated that it was not “necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject”⁵⁴ and that the data subject’s rights under Articles 7 and 8 of the Charter override both the economic interest of the operator of the search engine as well as the interest of the general public in having access to the information in question. The CJEU also adopted a broad definition of a data controller in this case, holding that a search engine was a data controller under the terms of the Directive.⁵⁵

- 3.36 The Court’s robust protection of the right to privacy is also visible in its decision in *Ryneš v Úřad pro ochranu osobních údajů*,⁵⁶ where a narrow interpretation of the household exemption was adopted. In this case, the Court held that in order to avail of the exemption, the individual must be engaged in “a purely personal or household related activity”.⁵⁷ Thus, Ryneš was held to be a data controller as his domestic CCTV system, as well as surveying his own private property, also overlooked a small area of public space.
- 3.37 Finally, in *Schrems v Data Protection Commissioner*,⁵⁸ the CJEU struck down Commission Decision 2000/520/EC, which provided for safe harbour privacy principles to be used where US organisations received personal data from the EU, as incompatible with Articles 7 and 8. The CJEU referred to its “settled case law” on data protection, stressing that “above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary”.⁵⁹
- 3.38 The case law of the CJEU thus establishes that any limitations upon the related rights of privacy and data protection must be imposed strictly and that the rights occupy a position of fundamental importance within the EU.

(iii) **2016 General Data Protection Regulation (GDPR)**

- 3.39 Regulation (EU) 2016/679, the 2016 General Data Protection Regulation (GDPR) was adopted in April 2016 and will come into force in May 2018 when it will also replace the 1995 Directive. The European Commission has stated that the GDPR will “strengthen the right to data protection, which is a fundamental right in the EU”.⁶⁰ One of the most notable features of the GDPR is that it enhances and clarifies the right to erasure and specifically

⁵³ *Ibid*, paragraph 88. The right to be forgotten was said to be established under Articles 12(b) and 14(a) of the Directive, which relate to the data subject’s right of access and right to object respectively.

⁵⁴ *Ibid*, paragraph 99.

⁵⁵ *Ibid*, paragraph 33.

⁵⁶ Case C-212/13, *Ryneš v Úřad pro ochranu osobních údajů* (judgment of 11 December 2014)

⁵⁷ *Ibid*, paragraph 33.

⁵⁸ Case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (judgment of 6 October 2015).

⁵⁹ *Ibid*, paragraph 92.

⁶⁰ “Agreement on Commission’s EU data protection reform will boost Digital Single Market” European Commission Press Release, 15 December 2015 available at http://europa.eu/rapid/press-release_IP-15-6321_en.htm.

refers to it as the right to be forgotten. It also introduces, among other provisions, new provisions on consent and the right to data portability, as well as providing for a more onerous enforcement regime which enables significant fines to be imposed on data controllers and processors for breach of the Regulation.

- 3.40 Article 17 of the GDPR provides for a “right to erasure (right to be forgotten)” This is far more substantial than the equivalent Articles in the Directive and entitles data subjects to the “right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay”⁶¹ where one of a number of grounds apply, including where the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed, consent on which the data processing is based is withdrawn by the data subject, where the data subject objects to the processing of personal data and there are no legitimate grounds for the processing and where the processing of the data subject’s data otherwise does not comply with the Regulation.⁶² The Recitals of the Regulation also make clear that the right to be forgotten is particularly relevant where the data subject has given their consent as a child “when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the internet”.⁶³ The Article additionally requires, “in order to strengthen the ‘right to be forgotten’ in the online environment”⁶⁴ data controllers who have made the personal data public to inform the controllers which are processing such data to erase any links to or copies or replications of that data.
- 3.41 The right to be forgotten, along with the other rights of data subjects recognised in the Regulation, is bolstered by a strong enforcement regime which allows significant fines to be imposed for breaches of the Regulation. Under Article 83(3)(a), fines of up to €10,000,000 or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding year, whichever is higher, shall apply for infringements of the rights of data subjects. Thus, Keller suggests that the Regulation “strongly encourages Internet intermediaries to delete challenged content, even if the challenge is legally groundless” because while there are no consequences to over-removing content, intermediaries risk very large fines for not honouring right to be forgotten requests.⁶⁵
- 3.42 Another significant element of the Regulation is the emphasis placed on consent for data processing. Article 6(1)(a) of the Regulation provides that data processing is lawful only if “the data subject has given consent to the processing of their personal data for one or more specific purposes”. The conditions for consent are then set out in Article 7, requiring that consent be freely given and that the request for consent be “presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible

⁶¹ Article 17(1) of the *General Data Protection Regulation*.

⁶² Article 17(1)(a)–(f) of the *General Data Protection Regulation*.

⁶³ Recital 65 of the *General Data Protection Regulation*.

⁶⁴ Recital 66 of the *General Data Protection Regulation*.

⁶⁵ Keller, “Final Draft of Europe’s ‘Right to be Forgotten’ Law” *The Center for Internet and Society* Blog 17 December 2015 available at <http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law>.

form, using clear and plain language”.⁶⁶ Data subjects also have the right to withdraw consent at any time.⁶⁷

- 3.43 Specific provision is made for children’s consent in Article 8. This Article states that the consent of a child will only be lawful in the case of a child under the age of 16 years or “where Member State law provides a lower age which shall not be below 13 years” where such consent is given or authorised by the holder of parental responsibility of the child.⁶⁸ An earlier draft of the Regulation removed Member State discretion in this area and required parental authorisation in all cases for children under the age of 16 years. However, there was significant criticism of this proposal with commentators arguing that it restricted children’s right to freedom of expression, effectively banning them from social media platforms without explicit parental consent, and that it would be very difficult to enforce in practice.⁶⁹
- 3.44 It is notable that the Regulation retains the wording of the Directive in relation to the household exemption. Thus, Article 2 of the Regulation provides that the Regulation does not apply to the processing of personal data “by a natural person in the course of a purely personal or household activity”.⁷⁰ Some of the earlier versions of the Regulation appeared to favour a broader exemption, by omitting the word “purely”, which would have negated the CJEU’s findings in *Ryneš*.⁷¹ Social Networking is also specifically referred to in Recital 18 of the Regulation as an example of personal and household activities but only when it is undertaken “within the context of such personal and household activities”.

(iv) **Conclusion**

- 3.45 The Data Protection regime is thus gaining increasing importance as well as growing in public awareness, with the decisions in the *Google Spain* and *Schrems* cases attracting particular attention. The regime also has a number of advantages over court proceedings. Firstly, it is cost effective and fast compared to civil actions. Secondly, the focus of data protection is on protecting privacy and “ensuring that individuals have control over how information about them is used or at the very least, how this information is used by others”.⁷² Thus, the system is less punishment focused than the criminal justice system which may make it a more suitable avenue for disputes involving young people, who are responsible for a considerable amount of harmful digital communications. Finally, data protection is a well- established and European wide regime and is only likely to increase in visibility after the high profile series of cases discussed above. The regime will also become increasingly harmonised once the General Data Protection Regulation comes into force in 2018, which will make it easier for individuals to exercise their rights within the

⁶⁶ Article 7(2) of the *General Data Protection Regulation*.

⁶⁷ Article 7(3) of the *General Data Protection Regulation*.

⁶⁸ Article 8(1) of the *General Data Protection Regulation*.

⁶⁹ “Is Europe really going to ban teenagers from Facebook and the internet?” *The Guardian* 15 December 2015 available at <http://www.theguardian.com/technology/2015/dec/15/europe-ban-teenagers-facebook-internet-data-protection-under-16>.

⁷⁰ Article 2(c) of the *General Data Protection Regulation*.

⁷¹ See “Council of Ministers’ Regulation text negates ECJ rulings in Lindqvist and Ryneš” *Hawktalk* 14 July 2015 available at <http://amberhawk.typepad.com/amberhawk/2015/07/council-of-ministers-regulation-text-negates-ecj-rulings-in-lindqvist-and-ryne%C5%A1.html>.

⁷² Office of the Data Protection Commissioner, *Statement of Strategy 2014-2016*, page 1 available at <https://www.dataprotection.ie/docimages/1%20Strategy%20Statement%202014%20-%202016.pdf>.

EU. The Regulation will also strengthen the rights of data subjects, particularly, the right to be forgotten.

- 3.46 Nevertheless, data protection might not offer a suitable remedy in all cases. A number of speakers at the Commission's April 2015 seminar emphasised the limitations of the regime, particularly in more serious cases where the deterrent potential of data protection may be limited. In a consultation meeting with the Commission, the Office of the Data Protection Commissioner (ODPC) also indicated that the criminal law would be more suitable for serious cases involving harmful digital communications. The ODPC is also a relatively small organisation and would appear to require additional resources, particularly in light of the recent *Schrems* litigation. However, for less serious forms of activity where the individual's priority is removal of content and protection of personal privacy rather than punishment of the wrongdoer, then data protection does offer effective remedies. Thus, while the Commission considers that data protection cannot be the sole solution for those seeking remedies for harmful digital communications, increased awareness of the remedies available under the *Data Protection Acts* would be welcome.

(2) Alternative civil enforcement mechanisms

- 3.47 The potential cost, complexity and length of civil proceedings may deter victims of harmful digital communications and available processes and remedies may not be effective. A key matter is the extent to which a victim of online abuse, such as the plaintiff in *McKeogh v Doe*,⁷³ may obtain a takedown order in a speedy and inexpensive manner. A possible solution to this is to establish a body with functions connected to promoting digital safety and overseeing an efficient and effective take down procedure. This option has already been explored by Australia and New Zealand who have both introduced Acts which establish independent bodies designed to regulate the removal of harmful online content and promote digital safety.

(a) *New Zealand's Harmful Digital Communications Act 2015*

- 3.48 In July 2015, the New Zealand Parliament enacted the *Harmful Digital Communications Act 2015*. This Act was a response to a 2012 Report of the New Zealand Law Commission which recommended reform of its laws on civil remedies to deal with harmful digital communications, including the need to establish an independent body with a remit to resolve harmful digital communications based complaints quickly through a mediation-type process.⁷⁴ As well as introducing a new civil regime to target harmful digital communications, the Act also introduced a criminal offence of causing harm by posting digital communication⁷⁵ and amended offences relating to harassment⁷⁶ and aiding and abetting suicide.⁷⁷

⁷³ *McKeogh v Doe* [2012] IEHC 95, discussed at paragraph 3.24 above.

⁷⁴ New Zealand Law Commission, Ministerial Briefing Paper *Harmful Digital Communications: The Adequacy of the Current Sanctions and Remedies* (2012).

⁷⁵ Section 22 of the *Harmful Digital Communications Act 2015*. This offence is discussed further in Chapter 2, paragraphs 2.112-2.115.

⁷⁶ Section 32 of the *Harmful Digital Communications Act 2015*. The Act inserted two new subsections into section 3 of the *Harassment Act 1997* which establish that "one continuing act" can constitute harassment. A continuing act includes "a specified act done on any one occasion that continues to have effect over a protracted period (for example, where offensive material about a person is placed in any electronic media and remains there for a protracted period)". Section 4

- 3.49 The 2015 Act provides that harmful digital communications complaints be made initially to an “Approved Agency”⁷⁸ to investigate and attempt to resolve them by advice, negotiation, mediation or persuasion.⁷⁹ This body will also have a responsibility to provide education on policies for online safety and conduct on the Internet. If the Approved Agency fails to resolve the complaint, the Act provides that an individual⁸⁰ may apply to the District Court for a number of civil orders which can be made against defendants and online content hosts. The Act also provides that the court may make a declaration that a communication breaches a “communication principle”,⁸¹ which would be intended primarily to have a persuasive effect on website hosts or internet service providers operating outside New Zealand.⁸²
- 3.50 The Court can make one or more of the following types of orders against a defendant: an order to take down material, to refrain from the conduct concerned, an order not to encourage any other persons to engage in similar communications towards the affected individual, for a correction to be published, for a right to reply to be given to the affected individual and finally for an apology to be published.⁸³ In deciding whether or not to make an order, the Court is required to take into account factors including the content of the communication and the level of harm caused or likely to be caused by it, the purpose of the communicator, the context, the age and vulnerability of the affected individual and whether the communication is in the public interest.⁸⁴ The Act also expressly requires the Court to act consistently with the *New Zealand Bill of Rights Act 1990* when deciding

outlining the specified acts which can amount to harassment has also been amended to include “giving offensive material to a person by placing the material in any electronic media where it is likely that it will be seen by, or brought to the attention of, that person”.

⁷⁷ Section 30 of the *Harmful Digital Communications Act 2015* amends section 179 of the *Crimes Act 1961* whereby a person commits an offence who “incites, counsels, or procures another person to commit suicide, even if that other person does not commit or attempt to commit suicide in consequence of that conduct”. Previously, an offence was only committed where a person committed suicide or attempted to commit suicide as a result of the incitement etc.

⁷⁸ NetSafe, an NGO that promotes “confident, safe and responsible use of online technologies”, was appointed as the “Approved Agency” for the purposes of the *Harmful Digital Communications Act 2015* in May 2016. See <http://www.netsafe.org.nz/>.

⁷⁹ Sections 7 and 8 of the *Harmful Digital Communications Act 2015*.

⁸⁰ Proceedings may also be brought by the parent or guardian of the affected individual, the professional leader of a registered school or his delegate if the individual is a student of that school and consents to the professional leader/delegate bringing proceedings and the Police if the digital communication constitutes a threat to the safety of an individual. Section 11(1) of the *Harmful Digital Communications Act 2015*.

⁸¹ Section 6 of the *Harmful Digital Communications Act 2015* 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).

⁸² Section 19(4)(b) of the *Harmful Digital Communications Act 2015*.

⁸³ Section 19(1) of the *Harmful Digital Communications Act 2015*.

⁸⁴ Section 19(5) of the *Harmful Digital Communications Act 2015*.

whether or not to make an order.⁸⁵ Failure to comply with an order is a criminal offence under the Act.⁸⁶

- 3.51 The Court can also make take down orders against the online content host as well as orders to release the identity of the anonymous author and orders for correction and right of reply.⁸⁷ However, a safe harbour provision is included in the Act whereby no civil or criminal proceedings may be brought where the online content host receives a notice of complaint of the specific content and notifies the author of the content of the complaint and informs them that they may submit a counter-notice to the host within 48 hours of receiving that notification.⁸⁸ If after taking reasonable steps, the host is unable to contact the author, they must remove the content within 48 hours of receiving the notice of complaint. The host must also remove the content within this time frame if the author fails to submit a counter-notice. If the author submits a counter-notice consenting to the removal of the content, then it must be removed as soon as practicable. However, if the author does not consent to the removal of the content, the host must leave it in place and inform the complainant of the author's decision and, if the author consents, provide the complainant with personal information which identifies the author.
- 3.52 The civil enforcement regime introduced under the *Harmful Digital Communications Act 2015* has the potential to offer victims of harmful digital communications a quick and cost effective means of obtaining civil remedies. However, while the Approved Agency may have a valuable function in offering victims support and advice, it is unclear how effective mediation and similar methods may be in the online context. Mediation may be an unsuitable response to harmful digital content because it takes time and most complainants will be focused on trying to get the content removed as quickly as possible. This is exacerbated by the Approved Agency's lack of power to make orders, meaning there is no possibility of an interim order to disable the content during the mediation process. Mediation and similar mechanisms are also only 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. Thus, in practice, the District Court system has the potential to have a greater impact with mediation and the other mechanisms offered by the Approved Agency only likely to be effective in less serious or urgent cases.
- 3.53 It is important to note that the civil remedies sections of the *Harmful Digital Communications Act 2015* have not yet been commenced and so this system has not been tested in practice.⁸⁹ However, Australia established a similar mechanism designed to target cyber-bullying amongst children which has been operational since July 2015.

⁸⁵ Section 19(6) of the *Harmful Digital Communications Act 2015*.

⁸⁶ Section 21 of the *Harmful Digital Communications Act 2015*. If convicted of this offence, a natural person is liable for a term of imprisonment not exceeding 6 months or a fine not exceeding \$5000 (€2789.66), while a body corporate is liable for a fine not exceeding \$20,000 (€11,158.65).

⁸⁷ Section 19(2) of the *Harmful Digital Communications Act 2015*.

⁸⁸ Section 24 of the *Harmful Digital Communications Act 2015*.

⁸⁹ The Approved Agency is expected to begin operating in November 2016. See "NetSafe appointed to cyberbullying role" *Scoop* 31 May 2016 available at <http://www.scoop.co.nz/stories/PA1605/S00651/netsafe-appointed-to-cyberbullying-role.htm>.

(b) Australia's Enhancing Online Safety for Children Act 2015

- 3.54 In March 2015, the *Enhancing Online Safety for Children Act 2015* became law in Australia. This Act provides for a new civil enforcement mechanism designed to ensure the swift removal of harmful online content. However, it only applies to cyber-bullying involving children. The Act introduces a Children's e-safety Commissioner whose main function is to administer a complaint system in relation to cyber-bullying material which targets Australian children.⁹⁰ "Cyber-bullying material" is defined as material provided on a social media service or other electronic service which an ordinary reasonable person would conclude was intended to have the effect of "seriously threatening, seriously intimidating, seriously harassing or seriously humiliating" a child.⁹¹ The Commissioner also has additional functions including the promotion of online safety for children and coordinating the activities of other authorities and agencies in the area of internet safety.⁹²
- 3.55 This complaints system is comprised of a two-tier scheme intended to ensure the rapid removal of material from social media services:
- Tier 1 social media services- under the scheme, social media services can apply to become tier 1 social media services. Social media services will be granted this status if they satisfy the "basic online safety requirements"⁹³ which require the service to have terms of use that prohibit the posting of cyber-bullying material, a complaints scheme under which users can request removal of cyber-bullying material and an employee or an agent designated as a contact person for the purposes of the 2015 Act. Tier 1 social media services are thus engaged in a cooperative relationship with the Commissioner and are requested to remove material from their services rather than formally given notice to do this.⁹⁴
 - Tier 2 social media services- tier 2 social media services are engaged through a more formal regulated structure compared to tier 1 services. If a social media service fails to be granted tier 1 status because they do not satisfy the basic online safety requirements, or they do not apply for tier 1 status or they lose their tier 1 status because of non-compliance with the scheme, then they will be designated as

⁹⁰ Section 15 of the *Enhancing Online Safety for Children Act 2015*.

⁹¹ Section 5 of the *Enhancing Online Safety for Children Act 2015*.

⁹² Section 15 of the *Enhancing Online Safety for Children Act 2015*.

⁹³ Section 21 of the *Enhancing Online Safety for Children Act 2015* provides:

"(1) For the purposes of this Act, the basic online safety requirements for a social media service are as follows:

(a) the service's terms of use must contain:

(i) a provision that prohibits end users from posting cyber bullying material on the service; or

(ii) a provision that may reasonably be regarded as the equivalent of a provision covered by subparagraph (i);

(b) the service must have a complaints scheme under which end users of the service can request the removal from the service of cyber bullying material that breaches the service's terms of use;

(c) there must be an individual who is:

(i) an employee or agent of the provider of the service; and

(ii) designated as the service's contact person for the purposes of this Act;

(d) the contact details of the contact person must be notified to the Commissioner."

⁹⁴ However, if the material is not removed within 48 hours then the site will be given formal notice to remove the content. Failure to comply with this notice will result in the Commissioner publishing a statement that the site has not complied with the notice on its website- section 39 of the *Enhancing Online Safety for Children Act 2015*.

tier 2 social media services and given formal notice to remove the relevant material⁹⁵ with failure to remove the content within 48 hours resulting in a fine.⁹⁶

The person who posted the material may also be issued with a notice requiring them to remove it or refrain from posting cyber-bullying material or apologise for posting the material.⁹⁷

- 3.56 This Act has been met with some criticism from commentators such as Berg and Breheny, who view it as “a serious threat to freedom of speech and digital liberties” and an intrusion into the realm of civil society and the relationships between parents and children.⁹⁸ They argue that granting the Commissioner the power to issue notices to children requiring them to apologise is an unacceptable interference by the government into the domain of parents and schools. They suggest that one of the great challenges in developing policies to tackle bullying is that the “dynamics of social relationships among children are extremely opaque to outsiders” and the relationships between children are highly fluid.⁹⁹ Thus, behaviour which may appear to adults to be threatening, may not be understood as such by children. Inserting the state in the form of a body like the e-safety Commissioner is therefore highly undesirable as it has the potential to stifle children’s freedom of speech and act as a form of censorship. It may also drive cyber-bullying underground away from mainstream sites such as Twitter and Facebook and onto less controlled sites.¹⁰⁰
- 3.57 Fundamentally, Berg and Breheny believe that cyber-bullying amongst children should not be treated differently to “traditional” bullying and that this is a matter primarily for parents and schools.¹⁰¹ However, they are also careful to differentiate between bullying behaviour and “serious criminal conduct” such as “stalking with intent to intimidate or cause fear of physical or mental harm, physical or sexual assault, threats to kill or harm”, for which they believe sufficient criminal penalties already exist.¹⁰²
- 3.58 In December 2015, the Children’s e-safety Commissioner released a six month report which stated that the office had helped to resolve 92 complaints of serious cyber-bullying and 5,561 online content investigations had been undertaken.¹⁰³ The Report also provides that the office works “fast” with an eight hour turnaround to remove serious content.¹⁰⁴ As well as this, the Office has responsibility for education and has educated over 60,000 students, parents and teachers face to face and over 10,000 via virtual classrooms in relation to online safety.¹⁰⁵ In a submission to an Australian Parliamentary Inquiry on Revenge Porn, the Office of the Children’s e-Safety Commissioner noted that it had

⁹⁵ Section 30 of the *Enhancing Online Safety for Children Act 2015*.

⁹⁶ Section 36 of the *Enhancing Online Safety for Children Act 2015*.

⁹⁷ Section 42 of the *Enhancing Online Safety for Children Act 2015*.

⁹⁸ Berg and Breheny (Institute of Public Affairs) *A social problem not a technological problem: Bullying, cyber-bullying and public policy* (August 2014) at 3.

⁹⁹ *Ibid* at 6.

¹⁰⁰ *Ibid* at 23.

¹⁰¹ *Ibid* at 28.

¹⁰² *Ibid* at 18.

¹⁰³ Office of the Children’s eSafety Commissioner, *eSafety six month report* (31 December 2015) available at <https://www.esafety.gov.au/about-the-office/research-library/esafety-six-month-report>.

¹⁰⁴ *Ibid*.

¹⁰⁵ *Ibid*.

“worked collaboratively” with social media companies who are partners to the scheme¹⁰⁶ and that it had not had to use its formal powers to remove content yet.¹⁰⁷ The submission also states that all the social media companies that are partners to the scheme have “been efficient in removing content and actively cooperating to help address the behaviour of cyber-bullying” and that this demonstrates “the effectiveness of a cooperative civil scheme for serious cyber-bullying”.¹⁰⁸

- 3.59 The Australian scheme thus appears to be operating successfully and suggests that specialist disputes bodies for harmful digital communications can be effective. Although the Australian body is confined to cyber-bullying among children and no similar remedies are currently available to adult victims of harmful digital communications, this may change in the future because in 2016 the Australian Parliamentary Inquiry on victim-shaming (so called “revenge porn”) recommended that the Australian government consider empowering an agency to issue takedown notices for non-consensually shared intimate images.¹⁰⁹ This body would operate in a similar way as the Office of the Children’s e-Safety Commissioner, working in partnership with social media companies to promptly remove harmful content. Although the Australian Parliamentary Inquiry report also recommended introducing criminal offences designed to target the non-consensual distribution of intimate images,¹¹⁰ it was noted that take down notices outside of a court process “often offer a more expeditious remedy in the first instance for removing intimate images and affording victims some protection”¹¹¹. With regard to the agency which should be empowered with this role, the Committee did not reach a conclusive view as to whether this should be the Office of the Children’s e-Safety Commissioner or whether it would be more suitable for another government agency to be given this role.¹¹²

(3) Consultation responses

- 3.60 The Issues Paper asked whether a specialist body should be established that would offer non-court, fast yet enforceable remedies for harmful digital communications. The majority of respondents to the Issues Paper were in favour of such a proposal. Consultees suggested that a specialist body could be beneficial to both victims and ISPs by enabling both sides to avoid costly and slow civil proceedings or, in the case of victims, potentially distressing criminal proceedings, and this could in turn encourage more victims of harmful digital communications to come forward. Consultees also felt that a specialist civil enforcement body would be beneficial in cases involving young people where

¹⁰⁶ Nine social media companies are partners to the scheme: Facebook, Instagram, YouTube, Twitter, Google+, Ask.fm, Flickr, Yahoo! Answers and Yahoo! Groups.

¹⁰⁷ Office of the Children’s eSafety Commissioner, Submission on “Phenomenon colloquially referred to as ‘revenge porn’, which involves sharing private sexual images and recordings of a person without their consent, with the intention to cause that person harm” (January 2016) available at 4.

http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Revenge_porn/Submissions.

¹⁰⁸ *Ibid.*

¹⁰⁹ The Senate Legal and Constitutional Affairs References Committee, *Phenomenon colloquially referred to as ‘revenge porn’* (Senate Legal and Constitutional Affairs Committee secretariat, 2016) at 53.

¹¹⁰ *Ibid* at 52.

¹¹¹ *Ibid.*

¹¹² *Ibid.*

criminal proceedings may be unsuitable and civil actions are currently prohibitively expensive.

- 3.61 However, many consultees, while generally supporting the creation of such a body, also had particular concerns. One consultee stressed that were the body to have mediation functions then this would require effective resources, personnel, expertise and independence. In relation to the issue of resources, this consultee noted the lack of resources available to the Data Protection Commissioner and the criticism this has attracted, and suggested that the proposed body could experience similar difficulties. This consultee also noted that if the Office of Internet Safety were to take on a more proactive resolution function, as suggested in the Issues Paper, then this would require “careful consideration” on account of resources and expertise.
- 3.62 Consultees opposed to introducing a specialist body questioned whether such a body would be faster than the courts, especially as the specialist body’s proceedings are likely to be without prejudice to any criminal proceedings. One consultee noted that “[w]here the harmful activity complained of is undertaken maliciously, it is unlikely that it will cease on foot of anything short of an order of the court” and thus pursuing a complaint through the specialist body “would serve only to draw out proceedings”. They also maintained that “the institution of criminal or civil proceedings has an immediate chilling effect on the misbehaving party unrivalled by any non-court process.”
- 3.63 Another consultee noted that establishing such a body would require significant resources which “could be more effectively spent educating young people about their responsibilities online and the consequences that can attach to their actions should they choose to target other internet users.” They noted that individuals already have the option of making a complaint to the Data Protection Commissioner where data protection rights are potentially infringed. They also referred to the Commission’s proposal to introduce civil restraining orders for harassment and other harmful communications offences¹¹³ and suggested that this could “provide an effective remedy that would negate the need to establish a specialist body”, particularly if such orders could be obtained in the District Court through “a relatively straightforward and low cost process.”
- 3.64 Consultees also expressed concerns relating to due process and procedural fairness, and questioned whether such a body was “appropriate” for dealing with harmful digital communications given the importance of the rights that are infringed by such activity. One respondent to the Issues Paper believed that the creation of a non-court body to regulate such behaviour and protect the rights to privacy and data protection “would be rightly seen internationally as a relegation of these rights to secondary status.”
- 3.65 A consultee suggested that children and adults should be treated differently within this area, as posting harmful content online relating to children raises child protection issues that do not arise in the case of adults. Ireland has positive obligations under the Constitution and the UN Convention on the Rights of the Child to protect and vindicate the rights of children. Among the rights children have under the Convention is the right not to be “subjected to arbitrary or unlawful interference with his or her privacy, family or correspondence, nor to unlawful attacks on his or her honour and reputation” and children

¹¹³ See paragraphs 3.92-3.98 below.

have the “right to the protection of the law against such interference or attacks”.¹¹⁴ Thus, there is an obligation on the State to protect the right of children to privacy including protection of their reputation which requires a response that is specifically designed to meet the particular needs and vulnerabilities of children. This consultee suggested that the Ombudsman for Children would be a suitable entity to fulfil this role as this Office already has an investigative function alongside its role in promoting the rights and welfare of children.¹¹⁵

(4) Office of the Digital Safety Commissioner

- 3.66 As matters currently stand, while it would appear that the non-statutory self-regulation by social media companies, through their content and conduct policies, has improved in recent years, this may not be sufficient to address harmful communications effectively. A non-statutory approach depends on voluntary compliance, and is subject to change without any external assessment against standards. Thus, while recent years have seen improvements in these arrangements, additional measures may be necessary to ensure that an adequate response to harmful digital communications is available into the future. In the Commission’s 2015 *Report on Consumer Insurance Contracts* the Commission similarly identified the shortcomings of a non-statutory, voluntary, system of self-regulation.¹¹⁶ The Commission has therefore concluded that Ireland should follow the approach taken in Australia and therefore recommends that an office be established on statutory basis with dual roles in promoting digital and online safety and overseeing an efficient and effective take down procedure in relation to harmful digital communications.
- 3.67 The Australian model is preferable to the New Zealand scheme for a number of reasons. Firstly, the Australian model consists of a single body, which appears to be more efficient than the New Zealand two tier system which requires individuals to apply to a mediation type body first and then if this fails, to apply to court. This means that individuals could be waiting a significant amount of time for a solution to their case under the New Zealand system. In contrast, the Australian system has already proved to be working efficiently with an average turnaround on complaints of eight hours. Secondly, the Australian scheme allows social media sites to opt into it compared to the New Zealand mechanism which makes no provision for actively engaging and cooperating with social media companies. This cooperative aspect of the Australian scheme also appears to be a factor in the apparent efficacy of the scheme thus far.
- 3.68 However, unlike the Australian system which is confined to children, the Commission considers that both adults and children should have access to such a mechanism, as swift takedown of harmful content is a priority for all victims of harmful digital communications.
- 3.69 The Commission thus recommends that the Office of the Digital Safety Commissioner of Ireland should be established to promote digital and online safety as well as overseeing and regulating an efficient and effective procedure for takedown of harmful digital

¹¹⁴ UN General Assembly, *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, article 16.

¹¹⁵ See *Ombudsman for Children Act 2002*, sections 7-10.

¹¹⁶ Law Reform Commission, *Report on Consumer Insurance Contracts* (LRC 113-2015), at paragraphs 1.25 to 1.32

communications. The work of this Office would apply to material relating to both adults and children.

- 3.70 The Commission recommends that the oversight and regulatory role of the Digital Safety Commissioner should apply to a wide spectrum of digital or online service providers, including any undertaking that provides a digital or online service whether by the internet, a telecommunications system, the world wide web or otherwise. The Commission therefore proposes that the term “digital service undertaking” be used to describe the types of providers that the Digital Safety Commissioner would have responsibility for regulating in relation to the removal of harmful communications. The definition of “digital service undertaking” would include a non-exhaustive list extending to any undertaking that is described, whether in an enactment or otherwise, as an intermediary service provider, an internet service provider, an internet intermediary, an online intermediary, an online service provider, a search engine, a social media platform, a social media site, or a telecommunications undertaking.
- 3.71 The Commissioner would thus have two core functions, the first being an educational function which would involve promoting digital safety for all persons as well as supporting and encouraging the implementation of measures to improve digital safety and disseminating information relating to digital safety. This function would also extend to coordinating the activities of Government Departments and other public bodies and authorities relating to digital safety, supporting and conducting research on digital safety and publishing reports and papers related to digital safety.
- 3.72 The Commission also considers that the Office of the Ombudsman for Children (OCO) should have a role connected to the functions of the Digital Safety Commissioner. The OCO was established to promote children’s rights and welfare and so would be well placed to adopt a significant role in protecting children’s rights online. The OCO’s *Strategic Plan 2016-2018*¹¹⁷ appears to indicate that such a role would be consistent with its current priorities. The Strategic Plan contains three objectives, the second of which relates to building capacity among public organisations whose work impacts on children and young people to develop and implement a child rights based approach to their practice. One of the actions listed to help achieve this objective is a pledge to “work with others to encourage and support safe and effective participation in social and digital media by children and young people”.¹¹⁸
- 3.73 The Commission thus considers that the Digital Safety Commissioner could work in conjunction with the OCO in developing guidance material for schools on digital safety. Such guidance material should be prepared and distributed in partnership with the relevant Government Departments, notably the Department of Education and Skills and the Department of Children and Youth Affairs. This exercise should also involve other educational partners such as the National Council for Curriculum and Assessment, the National Parents Council and representative bodies of students and young people. The Commission has already discussed in Chapters 1 and 2 the importance of promoting positive digital citizenship, and also the need to avoid the application of the criminal law to children and young people. The guidance material envisaged, which would focus on

¹¹⁷ *Strategic Plan 2016-2018* (Office of the Ombudsman for Children, 2016).

¹¹⁸ *Strategic Plan 2016-2018* (Office of the Ombudsman for Children, 2016).

education and empowerment of children and young people, would therefore form a key aspect of national policy to deal with harmful communications by children and young people. This material could include guidance and assistance on the use of mediation within schools to resolve issues around harmful communications and to encourage restorative solutions. The Commission considers that this approach is also consistent with the analysis in the 2014 *Report of the Internet Content Governance Advisory Group*.¹¹⁹

- 3.74 The second core function of the Digital Safety Commissioner would involve overseeing a system of take down orders by digital service undertakings. This role would involve the development of a code of practice on take down procedure which the Commissioner would consult on widely before publishing in a form that is easily accessible.
- 3.75 The code of practice would, amongst other matters, (a) describe in detail, and provide practical guidance on, the take down procedure of digital service undertakings for harmful digital communications, (b) require that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge; (c) describe the steps required by a digital service undertaking to meet the National Digital Safety Standards (discussed below)(d) contain time lines within which a digital service undertaking must respond to complaints about different categories of harmful digital communications, and, in the event that such a complaint is upheld, the time lines within which the digital service undertaking is to take down each category of harmful digital communication. The Commission also recommends that the Commissioner should be able, if he or she considers it appropriate, to form an advisory working group to assist in the preparation of the code of practice and appoint suitable persons for that purpose.
- 3.76 The Digital Safety Commissioner's regulatory role would operate in a similar way as the Australian Children's e-Safety Commissioner by requiring digital service undertakings to comply with the code of practice developed by the Digital Safety Commissioner as well as National Digital Safety Standards. These standards would require a digital service undertaking to have in place a provision prohibiting the posting of harmful digital communications, a complaints scheme whereby users can request removal of harmful digital communications free of charge, a timeline for responding to complaints which would be no less stringent than the time lines specified in the code of practice and a contact person to engage with the Commissioner. If the Commissioner is satisfied that a digital service undertaking complies with the code of practice and the National Digital Safety Standards, then the Commissioner would be empowered to issue a certificate of compliance following an application by the undertaking.
- 3.77 The take down procedure regulated by the Commissioner would require a user to initially make their complaint directly to the relevant digital service undertaking. If the content was not taken down or did not comply with a take down timeline specified in the code of practice, then the user could make a complaint to the Commissioner. The digital service undertaking would thus be the first port of call and the Digital Safety Commissioner would be an appeal body only.
- 3.78 As part of this appeal process, the Commissioner would first investigate the complaint and consider submissions from the individual and the digital service undertaking. If the

¹¹⁹ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014).

Commissioner is satisfied after this investigative process that the undertaking has not complied with the code of practice or the National Digital Safety Standards, he or she would then make a determination that the complaint is upheld and direct the digital service undertaking to remove the specified communication. The Commissioner would also revoke the certificate of compliance issued to the relevant undertaking in the event that an appeal against that undertaking is upheld. The revocation would be subject to such terms as the Commissioner considers appropriate, including the circumstances in which the digital service undertaking may re-apply for a certificate of compliance.

- 3.79 If the undertaking refuses to comply with the direction of the Commissioner to remove the communication, then the Commissioner could apply to the Circuit Court for an order requiring compliance by the undertaking. If the Court is satisfied that the digital service undertaking has not complied with the code of practice or with the National Digital Safety Standards it would issue an injunction directing the undertaking to comply with the Commissioner's direction. The Commission does not consider it necessary to put in place any specific offence to ensure compliance with such an order of the Circuit Court. However, if the digital service undertaking does not comply with the injunction issued by the Circuit Court, then this would constitute criminal contempt of court.
- 3.80 The Commission considers that the Office of Internet Safety (OiS), which was established to take a lead responsibility for internet safety in Ireland, may be a suitable body to take on the role of the Digital Safety Commissioner. If the OiS was entrusted with this role this would be in keeping with, as well as expand upon, recommendations made in the 2014 *Report of the Internet Content Governance Advisory Group*.¹²⁰ The 2014 Report recommended an enlarged role for the OiS, stating that it "should be reconfigured to deal exclusively with issues of law enforcement and illegal online content" and that it "should be given clear terms of reference clarifying its role in providing oversight of the system of self-regulation for illegal internet content."¹²¹
- 3.81 The Commission does not in this Report make any recommendations on the details as to the funding, staffing and related matters concerning the Digital Safety Commissioner. These are matters outside the scope of the Commission's role and they require policy decisions on funding by the Government and Oireachtas.

- 3.82 **The Commission recommends that the Office of a Digital Safety Commissioner of Ireland should be established on a statutory basis to promote digital and online safety and to oversee and regulate a system of "take down" orders for harmful digital communications.**
- 3.83 **The Commission recommends that the Digital Safety Commissioner should have responsibility for overseeing and regulating a wide group of digital service undertakings including an intermediary service provider, an internet service provider, an internet intermediary, an online intermediary, an online service provider, a search engine, a social media platform, a social media site, or a telecommunications undertaking.**
- 3.84 **The Commission recommends that the general functions of the Digital Safety Commissioner should include: (a) to promote digital safety for all persons, (b)**

¹²⁰ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014).

¹²¹ *Ibid* at 63.

to support and encourage the implementation of measures to improve digital safety, (c) to ensure the oversight and regulation of a timely and efficient procedure for the take down, that is, removal, by digital service undertakings, of harmful digital communications (the “take down procedure”), (d) to ensure that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge, (e) to consult widely in the development of the code of practice, (f) to support the preparation and publication by the Ombudsman for Children of guidance material, including guidance material for schools, relevant to digital safety of children and to harmful digital communications, (g) to coordinate the activities of Government Departments and other public bodies and authorities relating to digital safety, (h) to collect, analyse, interpret and disseminate information relating to digital safety, (i) to support, encourage, conduct and evaluate research about digital safety and (j) to publish (whether on the internet or otherwise) reports and papers relating to digital safety.

- 3.85 The Commission recommends that the Digital Safety Commissioner should prepare and publish, in a form that is easily accessible, a Code of Practice on Take Down Procedure for Harmful Communications.
- 3.86 The Commission recommends that the code of practice must, among other matters: (a) describe in detail, and provide practical guidance on, the take down procedure of digital service undertakings for harmful digital communications; (b) require that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge; (c) describe the steps required by an digital service undertaking to meet the National Digital Safety Standards; and (d) contain time lines within which a digital service undertaking must respond to complaints about different categories of harmful digital communications, and, in the event that such a complaint is upheld, the time lines within which the digital service undertaking is to take down each category of harmful digital communication.
- 3.87 The Commission recommends that the Commissioner may, if he or she considers it appropriate, form an advisory working group to assist in the preparation of the code of practice and, if so, may appoint such persons as he or she considers suitable for that purpose.
- 3.88 The Commission recommends that digital service undertakings, including internet service providers and social media sites, must comply with specified National Digital Safety Standards.
- 3.89 The Commission recommends that a digital service undertaking should be able to apply to the Digital Safety Commissioner for a certificate that it complies with the code of practice and the National Digital Safety Standards.
- 3.90 The Commission recommends that the Digital Safety Commissioner should have jurisdiction to hear an appeal by an individual who has sought to have specified communications concerning him or her removed using the complaints scheme and take down procedure of a digital service undertaking.
- 3.91 The Commission recommends that, where a digital service undertaking refuses to comply with a direction issued by the Commissioner, the Commissioner should be empowered to apply to the Circuit Court for an injunction requiring compliance with the direction.

D Civil Restraint Orders

- 3.92 Unlike the UK *Protection from Harassment Act 1997*, section 10 of the *Non-Fatal Offences Against the Person Act 1997* does not allow separate civil proceedings to be brought based on its provisions. However, section 10(3) of the 1997 Act enables the court 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.”

- 3.93 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*¹²² 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 an order.

- 3.94 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” powers conferred by section 10.¹²³ 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.

¹²² [2014] IEHC 406.

¹²³ *Ibid* at paragraph 42.

- 3.95 Although this issue was not addressed by many of the respondents to the Issues Paper, all of those that did were in favour of introducing a separate statutory procedure to provide civil remedies for harassment. Respondents noted the lack of accessibility of the current procedure under section 10(5) which requires a victim to have initiated criminal proceedings in order to avail of civil redress. One consultee emphasised that such interdependence clearly limits proper redress and is likely to dissuade victims of harassment from taking formal action.
- 3.96 A number of consultees noted that that the UK *Protection from Harassment Act 1997* already provides for a hybrid criminal-civil system. Section 3 of the UK Act provides for a civil claim for “(among other things) any anxiety caused by the harassment and any financial loss resulting from the harassment”¹²⁴ as well as providing for an injunction to restrain the defendant from conduct amounting to harassment.¹²⁵ A consultee expressed the view that introducing a statutory tort for harassment would provide “a real deterrent against harassment and place an effective remedy directly in the hands of the victim” with criminal sanctions still available in the most egregious cases.
- 3.97 It was also noted by one consultee that many women who are harassed by their partner or ex-partner are not eligible as applicants for safety orders under section 2 of the *Domestic Violence Act 1996*, in particular, women in dating relationships who are not cohabiting with the perpetrator. Young women often have such relationships, and are also more likely to be victims of stalking and cyber-stalking in particular. This consultee also observed that even in the case of women who may be eligible as applicants for safety orders, “some stalking tactics, especially cyber-stalking” may be insufficient to actually trigger an order.¹²⁶ Thus, a civil non-harassment order could be of significant benefit in such cases.
- 3.98 The Commission thus recommends that the power to issue a restraining order should not be limited to instances where a criminal prosecution has been brought. The Commission considers that individuals should be able to apply to the Circuit Court for civil restraining orders which would prevent, for such a period as the court may specify, a person from communicating by any means of communication with or about the individual or require that the respondent shall not approach within such distance as the court shall specify of the place of residence or employment of the individual seeking the order. Failure to comply with the terms of such an order would constitute an offence with maximum penalties of a Class A fine and/or 6 months imprisonment on summary conviction and a fine and/or 2 years imprisonment on conviction on indictment.

- 3.99 **The Commission recommends that the Circuit Court may, on an application to it, make an order, having regard to the evidence presented and if the court is satisfied that it is in the interests of justice so to do, that a person shall not, for such period as the court may specify: (a) communicate by any means of communication with or about a named person, or (b) that the respondent shall**

¹²⁴ *Protection from Harassment Act 1997*, Section 3(2).

¹²⁵ *Protection from Harassment Act 1997*, Section 3(3).

¹²⁶ Under section 2(2) of the *Domestic Violence Act 1996*, a court may make a safety order if it “is of the opinion that there are reasonable grounds for believing that the safety or welfare of the applicant or any dependent so requires.”

not approach within such distance as the court shall specify of the place of residence or employment of a named person. This power to issue a restraining order should not be limited to instances where a criminal prosecution has been brought.

E *Norwich Pharmacal Orders*

- 3.100 *Norwich Pharmacal* orders are a type of discovery order which can be made where discovery is the sole object of the proceedings in circumstances where wrongdoing has been established and it is sought to establish the identity of those responsible for it.¹²⁷ The jurisdiction to make such orders was first established by the UK House of Lords in *Norwich Pharmacal Co. v Commissioners of Customs and Excise*¹²⁸ where Lord Reid articulated the principle underpinning the granting of such orders:

“If through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrongdoing, he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers”.¹²⁹

- 3.101 The jurisdiction to grant such orders was approved in Ireland by the Supreme Court in *Megaleasing UK Ltd v Barrett (No. 2)*.¹³⁰
- 3.102 In the type of cases with which this Report are concerned, *Norwich Pharmacal* orders are usually sought against an internet service provider, a social media site, or a telecoms company to reveal the name of a person who has posted harmful communications online but who has disguised his or her real identity.

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.¹³¹ Brookes successfully applied for a *Norwich Pharmacal* order compelling Facebook to reveal the identities of seven users who had abused her.¹³²

- 3.103 Clear wrongdoing has to be established before a *Norwich Pharmacal* order will be granted. This was emphasised by Finlay CJ in *Megaleasing*, where he noted that while such orders “may be of very considerable value towards the attainment of justice” the power to grant such orders “for good reasons must be sparingly used” and that in the original *Norwich Pharmacal* case “considerable stress was laid upon the very clear and unambiguous establishment of wrongdoing”.¹³³ Similarly, in *O’Brien v Red Flag Consulting Ltd & ors*, Mac Eochaidh J stated that the one feature that stands out amongst

¹²⁷ Delaney and McGrath *Civil Procedure in the Superior Courts* 3rd ed (Roundhall, 2012) at 455.

¹²⁸ [1974] AC 133.

¹²⁹ *Ibid* at 175.

¹³⁰ [1993] ILRM 497.

¹³¹ “Police officer arrested over Nicola Brookes Facebook abuse” *BBC News* 29 August 2012 available at <http://www.bbc.co.uk/news/uk-england-19414045>.

¹³² See Khan, “Can the trolls be put back under the bridge?” (2013) CTLR 9, at 11.

¹³³ [1993] ILRM 497 at 503.

the Irish *Norwich Pharmacal* cases is that “wrongdoing by unidentified persons, to a very high degree of probability, had been made out by the plaintiffs”.¹³⁴

- 3.104 The jurisdiction to grant a *Norwich Pharmacal* order is discretionary and necessitates that the requirements of justice and privacy be balanced. In *EMI Records Ltd v Eircom plc*¹³⁵ 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 clear wrongdoing and the potential for the procedure to interfere significantly with the right to privacy mean that such orders would appear to be rarely granted.¹³⁶ However, as these orders are often granted on an *ex parte* basis and are not reported in the media, it is difficult to know how many are actually granted.¹³⁷
- 3.105 *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. Neither the Circuit nor District Court has this jurisdiction being courts of local and limited jurisdiction.¹³⁸ This means that the cost of obtaining such an order is high and the remedy is not available to many individuals. The high cost of such orders was observed by Cregan J in *Sony Music Entertainment (Ireland) Ltd & ors v UPC (No. 1)* where he noted that the plaintiffs in the case had sought and obtained a number of *Norwich Pharmacal* orders against copyright infringers over the past number of years, however, “the legal costs involved in bringing such applications were enormous and utterly disproportionate to the financial returns from such applications”.¹³⁹ The plaintiffs thus ceased bringing such applications “because they were, quite simply, not worth the effort”.¹⁴⁰ Cregan J also noted in this case that having a protocol in place between the intended claimant and the ISP, as was the case between the plaintiffs and Eircom, would usually avoid any litigation costs and could also lead to an uncontested *Norwich Pharmacal* application if that was considered ultimately necessary.¹⁴¹ Thus, having a statutory regime in place in relation to the removal of harmful communications, as the Commission proposes, would also avoid much of the litigation costs associated with *Norwich Pharmacal* applications.
- 3.106 The 2014 *Report of the Internet Content Governance Advisory Group* has described existing civil procedures for tracing persons involved in harmful digital communications cases as “expensive, lacking detail and out of date”.¹⁴² The Report recommended that the *Rules of the Superior Court 1986*¹⁴³ be amended to provide specifically for the jurisdiction

¹³⁴ [2015] IEHC 867 at paragraph 21.

¹³⁵ [2005] 4 IR 148 at paragraph 10.

¹³⁶ See Abrahamson, Dwyer and Fitzpatrick *Discovery and Disclosure* 2nd ed (Round Hall, 2013) at 200, where the authors state that the jurisdiction to grant *Norwich Pharmacal* orders has “rarely been invoked in this jurisdiction”.

¹³⁷ One consultee observed that in their experience, the High Court is willing to issue such orders. They stated that many of the applications are heard on an *ex parte* basis as part of ongoing proceedings and are often dealt with “quickly and with a minimum of fuss”.

¹³⁸ Abrahamson, Dwyer and Fitzpatrick *Discovery and Disclosure* 2nd ed (Round Hall, 2013) at 207.

¹³⁹ [2015] IEHC 317 at paragraph 236.

¹⁴⁰ *Ibid.*

¹⁴¹ *Ibid* at paragraphs 237-239.

¹⁴² *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014) at 45.

¹⁴³ The Rules of the Superior Courts (S.I. No. 15 of 1986).

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”.¹⁴⁴

3.107 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;¹⁴⁵
- 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.”¹⁴⁶

3.108 A number of respondents to the Issues Paper agreed with the Internet Content Governance Advisory Group’s proposal to place *Norwich Pharmacal* orders on a statutory basis and allow applicants to seek such orders from the Circuit Court. However, consultees also suggested further reforms that could be made in connection to such orders. One consultee noted that at present, *Norwich Pharmacal* orders usually involve a two-step mechanism whereby an individual has to first seek an order against the relevant website to disclose user and IP details. This data once furnished may lead to data held by a telecoms company, many of whom require a second *Norwich Pharmacal* order before agreeing to disclosure. Thus, this consultee advocated introducing a one-step *Norwich Pharmacal* order which would apply to the named website and any service providers and telecoms companies who may be disclosed by the named website, which would be simpler and more cost effective for individuals as well as saving time for the courts.

3.109 Another respondent to the Issues Paper highlighted that *Norwich Pharmacal* orders are granted on “effectively an *ex-parte* basis” and that this is “deeply undesirable” particularly as such orders are irreversible. Thus, they submitted that anonymous users should be able to make representations to the court before they are stripped of their anonymity and that this could be done by adopting the procedure suggested in the UK case *Totalise plc. v The Motley Fool*.¹⁴⁷ This procedure would require the internet service provider (ISP) to notify the user who could then make written submissions via the ISP. The user would thus be given the opportunity to be heard on the application through a mechanism that would preserve their anonymity. This consultee emphasised that a procedure such as the one suggested “must be adopted if unwarranted infringements on the right to anonymity are to be avoided”.

3.110 The Commission supports the recommendations made by the Internet Content Governance Advisory Group in relation to *Norwich Pharmacal* orders. By placing such orders on a statutory basis and extending the jurisdiction to grant orders to the Circuit

¹⁴⁴ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014) at 46.

¹⁴⁵ This rule would seek to modernise and enhance Order 31, Rule 29 of the *Rules of the Superior Courts 1986*.

¹⁴⁶ *Report of the Internet Content Governance Advisory Group* (Department of Communications, Climate Action and Environment, 2014) at 46.

¹⁴⁷ [2001] EWCA Civ 1897.

Court, as well as the High Court, the accessibility of this procedure would be increased. Costs for litigants would also be reduced by making such orders available in the lower courts.

- 3.111 The Commission recommends that a one-step procedure for *Norwich Pharmacal* orders should be adopted as this would also reduce expenses as well as ensure a faster, more efficient process. The Commission also recommends that the person alleged to have posted the harmful communications should be given the opportunity of appearing and making representations to the court before the court makes a *Norwich Pharmacal* order. This would increase the transparency of the *Norwich Pharmacal* process and ensure that the right to fair procedures and anonymous speech is safeguarded.

3.112 The Commission recommends that the jurisdiction to grant *Norwich Pharmacal* orders be placed on a statutory basis and that both the High Court and the Circuit Court should be empowered to make such an Order.

3.113 The Commission recommends that a one-step procedure be adopted for such orders whereby only one application would be required which would apply, in the online context, to the website and the telecoms company.

3.114 The Commission recommends that the person alleged to have posted the harmful communications should be given the opportunity of appearing and making representations to the court before the court makes a *Norwich Pharmacal* order.

F Jurisdictional Issues and Civil Remedies Related to Harmful Digital Communications

- 3.115 As in criminal cases involving harmful digital communications,¹⁴⁸ jurisdiction also raises difficulties in the civil context, in particular, orders made by the Irish courts in online defamation cases involving foreign defendants may prove difficult to enforce. The Brussels 1 Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters,¹⁴⁹ provides that in general persons shall be sued in the State in which they are domiciled.¹⁵⁰ For tort actions, however, a person may be sued “in the courts for the place where the harmful event occurred.”¹⁵¹ In *Shevill v Presse Alliance SA*¹⁵² the EU Court of Justice held that this allows a plaintiff to bring civil proceedings

¹⁴⁸ See also the discussion in Chapter 2 at paragraphs 2.223-2.234, of the similar considerations that arise in connection with jurisdiction and extra-territorial effect in the context of harmful communications offences.

¹⁴⁹ 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)*.

¹⁵⁰ 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.

¹⁵¹ Article 5(3) of the Brussels 1 Regulation.

¹⁵² *Shevill v Presse Alliance SA* [1995] ECR I-415.

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*,¹⁵³ 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.¹⁵⁴

- 3.116 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".¹⁵⁵ 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 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.¹⁵⁶
- 3.117 The Commission considers that this may be an area which ultimately requires international coordination and cooperation, as the extra-territorial enforceability of Irish court orders depends not on Irish law but on the law of the foreign state in which the plaintiff seeks to enforce the particular order. This view was shared by respondents to the Issues Paper. This type of cooperation has already occurred at EU level, but beyond the EU, an international agreement may be needed to ensure that civil orders are enforceable. Nevertheless, the Commission recommends that limited extra-territorial jurisdiction apply in relation to the territorial scope of the Digital Safety Commissioner and the power of the High Court and the Circuit Court to issue *Norwich Pharmacal* orders.
- 3.118 Thus, the territorial scope of the Digital Safety Commissioner and *Norwich Pharmacal* orders should apply to harmful communications where: a) such harmful communications affect an Irish citizen or a person ordinarily resident in the State, and (b) the means of communication used in connection with such harmful communications are within the control of an undertaking or company established under the law of the State.
- 3.119 However, these should also have some extra-territorial effect in connection with an Irish citizen or a person ordinarily resident in the State. This would be where the means of communication used in connection with such harmful communications are within the control of an undertaking established under the law of another State but where a court established in the State would have jurisdiction to give notice of service outside the State in respect of civil proceedings to which such harmful communications refer. This therefore corresponds with the approach taken in connection with the extra-territorial

¹⁵³ Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH v X; Olivier Martinez v MGN Ltd* (25 October 2011).

¹⁵⁴ 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.

¹⁵⁵ *Grehan v Medical Inc* [1986] ILRM 629.

¹⁵⁶ See *Yahoo! Inc v LICRA* 169 F Supp 2d. 1181 (N.D. Cal. 2001) at 1185-6. This case is discussed at paragraph 1.64 above.

enforcement of civil proceedings generally, including under the “service out” procedures in Orders 11-11D of the *Rules of the Superior Courts 1986*.¹⁵⁷ This jurisdiction applies where a defendant is not within the State, but the proceedings may by reason of the subject matter or otherwise be so closely connected with Ireland or Irish law that the Irish courts should assume jurisdiction.¹⁵⁸ In such a case, leave to serve the proceedings will be granted either under Order 11 of the 1986 Rules which deals with service of proceedings on any person (individual or corporate) outside the State (other than in the EU), or under Orders 11A-D of the 1986 Rules, which deals with service on any person (individual or corporate) in the EU or from a Lugano Convention¹⁵⁹ contracting state.

- 3.120 The Commission’s recommendations on extra-territorial jurisdiction involving the role of the Digital Safety Commissioner and *Norwich Pharmacal* orders are also based on the provision on service out contained in the Commission’s *Report on Consolidation and Reform of the Courts Acts*.¹⁶⁰ This Report reiterates the existing rules concerning service out by providing that a Court document may be served, or notice given of a Court document outside the State: (a) as of right, and in accordance with rules of court where jurisdiction over the proceedings to which the Court document relates is conferred on a Court in the State under a European Union enactment or Convention; or (b) in any other case, with the permission of the Court before which it is intended to begin proceedings, and in accordance with the order of the Court giving permission and with rules of court.

3.121 The Commission recommends that the provisions concerning the Office of the Digital Safety Commissioner and concerning *Norwich Pharmacal* orders should apply to harmful communications where:

- a) such harmful communications affect an Irish citizen or a person ordinarily resident in the State, and the means of communication used in connection with such harmful communications are within the control of an undertaking or company established under the law of the State and**
- b) such harmful communications affect an Irish citizen or a person ordinarily resident in the State and where the means of communication used in connection with such harmful communications are within the control to any extent of an undertaking established under the law of another State and where a court established in the State would have jurisdiction to give notice of service outside the State in respect of civil proceedings to which harmful communications refer.**

¹⁵⁷ *The Rules of the Superior Courts* (S.I. No. 15 of 1986), Orders 11-11D.

¹⁵⁸ Delaney and McGrath *Civil Procedure in the Superior Courts* 3rd ed (Roundhall, 2012) at 12.

¹⁵⁹ *Convention on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters* signed in Lugano on 30 October 2007. The signatories of this Convention are the EU, Switzerland, Denmark, Norway and Iceland.

¹⁶⁰ Law Reform Commission, *Report on Consolidation and Reform of the Courts Acts* (LRC 97-2010), at 203 and 484-485.

CHAPTER 4 SUMMARY OF RECOMMENDATIONS

The Recommendations made by the Commission in this Report are as follows:

A Chapter 2: Reform of Criminal Law Concerning Harmful Communications

- 4.01 The Commission recommends that the legislation included in this Report on harmful communications should apply to all forms of communication, whether offline or online, analogue or digital, and therefore should include communication by letter, telephone (including SMS text message), camera, or digital or online communication such as through a social media site or other internet medium. The Commission also recommends that the existing criminal law on harmful communications, together with the reforms proposed in this Report, should be consolidated into a single piece of legislation. [paragraph 2.53]
- 4.02 The Commission recommends that section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be repealed, and replaced by an offence of harassment that is modelled on section 10 and that includes two additional provisions: (a) that the harassment offence should expressly apply to harassment by any means of communication, including through digital and online communications; and (b) that it should deal with indirect forms of communication, such as setting up fake online social media profiles. [paragraph 2.54]
- 4.03 The Commission recommends that an offence of stalking separate from the related offence of harassment should be enacted. The Commission recommends that the essential ingredients of the stalking offence should be the same as the harassment offence, whereby the offence would be committed where a person “stalks” another person by persistently following, watching, pestering or besetting another person or by persistently communicating by any means of communication with the other person or by persistently communicating with a third person by any means of communication about the other person. However, the stalking offence would differ from the harassment offence by requiring the intentional or reckless acts of the perpetrator to interfere seriously with the victim’s peace and privacy and cause him or her alarm, distress or harm, as opposed to the harassment offence which makes these alternative requirements. [paragraph 2.76]
- 4.04 The Commission recommends that section 13 of the *Post Office (Amendment) Act 1951* be repealed and replaced with an offence of distributing a threatening, false, indecent or obscene message by any means of communication and with the intent to cause alarm, distress or harm or being reckless as to this. [paragraph 2.187]
- 4.05 The Commission recommends that the provision for forfeiture of any apparatus, equipment or other thing under section 13 of the *Post Office (Amendment) Act 1951* should apply to all harmful communications offences included in the Report. [paragraph 2.188]

- 4.06 The Commission recommends the enactment of an indictable offence of distributing an intimate image without the consent of the person depicted in the image, or threatening to do so, and with the intent to cause alarm, distress of harm or being reckless as to this. [paragraph 2.204]
- 4.07 The Commission recommends the enactment of a summary, strict liability offence of taking or distributing an intimate image of another person without the other person's consent. [paragraph 2.205]
- 4.08 The Commission recommends that the definition of "consent" applicable to the intimate images offences should be that a person agrees by choice and that the person has the freedom and capacity to make that choice. [paragraph 2.206]
- 4.09 The Commission recommends "intimate image" should be defined as a visual recording of a person made by any means including a photographic, film or video recording: (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, and (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 image is communicated. [paragraph 2.207]
- 4.10 The Commission recommends that the definition of "intimate image" should also include what has been described as "upskirting" and "downblousing", that is, an image of the person's genital or anal region or in the case of a female of her breasts, whether the genital or anal region or, as the case may be, the breasts were covered by underwear or were bare. [paragraph 2.208]
- 4.11 The Commission recommends that the definition of "intimate image" should include "photo-shopping," that is, where part of a person's image, usually his or her face, is superimposed on the intimate parts (nude, or partially nude) of another person's body, so that the definition should apply to a photographic, film or video recording, whether or not the image of the person has been altered in any way. [paragraph 2.209]
- 4.12 The Commission recommends that in any prosecution for a harmful communications offence provided for in the Report, the privacy of the person to whom the offence relates should be protected, broadly by analogy with comparable provisions as to reporting restrictions in existing legislation (including their modification or removal), as well as providing for waiver by the person to whom the offence relates. [paragraph 2.215]
- 4.13 The Commission recommends that no prosecution for the harmful communications offences discussed in the Report should be brought against persons under the age of 17 years except by or with the consent of the Director of Public Prosecutions. [paragraph 2.218]
- 4.14 The Commission recommends that the general 6 month time limit for prosecuting summarily, provided for in section 10(4) of the *Petty Sessions Ireland Act 1851*, be extended to 2 years for the harmful communications offences in the Report. [paragraph 2.221]
- 4.15 The Commission recommends that extra-territorial effect should apply to the harmful communications offences in the Report:
- where a harmful communications offence is committed by a person in the State in relation to a means of communication that is located outside the State,

- where a harmful communications offence is committed by a person outside the State in relation to a means of communication that is located in the State or
 - where a harmful communications offence is committed by a person outside the State if the person is an Irish citizen, a person ordinarily resident in the State, an undertaking established under the law of the State, a company formed and registered under the *Companies Act 2014* or an existing company within the meaning of the *Companies Act 2014* and the offence is an offence under the law of the place where the act was committed. [paragraph 2.233]
- 4.16 The Commission recommends, because the maximum penalties for the harassment offence in section 10 of the *Non-Fatal Offences Against the Person Act 1997* are sufficient and provide a suitable upper level for penalties, these penalties should apply to all comparable indictable harmful communications offences provided for in the Report. The Commission also recommends that the offence of taking or distributing an intimate image without consent should be a summary offence only, with maximum penalties on conviction of a Class A fine and/or 6 months imprisonment. [paragraph 2.244]
- 4.17 The Commission recommends that hate speech should be addressed as part of the general reform of hate crime law, which falls outside the scope of this Report. [paragraph 2.256]

B Chapter 3: Digital Safety, Takedown Procedure and Civil Law

- 4.18 The Commission recommends that the Office of a Digital Safety Commissioner of Ireland should be established on a statutory basis to promote digital and online safety and to oversee and regulate a system of “take down” orders for harmful digital communications. [paragraph 3.82]
- 4.19 The Commission recommends that the Digital Safety Commissioner should have responsibility for overseeing and regulating a wide group of digital service undertakings including an intermediary service provider, an internet service provider, an internet intermediary, an online intermediary, an online service provider, a search engine, a social media platform, a social media site, or a telecommunications undertaking. [paragraph 3.83]
- 4.20 The Commission recommends that the general functions of the Digital Safety Commissioner should include: (a) to promote digital safety for all persons, (b) to support and encourage the implementation of measures to improve digital safety, (c) to ensure the oversight and regulation of a timely and efficient procedure for the take down, that is, removal, by digital service undertakings, of harmful digital communications (the “take down procedure”), (d) to ensure that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge, (e) to consult widely in the development of the code of practice, (f) to support the preparation and publication by the Ombudsman for Children of guidance material, including guidance material for schools, relevant to digital safety of children and to harmful digital communications, (g) to coordinate the activities of Government Departments and other public bodies and authorities relating to digital safety, (h) to collect, analyse, interpret and disseminate information relating to digital safety, (i) to support, encourage, conduct and

- evaluate research about digital safety and (j) to publish (whether on the internet or otherwise) reports and papers relating to digital safety. [paragraph 3.84]
- 4.21 The Commission recommends that the Digital Safety Commissioner should prepare and publish, in a form that is easily accessible, a Code of Practice on Take Down Procedure for Harmful Communications. [paragraph 3.85]
- 4.22 The Commission recommends that the code of practice must, among other matters: (a) describe in detail, and provide practical guidance on, the take down procedure of digital service undertakings for harmful digital communications; (b) require that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge; (c) describe the steps required by a digital service undertaking to meet the National Digital Safety Standards; and (d) contain time lines within which a digital service undertaking must respond to complaints about different categories of harmful digital communications, and, in the event that such a complaint is upheld, the time lines within which the digital service undertaking is to take down each category of harmful digital communication. [paragraph 3.86]
- 4.23 The Commission recommends that the Commissioner may, if he or she considers it appropriate, form an advisory working group to assist in the preparation of the code of practice and, if so, may appoint such persons as he or she considers suitable for that purpose. [paragraph 3.87]
- 4.24 The Commission recommends that digital service undertakings, including internet service providers and social media sites, must comply with specified National Digital Safety Standards. [paragraph 3.88]
- 4.25 The Commission recommends that a digital service undertaking should be able to apply to the Digital Safety Commissioner for a certificate that it complies with the code of practice and the National Digital Safety Standards. [paragraph 3.89]
- 4.26 The Commission recommends that the Digital Safety Commissioner should have jurisdiction to hear an appeal by an individual who has sought to have specified communications concerning him or her removed using the complaints scheme and take down procedure of a digital service undertaking. [paragraph 3.90]
- 4.27 The Commission recommends that, where a digital service undertaking refuses to comply with a direction issued by the Commissioner, the Commissioner should be empowered to apply to the Circuit Court for an injunction requiring compliance with the direction. [paragraph 3.91]
- 4.28 The Commission recommends that the Circuit Court may, on an application to it, make an order, having regard to the evidence presented and if the court is satisfied that it is in the interests of justice so to do, that a person shall not, for such period as the court may specify: (a) communicate by any means of communication with or about a named person, or (b) that the respondent shall not approach within such distance as the court shall specify of the place of residence or employment of a named person. This power to issue a restraining order should not be limited to instances where a criminal prosecution has been brought. [paragraph 3.99]
- 4.29 The Commission recommends that the jurisdiction to grant *Norwich Pharmacal* orders be placed on a statutory basis and that both the High Court and the Circuit Court should be empowered to make such an Order. [paragraph 3.112]

- 4.30 The Commission recommends that a one-step procedure be adopted for such orders whereby only one application would be required which would apply, in the online context, to the website and the telecoms company. [paragraph 3.113]
- 4.31 The Commission recommends that the person alleged to have posted the harmful communications should be given the opportunity of appearing and making representations to the court before the court makes a *Norwich Pharmacal* order. [paragraph 3.114]
- 4.32 The Commission recommends that the provisions concerning the Office of the Digital Safety Commissioner and concerning *Norwich Pharmacal* orders should apply to harmful communications where:
- a) such harmful communications affect an Irish citizen or a person ordinarily resident in the State, and the means of communication used in connection with such harmful communications are within the control of an undertaking or company established under the law of the State and
 - b) such harmful communications affect an Irish citizen or a person ordinarily resident in the State and where the means of communication used in connection with such harmful communications are within the control to any extent of an undertaking established under the law of another State and where a court established in the State would have jurisdiction to give notice of service outside the State in respect of civil proceedings to which harmful communications refer. [paragraph 3.121].

APPENDIX A

DRAFT
HARMFUL COMMUNICATIONS AND DIGITAL SAFETY BILL 2016

CONTENTS

Section

PART 1
Preliminary and General

1. Short title and commencement
2. Interpretation
3. Repeals

PART 2
Harmful Communications

4. Distributing intimate image without consent, or threatening to do so, with intent to cause harm
5. Taking or distributing intimate image without consent
6. Distributing threatening or false message
7. Harassment
8. Stalking
9. Liability of directors and officers of undertakings
10. Jurisdiction for Part 2
11. Evidence in proceedings for offences outside State
12. Double jeopardy
13. Summary proceedings: time limit of 2 years
14. Consent of Director of Public Prosecutions
15. Protection of privacy of person to whom offence relates
16. Forfeiture of apparatus etc on conviction
17. Civil restraint orders

PART 3
Digital Safety

18. Digital Safety Commissioner of Ireland¹
19. Functions of Commissioner
20. Code of practice on take down procedure for harmful communications
21. Duties of digital service undertakings: National Digital Safety Standards, including take down procedure
22. Certificate of compliance with code of practice and National Digital Safety Standards
23. Appeal to Commissioner: investigation and direction
24. Enforcement in Circuit Court of direction by Commissioner
25. Powers of courts in intended civil proceedings
26. Jurisdiction for Part 3

¹ As discussed in the Report, Part 3 of this Bill does not contain details as to the funding, staffing and related matters concerning the Digital Safety Commissioner. These are outside the scope of the Law Reform Commission's role, and require decisions by the Government and Oireachtas.

ACTS REFERRED TO

Companies Act 2014 (No.38 of 2014)
Interpretation Act 2005 (No.23 of 2005)
Non-Fatal Offences Against the Person Act 1997 (No.26 of 1997)
Petty Sessions (Ireland) Act 1851 (14 & 15 Vict, c.93)
Post Office (Amendment) Act 1951 (No.17 of 1951)

DRAFT

HARMFUL COMMUNICATIONS AND DIGITAL SAFETY BILL 2016

BILL

entitled

An Act to consolidate and reform the criminal law concerning harmful communications, to repeal certain provisions of the Post Office (Amendment) Act 1951 and the Non-Fatal Offences Against the Person Act 1997, to provide for the establishment of a body to be known, in the English language, as the Office of the Digital Safety Commissioner of Ireland or, in the Irish language, as Oifig an Choimisinéara Sábháilteachta Dhigiteach na hÉireann, to promote and encourage measures to improve digital safety for all persons, to provide for a take-down procedure for harmful digital communications, to provide for oversight of the take-down procedure by the Digital Safety Commissioner of Ireland, to confer certain powers on the courts in respect of intended civil proceedings, and to provide for related matters.

Be it enacted by the Oireachtas as follows:

PART 1

Preliminary and General

Short title and commencement

1. — (1) This Act may be cited as the Harmful Communications and Digital Safety Act 2016.

(2) This Act comes into operation on such day or days as the Minister for Justice and Equality, with the consent of the Minister for Children and Youth Affairs and the Minister for Communications, Climate Action and Environment, may appoint by order or orders either generally or with reference to any particular purpose or provision, and different days may be so appointed for different purposes or provisions.

Explanatory Note

Section 1 contains standard provisions on the Short Title of the Bill and commencement arrangements.

Interpretation

2. — In this Act —

“communication” means any form of communication, including by speech, by letter, by camera, by telephone (including SMS text message), by smart phone, by any digital or online communication (including the internet, a search engine, a social media platform, a social media site or the world wide web), or by any other telecommunications system; and “communicated”, “communications” and “means of communication” shall be interpreted accordingly;

“consent” means that a person agrees by choice and that the person has the freedom and capacity to make that choice;

“digital service undertaking” means an undertaking that provides a digital or online service whether by the internet, a telecommunications system, the world wide web or otherwise, and includes an undertaking that is described, whether in an enactment or otherwise, as an intermediary service provider, an internet service provider, an internet intermediary, an online intermediary, an online service provider, a search engine, a social media platform, a social media site, or a telecommunications undertaking;

“enactment” has the same meaning as in the Interpretation Act 2005;

“intimate image” means a visual recording of a person made by any means including a photographic, film or video recording (whether or not the image of the person has been altered in any way)—

- (a) (i) of the person’s genital or anal region or in the case of a female of her breasts (whether the genital or anal region or, as the case may be, the breasts are covered by underwear or are bare), or
- (ii) in which the person is nude, is exposing his or her genital organs or anal region or in the case of a female is exposing her breasts, or
- (iii) in which the person is engaged in explicit sexual activity,

and

- (b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy (and such circumstances can include that the recording was made when the person whose image was recorded was in a public place),

and

- (c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the image is communicated;

“undertaking” means a person being an individual, a body corporate or an unincorporated body of persons engaged in the production, supply or distribution of goods or the provision of a service (whether carried on by him or her for profit or not).

Explanatory Note

Section 2 contains important definitions for the purposes of the Bill.

The definition of “communication” implements the recommendation in **paragraph 2.53** that the proposed legislation on harmful communications should apply to all forms of communication, whether offline or online, analogue or digital, and therefore the definition includes communication by speech, by letter, by camera, by telephone (including SMS text message), by smart phone, by any digital or online communication (including the internet, a search engine, a social media platform, a social media site or the world wide web), or by any other telecommunications system.

The definition of “consent” implements the recommendation in **paragraph 2.206** that consent should correspond to the Commission’s general approach to consent for the purposes of the law on sexual offences, namely, that it means that a person agrees by choice and where the person has the freedom and capacity to make that choice. The Report notes that, while the primary

purpose of the offences proposed in *sections 4 and 5* of this Bill is to protect against harmful interferences with privacy and that they are therefore not sexual offences as such, it is appropriate that because they involve issues of great intimacy the general concept of consent that applies in sexual offences should apply to them.

The definition of “digital service undertaking” implements the recommendation in **paragraph 3.83** that the legislation should apply to a wide spectrum of digital or online service providers. The definition therefore refers to any undertaking that provides a digital or online service whether by the internet, a telecommunications system, the world wide web or otherwise. The definition also includes a non-exhaustive list: any undertaking that is described, whether in an enactment or otherwise, as an intermediary service provider, an internet service provider, an internet intermediary, an online intermediary, an online service provider, a search engine, a social media platform, a social media site, or a telecommunications undertaking.

The definition of “intimate image” implements the recommendation in **paragraph 2.207** that this should include the definition used in the *Canadian Criminal Code*, namely a visual recording of a person made by any means including a photographic, film or video recording: (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, and (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 image is communicated.

The definition of “intimate image” also implements the recommendation in **paragraph 2.208** that the definition used in the *Canadian Criminal Code* should be supplemented to ensure that it includes what has been described as “upskirting” and “downblousing”, that is, an image of the person’s genital or anal region or in the case of a female of her breasts, whether the genital or anal region or, as the case may be, the breasts were covered by underwear or were bare.

The definition of “intimate image” also implements the recommendation in **paragraph 2.209** that it should include “photo-shopping,” that is, where part of a person’s image, usually his or her face, is superimposed on the intimate parts (nude, or partially nude) of another person’s body.

The definition of “undertaking” is a standard provision (to which, for example, *section 9* of the Bill refers) and is defined as a person being an individual, a body corporate or an unincorporated body of persons engaged in the production, supply or distribution of goods or the provision of a service (whether carried on by him or her for profit or not).

Repeals

3. — Section 13 of the *Post Office (Amendment) Act 1951* and section 10 of the *Non-Fatal Offences Against the Person Act 1997* are repealed.

Explanatory Note

Section 3 of the Bill implements the recommendation in **paragraph 2.187** that section 13 of the *Post Office (Amendment) Act 1951* should be repealed and replaced by the offence set out in *section 6* of the Bill; and the recommendation in **paragraph 2.54** that section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be repealed and replaced by the offence set out in *section 7* of the Bill.

PART 2

Harmful Communications

Distributing intimate image without consent, or threatening to do so, with intent to cause harm

4. —(1) A person commits an offence where he or she, without lawful authority or reasonable excuse and in the circumstances referred to in *subsection (2)*, by any means of communication distributes or publishes an intimate image of another person (in this section referred to as the other person) without the consent of the other person, or threatens to do so.

(2) The circumstances are that the person who distributes or publishes the intimate material, or who threatens to do so, does so where—

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

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

(3) A person who commits an offence under this section is liable—

(a) on summary conviction to a Class A fine or to imprisonment for a term not exceeding 12 months or to both, or

(b) on conviction on indictment to a fine or to imprisonment for a term not exceeding 7 years or to both.

Explanatory Note

Section 4 of the Bill implements the recommendation in **paragraph 2.204** that it should be an offence for a person to distribute or publish an intimate image of another person without the other person's consent, or to threaten to do so. This is intended to deal with the intentional shaming behaviour sometimes referred to as "revenge porn."

Section 4(2) provides that the offence can occur with a "once-off" act (by contrast with the persistence required in harassment or stalking: see *sections 7 and 8* of the Bill) or by more than one act. *Section 4(2)* also provides that the essential ingredients of the offence are, broadly, based on those in the harassment offence in section 10 of the *Non-Fatal Offences Against the Person Act 1997*, namely that: (a) the accused, by his or her act or acts intentionally or recklessly, seriously interferes with the other person's peace and privacy or causes alarm, distress or harm to the other person; and (b) his or her act or acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm, distress or harm to the other person. An important difference is that one act could be sufficient to constitute an offence under *section 4*, as opposed to the requirement of persistent acts for harassment and stalking: see *section 7* of the Bill (which is to replace the harassment offence in section 10 of the 1997 Act) and *section 8* of the Bill (the new offence of stalking).

Section 4(3) provides that the penalties for the offence are the same as those for the harassment offence in section 10 of the 1997 Act (and in *sections 7 and 8* of the Bill): (a) on summary conviction, a Class A fine (a fine of up to €5,000) and/or up to 12 months imprisonment; or (b) on conviction on indictment, an unlimited fine and/or up to 7 years imprisonment.

Taking or distributing intimate image without consent

5. —(1) A person commits an offence where he or she, without lawful authority or reasonable excuse and in the circumstances referred to in *subsection (2)*, by any means of communication takes, or distributes or publishes an intimate image of another person (in this section referred to as the other person) without the consent of the other person.

(2) The circumstances are that the person who takes, or distributes or publishes the intimate material does so where he or she, by his or her acts seriously interferes with the other person's peace and privacy or causes alarm, distress or harm to the other person.

(3) A person who commits an offence under this section is liable on summary conviction to a Class A fine or to imprisonment for a term not exceeding 6 months or to both.

Explanatory Note

Section 5 of the Bill implements the recommendation in **paragraph 2.205** that it should be an offence for a person to take, or distribute or publish, an intimate image of another person without the other person's consent.

Section 5 of the Bill is aimed at behaviour that falls short of the intentional, egregious, activity associated with the shaming offence sometimes referred to as "revenge porn dealt with in *section 4*. *Section 5* of the Bill therefore corresponds with the kind of behaviour that is sometimes described in other jurisdictions as "upskirting" or "downblousing." The offence in *section 5* may, in some respects, be thought of as being associated with the behaviour known as "sexting" but it differs in a fundamental way in that it is committed only where the intimate image is taken without consent. It remains a separate question, which is outside the scope of the criminal law, as to whether it is appropriate or suitable for persons, whether young persons or adults, to distribute intimate images. This might be more appropriate for discussion in, for example, the guidance material that the Office of the Ombudsman for Children (with the support of the Digital Safety Commissioner) may publish under *section 19(f)* of the Bill.

Section 5(2) provides that some ingredients of the offence are based on those in the harassment offence in section 10 of the *Non-Fatal Offences Against the Person Act 1997*, namely, that the accused by his or her acts seriously interferes with the other person's peace and privacy or causes alarm, distress or harm to the other person. However, the offence in *section 5* differs in an important respect from harassment because it does not require that the accused has acted either intentionally or recklessly: the offence occurs simply by the taking, distributing or publishing of an intimate image without consent. It is therefore a strict liability offence, and for this reason also it has been proposed as a summary offence only. It also differs from harassment or stalking in that it can involve a "once-off" act.

Section 5(3) provides that the offence is a summary offence, the penalties being a Class A fine (a fine of up to €5,000) and/or up to 6 months imprisonment.

Distributing threatening or false message

6. —(1) A person commits an offence where he or she, without lawful authority or reasonable excuse and in the circumstances referred to in *subsection (2)*, by any means of communication distributes or publishes a threatening, false, indecent or obscene message to or about another person (in this section referred to as the other person).

(2) The circumstances are that the person who distributes or publishes the message does so —

(a) intentionally or recklessly for the purpose of causing alarm, distress or harm to the other person, or

(b) persistently.

(3) A person who commits an offence under this section is liable —

(a) on summary conviction to a Class A fine or to imprisonment for a term not exceeding 12 months or to both, or

(b) on conviction on indictment to a fine or to imprisonment for a term not exceeding 7 years or to both.

Explanatory Note

Section 6 of the Bill implements the recommendation in **paragraph 2.187** that the offence in section 13 of the *Post Office (Amendment) Act 1951* of sending a menacing or false message by post or telephone (originally enacted to deal with “poison pen” letters, and later extended to include “crank” phone calls and text messages) should be replaced by a comparable offence that applies to all forms of communications, including messages distributed online through social media, and that this should include not only messages to a person but also about a person.

Section 6(2) provides that the essential ingredients of the offence are that the person distributes or publishes the message either: (a) intentionally or recklessly for the purpose of causing alarm, distress or harm to the other person, or (b) persistently. This is broadly based on the factors in section 13 of the 1951 Act, but the wording has been aligned with the “harm” test in section 10 of the *Non-Fatal Offences Against the Person Act 1997* (also used in *sections 4, 7 and 8* of the Bill).

Section 6(2)(a) reflects section 13 of the 1951 Act in that one act could be sufficient to constitute an offence under *section 6*, while *section 6(2)(b)* also reflects section 13 of the 1951 Act in that it can involve persistent acts, and can thus be compared with harassment and stalking: see *section 7* of the Bill (which is to replace the harassment offence in section 10 of the 1997 Act) and *section 8* of the Bill (the new offence of stalking).

Section 6(2) of the Bill has omitted any wording from section 13 of the 1951 Act that could be vulnerable to being found unconstitutional on the grounds that they were vague or overly broad in scope (notably the words “grossly offensive”).

Section 6(3) provides that the penalties for the offence are the same as those for the harassment offence in section 10 of the 1997 Act (and in *sections 4, 7 and 8* of the Bill): (a) on summary conviction to a Class A fine (a fine of up to €5,000) and/or up to 12 months imprisonment; or (b) on conviction on indictment to an unlimited fine and/or up to 7 years imprisonment.

Harassment

7.—(1) A person commits an offence where he or she, without lawful authority or reasonable excuse, harasses another person (in this section referred to as the other person) by —

- (a) persistently following, watching, pestering or besetting the other person, or
- (b) persistently communicating by any means of communication with the other person, or
- (c) persistently communicating with a third person by any means of communication about the other person.

(2) For the purposes of this section a person harasses the other person where—

- (a) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other person's peace and privacy or causes alarm, distress or harm to the other person, and
- (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm, distress or harm to the other person.

(3) A person who commits an offence under this section is liable —

- (a) on summary conviction to a Class A fine or to imprisonment for a term not exceeding 12 months or to both, or
- (b) on conviction on indictment to a fine or to imprisonment for a term not exceeding 7 years or to both.

Explanatory Note

Section 7 of the Bill implements the recommendation in **paragraph 2.54** that the harassment offence in section 10 of the *Non-Fatal Offences Against the Person Act 1997* should be replaced and re-enacted with two important amendments: (a) that the harassment offence should expressly apply to harassment by any means of communication, including through digital and online communications; and (b) that it should deal with indirect form of communications, such as setting up fake online social media profiles. As recommended in **paragraph 2.54**, *section 2* of the Bill therefore proposes to repeal section 10 of the 1997 Act, which is then replaced by *section 7*.

Section 7(2) provides that the essential ingredients of the offence are those in the harassment offence in section 10 of the 1997 Act, namely that: (a) the accused, by his or her acts intentionally or recklessly, seriously interferes with the other person's peace and privacy or causes alarm, distress or harm to the other person; and (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm, distress or harm to the other person. *Section 7* of the Bill retains the requirement of "persistence" which is a recognised aspect of harassment. By contrast, the offences in *sections 4 to 6* of the Bill can be committed by a "once-off" act.

Section 7(3) provides that the penalties for the offence are the same as those for the harassment offence in section 10 of the 1997 Act (and in *sections 4 and 8* of the Bill): (a) on summary conviction to a Class A fine (a fine of up to €5,000) and/or up to 12 months imprisonment for a term not exceeding; or (b) on conviction on indictment to an unlimited fine and/or up to 7 years imprisonment.

Stalking

8.—(1) A person commits an offence where he or she, without lawful authority or reasonable excuse, stalks another person (in this section referred to as the other person) by —

- (a) persistently following, watching, pestering or besetting the other person, or
- (b) persistently communicating by any means of communication with the other person, or
- (c) persistently communicating with a third person by any means of communication about the other person.

(2) For the purposes of this section a person stalks the other person where—

- (a) he or she, by his or her acts intentionally or recklessly, seriously interferes with the other person's peace and privacy, and
- (b) causes alarm, distress or harm to the other person, and
- (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy and cause alarm, distress or harm to the other person.

(3) A person who commits an offence under this section is liable —

- (a) on summary conviction to a Class A fine or to imprisonment for a term not exceeding 12 months or to both, or
- (b) on conviction on indictment to a fine or to imprisonment for a term not exceeding 7 years or to both.

Explanatory Note

Section 8 of the Bill implements the recommendation in **paragraph 2.76** that an offence of stalking, separate from the related offence of harassment, should be enacted. The essential ingredients of the stalking offence are, broadly, similar to those in the harassment offence now set out in *section 7* of the Bill. As discussed in the Report, the Commission agrees with the view that stalking is, in effect, an aggravated form of harassment that can be committed by a former relationship partner, although this is not the only setting in which it can occur. For this reason, the specific ingredients of stalking in *section 8* of the Bill differ in one, albeit significant, respect from those for the harassment offence now in *section 7* of the Bill: the accused must, by his or her acts intentionally or recklessly, seriously interfere with the other person's peace and privacy, *and must* (as opposed to "or" for harassment) cause alarm, distress or harm to the other person. As with harassment, the stalker's acts must be such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm, distress or harm to the other person.

Section 8(3) provides that the penalties for the stalking offence are the same as those for harassment under *section 7* (and the offences under *sections 4 and 6*): (a) on summary conviction to a Class A fine (a fine of up to €5,000) and/or up to 12 months imprisonment for a term not exceeding; or (b) on conviction on indictment to an unlimited fine and/or up to 7 years imprisonment. While stalking is an aggravated form of harassment, the Report concludes that it is not necessary to provide for a higher maximum sentence in *section 8* than is provided for in *section 7* (the maximum sentence in Irish law for harassment and stalking being already greater

than in other jurisdictions, such as the UK), and that the relevant aggravating factors in an individual case can suitably be taken into account at the sentencing stage.

Liability of directors and officers of undertakings

9.—(1) Where an offence under this Part has been committed by an undertaking and the doing of the acts that constituted the offence has been authorised, or consented to by, or is attributable to connivance or wilful neglect on the part of, a person, being a director, manager or other similar officer of the undertaking, or a person who purports to act in any such capacity, that person as well as the undertaking shall be guilty of an offence and shall be liable to be proceeded against and punished as if he or she were guilty of the first-mentioned offence.

(2) Where a person is proceeded against as aforesaid for such an offence and it is proved that, at the material time, he or she was a director of the undertaking concerned or a person employed by it whose duties included making decisions that, to a significant extent, could have affected the management of the undertaking, or a person who purported to act in any such capacity, it shall be presumed, until the contrary is proved, that the doing of the acts by the undertaking which constituted the commission by it of the offence concerned under any of the relevant statutory provisions was authorised, consented to or attributable to connivance or neglect on the part of that person.

(3) Where the affairs of a body corporate are managed by its members, subsections (1) and (2) shall apply in relation to the acts or defaults of a member in connection with his or her functions of management as if he or she were a director of the body corporate.

Explanatory Note

Section 9 of the Bill is a standard provision concerning the personal criminal liability of directors and officers of “undertakings” (defined in *section 2* of the Bill) where an offence under *Part 2* of the Bill has been committed by an undertaking.

Jurisdiction for Part 2

10. — (1) A person may be tried in the State for an offence under this Part in relation to an act, to which this subsection applies by virtue of subsection (2), committed, whether in whole or in part—

(a) by the person in the State in relation to a means of communication that is located outside the State,

(b) by the person outside the State in relation to a means of communication that is located in the State, or

(c) by the person outside the State in relation to a means of communication that is located outside the State if—

(i) that person is a person to whom this subparagraph applies by virtue of subsection (3), and

(ii) the act is an offence under the law of the place where the act was committed.

(2) Subsection (1) applies to an act which, if it had been committed by a person in the State in relation to a means of communication that is located in the State, would constitute an offence under this Part.

(3) Subsection (1)(c)(i) applies to each of the following persons—

- (a) an Irish citizen;
- (b) a person ordinarily resident in the State;
- (c) an undertaking established under the law of the State;
- (d) a company formed and registered under the Companies Act 2014;
- (e) an existing company within the meaning of the Companies Act 2014.

(4) For the purpose of this section, a person shall be deemed to be ordinarily resident in the State if he or she has had his or her principal residence in the State for the period of 12 months immediately preceding the alleged commission of an offence under this Part.

(5) Proceedings for an offence to which subsection (1)(c) applies may be taken in any place in the State and the offence may for all incidental purposes be treated as having been committed in that place.

Explanatory Note

Section 10 of the Bill implements the recommendation in **paragraph 2.233** concerning the territorial jurisdiction of the offences in the Bill. The text is based on section 10 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*, which proposes to implement the territorial provisions in Article 12 of Directive 2013/40/EU on attacks on information systems.

Evidence in proceedings for offences outside State

11. — (1) In any proceedings relating to an offence under this Part in circumstances in which *section 10* applies—

- (a) a certificate that is signed by an officer of the Minister for Foreign Affairs and Trade and stating that a passport was issued by the Minister to a person on a specified date, and
- (b) a certificate that is signed by an officer of the Minister and stating that, to the best of the officer's knowledge and belief, the person has not ceased to be an Irish citizen,

shall be evidence that the person was an Irish citizen on the date on which the relevant offence concerned is alleged to have been committed, unless the contrary is shown.

(2) A document purporting to be a certificate under subsection (1)(a) or (b) is deemed, unless the contrary is shown—

- (a) to be such a certificate, and
- (b) to have been signed by the person purporting to have signed it.

Explanatory Note

Section 11 of the Bill is a standard provision concerning evidential matters related to offences committed outside the State. The text is based on section 11 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

Double jeopardy

12.— (1) Where a person has been acquitted of an offence in a place outside the State, he or she shall not be proceeded against for an offence under this Part consisting of the alleged act or acts constituting the first-mentioned offence.

(2) Where a person has been convicted of an offence in a place outside the State, he or she shall not be proceeded against for an offence under this Part consisting of the act or acts constituting the first-mentioned offence.

Explanatory Note

Section 12 of the Bill is a standard provision to avoid double jeopardy in respect of offences comparable to those in this Bill committed outside the State. The text is based on section 12 of the *Criminal Justice (Offences Relating to Information Systems) Bill 2016*.

Summary proceedings: time limit of 2 years

13. — Notwithstanding section 10(4) of the Petty Sessions (Ireland) Act 1851, summary proceedings for an offence under this Part may be instituted at any time within 2 years from the date on which the offence was committed.

Explanatory Note

Section 13 implements the recommendation in **paragraph 2.221** that a 2 year time limit for bringing a summary prosecution for the offences under Part 2 of the Bill should apply, rather than the standard 6 month time limit in section 10(4) of the *Petty Sessions (Ireland) Act 1851*.

Consent of Director of Public Prosecutions

14.— Proceedings against a person under the age of 17 charged with an offence under this Part shall not be taken except by or with the consent of the Director of Public Prosecutions.

Explanatory Note

Section 14 implements the recommendation in **paragraph 2.218** that proceedings against a person under the age of 17 charged with an offence under the Bill should require the consent of the Director of Public Prosecutions. This is to ensure that in the case, for example, of distribution of intimate images between persons under the age of 17 (and in respect of which the summary offence in *section 5* of the Bill might arise), a clear decision-making process at national level is in place to ensure that a consistent prosecutorial approach applies. This is also intended to ensure that, where appropriate, the diversion provisions of the *Children Act 2001* can be applied in suitable cases.

Protection of privacy of person to whom offence relates

15. — (1) After a person is charged with an offence under this Part, no matter likely to lead members of the public to identify any person as a person in relation to whom the offence is alleged to have been committed (in this section referred to as the relevant person) shall be published in a publication available to the public or broadcast, except as authorised by a direction given in pursuance of this section.

(2) If, at any stage before the commencement of a trial of a person for an offence under this Part, the relevant person or the prosecution applies to a judge of the Circuit Court, on notice to the accused, for a direction in pursuance of this subsection and satisfies the judge—

(a) that the relevant person consents to waiving the application of subsection (1), or

(b) that the direction is required for the purpose of inducing persons to come forward who are likely to be needed as witnesses at the trial,

the judge shall direct that subsection (1) shall not apply to such matter relating to the relevant person as is specified in the direction.

(3) If, at any stage before the commencement of a trial of a person for an offence under this Part, he or she or another person, against whom the relevant person may be expected to give evidence at the trial, applies to a judge of the Circuit Court for a direction in pursuance of this subsection and satisfies the judge—

(a) that the direction is required for the purpose of inducing persons to come forward who are likely to be needed as witnesses at the trial, and

(b) that the conduct of the applicant's defence at the trial is likely to be adversely affected if the direction is not given,

the judge shall direct that subsection (1) shall not, by virtue of the charge alleging the offence under this Part, apply to such matter relating to the relevant person as is specified in the direction.

(4) If at a trial of a person for an offence under this Part, he or she or another person who is also charged at the trial applies to the judge for a direction in pursuance of this subsection and satisfies the judge—

(a) that the direction is required for the purpose of inducing persons to come forward who are likely to be needed as witnesses at the trial,

(b) that the conduct of the applicant's defence at the trial is likely to be adversely affected if the direction is not given, and

(c) that there was good reason for his or her not having made an application under subsection (3) before the commencement of the trial,

the judge shall direct that subsection (1) shall not, by virtue of the charge alleging the offence under this Part, apply to such matter relating to the relevant person as is specified in the direction.

(5) Without prejudice to subsection (2), if at a trial for an offence under this Part the judge is satisfied that the effect of subsection (1) is to impose a substantial and unreasonable restriction on the reporting of proceedings at the trial and that it is in the public interest to remove or relax the restriction, the judge shall direct that subsection (1) shall not apply to such matter relating to the

relevant person as is specified in the direction; but a direction shall not be given in pursuance of this subsection by reason only of an acquittal of an accused person at the trial.

(6) If a person who has been convicted of an offence under this Part and given notice of appeal against the conviction applies to the appellate court for a direction in pursuance of this subsection and satisfies the court—

(a) that the direction is required for the purpose of obtaining evidence in support of the appeal, and

(b) that the applicant is likely to suffer injustice if the direction is not given,

the court shall direct that subsection (1) shall not apply to such matter relating to a specified relevant person and offence under this Part as is specified in the direction.

(7) If any matter is published or broadcast in contravention of subsection (1), the following persons shall be guilty of an offence namely—

(a) in the case of matter published in a newspaper or periodical publication, the proprietor, the editor and the publisher;

(b) in the case of matter published in any other publication, the publisher; and

(c) in the case of matter broadcast, any person who transmits or provides the programme in which the broadcast is made and any person who performs functions in relation to the programme corresponding to those of the editor of a newspaper.

(8) Nothing in this section shall be construed as—

(a) prohibiting the publication or broadcast of matter consisting only of a report of legal proceedings other than proceedings at, or intended to lead to, or an appeal arising out of, a trial of a person for an offence under this Part, or

(b) affecting any prohibition or restriction imposed by virtue of any other enactment upon the publication or broadcasting of any matter.

(9) A person who commits an offence under this section is liable—

(a) on summary conviction, to a class B fine or to imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine or to imprisonment for a term not exceeding 3 years or both.

(10) It shall be a defence for a person who is charged with an offence under this section to prove that at the time of the alleged offence the person was not aware, and neither suspected nor had reason to suspect, that the matter alleged to have been published or broadcast was a matter specified in this section.

(11) In this section—

“broadcast” means the transmission, relaying or distribution by wireless telegraphy or by any other means or by wireless telegraphy in conjunction with any other means of communications, sounds, signs, visual images or signals, intended for direct reception by

the general public whether such communications, sounds, signs, visual images or signals are actually received or not;

“published” means published to any person, and includes published on the internet;

“publication” includes a film, sound track or any other record in permanent form (including a record that is not in a legible form but which is capable of being reproduced in a legible form) but does not include an indictment or other document prepared for use in particular legal proceedings.

Explanatory Note

Section 15 implements the recommendation in **paragraph 2.215** that in any prosecution for an offence under the Bill, the identity of the person in relation to whom the offence is alleged to have been committed should be protected; and that this protection should, in general, mirror the reporting restrictions that protect the privacy of a person in relation to whom a sexual offence is alleged to have been committed.

Thus, *section 15* is, broadly, modelled on the reporting restrictions in section 7 of the *Criminal Law (Rape) Act 1981* (as amended) and provides that, in general, no matter likely to lead members of the public to identify any person as a person in relation to whom the offence is alleged to have been committed (referred to in the 1981 Act as the complainant, and in *section 15* of the Bill as the relevant person) shall be published in a publication available to the public or broadcast, except as authorised by a direction given under the section.

Similarly *section 15* of the Bill, like section 7 of the 1981 Act, provides that the accused may apply to court for a direction to have the reporting restrictions removed and that the court must give such a direction if satisfied (a) that the direction is required for the purpose of inducing persons to come forward who are likely to be needed as witnesses at the trial, and (b) that the conduct of the applicant’s defence at the trial is likely to be adversely affected if the direction is not given.

Section 15(2) of the Bill adds an additional provision not found in section 7 of the 1981 Act by providing for an application by the person against whom an offence under the Bill is alleged to have been committed to consent to waiving the ban on reporting of her or his name. And, unlike section 7 of the 1981 Act, *section 15* of the Bill does not provide for anonymity of the accused: this is because, while it is important to protect the privacy of the person against whom an offence under the Bill is alleged to have been committed, the offences in the Bill are not sexual offences and therefore the full panoply of the provisions in the 1981 Act do not apply.

Forfeiture of apparatus etc on conviction

16. — Where a person is convicted of an offence under this Part, the court may, in addition to any other penalty imposed for the offence, order any apparatus, equipment or other thing used in the course of committing the offence to be forfeited to the State.

Explanatory Note

Section 16 implements the recommendation in **paragraph 2.188** that the provision for forfeiture of any apparatus, equipment or other thing used in the course of committing the offence under section 13 of the *Post Office (Amendment) Act 1951* (replaced by *section 6* of this Bill) should apply to all offences under this Bill.

Civil restraint orders

17.—(1) The Circuit Court may, upon an application to it in that behalf, make an order, having regard to the evidence presented and if the court is satisfied that it is in the interests of justice so to do, that a person (in this section referred to as the respondent) shall not, for such period as the court may specify—

(a) communicate by any means of communication with or about a named person, or

(b) that the respondent shall not approach within such distance as the court shall specify of the place of residence or employment of a named person.

(2) A person who fails to comply with the terms of an order under subsection (1) commits an offence and is liable—

(a) on summary conviction to a Class A fine or to imprisonment for a term not exceeding 6 months or to both, or

(b) on conviction on indictment to a fine or to imprisonment for a term not exceeding 2 years or to both.

Explanatory Note

Section 17 implements the recommendation in **paragraph 3.99** that the Circuit Court may, on an application to it, make an order, having regard to the evidence presented and if the court is satisfied that it is in the interests of justice so to do, that a person shall not, for such period as the court may specify: (a) communicate by any means of communication with or about a named person, or (b) that the respondent shall not approach within such distance as the court shall specify of the place of residence or employment of a named person. This is based on the comparable powers in section 10(3) of the *Non-Fatal Offences Against the Person Act 1997*, but which are limited to cases where a prosecution for harassment has been brought. The Commission recommends in **paragraph 3.99** that this power to issue a restraining order should not be limited to instances where a criminal prosecution has been brought.

PART 3

Digital Safety

Digital Safety Commissioner of Ireland²

18.— (1) The Minister for Justice and Equality, with the consent of the Minister for Children and Youth Affairs and the Minister for Communications, Climate Action and Environment, shall, by order, appoint a day to be the establishment day for the purposes of this Part.

(2) On the establishment day there shall stand established a body to be known, in the English language, as the Office of the Digital Safety Commissioner of Ireland or, in the Irish language, as Oifig an Choimisinéara Sábháilteachta Dhigiteach na hÉireann.

(3) On the establishment day the Minister for Justice and Equality, with the consent of the Minister for Children and Youth Affairs and the Minister for Communications, Climate Action and

² As discussed in the Report, Part 3 of this Bill does not contain details as to the funding, staffing and related matters concerning the Digital Safety Commissioner of Ireland. These are outside the scope of the Law Reform Commission's role, and require decisions by the Government and Oireachtas.

Environment, shall appoint a suitably qualified person to be the Digital Safety Commissioner of Ireland (in this Act referred to as the Commissioner).

Explanatory Note

Section 18 implements the recommendation in **paragraph 3.82** that the Office of a Digital Safety Commissioner of Ireland should be established to promote digital and online safety and to oversee and regulate a system of “take down” orders for harmful digital communications.

Section 18 provides that the Office is to be established by a statutory order to be made by the Minister for Justice and Equality, with the consent of two other relevant Government Ministers, the Minister for Children and Youth Affairs and the Minister for Communications, Climate Action and Environment. As discussed in the Report, the provisions of *Part 3* of the Bill do not contain details as to the funding, staffing and related matters concerning the Digital Safety Commissioner of Ireland. These are outside the scope of the Law Reform Commission’s role, and require decisions by the Government and Oireachtas.

As also discussed in the Report, the provisions in *Part 3* of the Bill are derived from comparable provisions in the Australian *Enhancing Online Safety for Children Act 2015*. As the title of the Australian 2015 Act indicates, the functions of its Online Safety Commissioner are limited to harmful material directed at children. The Commission recommends in the Report that the proposed legislation, as set out in *Part 3* of the Bill, should apply to harmful material directed at both adults and children.

Functions of Commissioner

19.— The functions of the Commissioner are —

- (a) to promote digital safety for all persons,
- (b) to support and encourage the implementation of measures to improve digital safety,
- (c) to ensure the oversight and regulation, in accordance with this Part, of a timely and efficient procedure for the take down, that is, removal, by digital service undertakings, of harmful digital communications, including the harmful communications referred to in *sections 4 to 8* (in this Part referred to as the “take down procedure”),
- (d) to ensure that the take down procedure is made available to all affected individual persons by digital service providers free of charge,
- (e) to consult widely in the development of the code of practice referred to in *section 20*, including with the public, with such Government Departments as he or she considers appropriate, with the Ombudsman for Children, with such other public bodies as he or she considers appropriate, with digital service undertakings and with such other persons as he or she considers appropriate,
- (f) to support the preparation and publication by the Ombudsman for Children of guidance material, including guidance material for schools, relevant to digital safety of children and to harmful digital communications, including the harmful communications referred to in *sections 4 to 8*,

- (g) to coordinate the activities of Government Departments and other public bodies and authorities relating to digital safety,
- (h) to collect, analyse, interpret and disseminate information relating to digital safety,
- (i) to support, encourage, conduct and evaluate research about digital safety,
- (j) to publish (whether on the internet or otherwise) reports and papers relating to digital safety, and
- (k) such other functions, if any, as may be conferred in writing by the Minister for Justice and Equality, with the consent of the Minister for Children and Youth Affairs and the Minister for Communications, Climate Action and Environment.

Explanatory Note

Section 19 implements the recommendation in **paragraph 3.84** to set out the general functions of the Digital Safety Commissioner in connection with promoting digital and online safety and overseeing a system of “take down” orders by digital service undertakings, including internet service providers and social media sites, for harmful digital communications.

Section 19 therefore provides that the functions of the Digital Safety Commissioner include:

- (a) to promote digital safety for all persons,
- (b) to support and encourage the implementation of measures to improve digital safety,
- (c) to ensure the oversight and regulation, in accordance with *Part 3* of the Bill, of a timely and efficient procedure for the take down, that is, removal, by digital service undertakings, of harmful digital communications, including the harmful communications referred to in *sections 4 to 8* (the “take down procedure”),
- (d) to ensure that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge,
- (e) to consult widely in the development of the code of practice referred to in *section 20* of the Bill,
- (f) to support the preparation and publication by the Ombudsman for Children of guidance material, including guidance material for schools, relevant to digital safety of children and to harmful digital communications,
- (g) to coordinate the activities of Government Departments and other public bodies and authorities relating to digital safety,
- (h) to collect, analyse, interpret and disseminate information relating to digital safety,
- (i) to support, encourage, conduct and evaluate research about digital safety and
- (j) to publish (whether on the internet or otherwise) reports and papers relating to digital safety.

As noted in the Report and above, these are derived from comparable provisions in the Australian *Enhancing Online Safety for Children Act 2015*.

Code of practice on take down procedure for harmful communications

20.— (1) The Commissioner shall, as soon as is practicable after his or her appointment, prepare, and publish in a form that is easily accessible, a code of practice on take down procedure for harmful communications (in this section referred to as the code of practice) that shall, *inter alia*—

(a) describe in detail, and provide practical guidance on, the take down procedure of digital service undertakings for harmful digital communications, including the harmful communications referred to in *sections 4 to 8*,

(b) require that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge,

(c) describe the steps required by a digital service undertaking to meet the national digital safety standards referred to in *section 21*, and

(d) contain time lines within which a digital service undertaking shall respond to complaints about different categories of harmful digital communications, including the harmful communications referred to in *sections 4 to 8*, and, in the event that such a complaint is upheld, the time lines within which the digital service undertaking is to take down each category.

(2) The Commissioner may, if he or she considers it appropriate, form an advisory working group to assist in the preparation of the code of practice and, if so, may appoint such and so many persons as he or she considers suitable for that purpose.

Explanatory Note

Section 20 implements the recommendation in **paragraph 3.85** that the Digital Safety Commissioner must prepare and publish, in a form that is easily accessible, a statutory code of practice on take down procedure for harmful communications.

Section 20(1) implements the recommendation in **paragraph 3.86** that the code of practice must, among other matters: (a) describe in detail, and provide practical guidance on, the take down procedure of digital service undertakings for harmful digital communications, including the harmful communications referred to in *sections 4 to 8* of the Bill; (b) require that the take down procedure is made available to all affected individual persons by digital service undertakings free of charge; (c) describe the steps required by an digital service undertaking to meet the national digital safety standards referred to in *section 21*, below; and (d) contain time lines within which a digital service undertaking must respond to complaints about different categories of harmful digital communications, including the harmful communications referred to in *sections 4 to 8*, and, in the event that such a complaint is upheld, the time lines within which the digital service undertaking is to take down each category of harmful digital communication.

Section 20(2) implements the recommendation in **paragraph 3.87** that the Commissioner may, if he or she considers it appropriate, form an advisory working group to assist in the preparation of the code of practice and, if so, may appoint such persons as he or she considers suitable for that purpose.

Duties of digital service undertakings: National Digital Safety Standards, including take down procedure

21.— For the purposes of this Part, a digital service undertaking shall ensure that it complies with the following National Digital Safety Standards—

(a) the digital service undertaking's terms of use shall contain—

(i) a provision that prohibits end-users from posting harmful digital communications, including the harmful communications referred to in *sections 4 to 8*, or

- (ii) a provision that may reasonably be regarded as the equivalent of a provision covered by subparagraph (i),
- (b) the digital service undertaking shall have a complaints scheme under which its end-users can request the take down, that is, the removal from the digital service undertaking's service, of harmful digital communications (including the harmful communications referred to in *sections 4 to 8*) that breach the service's terms of use,
- (c) the digital service undertaking's take down procedure shall be made available to all affected individual persons free of charge,
- (d) the digital service undertaking's take down procedure shall comply with the requirements of the code of practice issued under *section 20*,
- (e) without prejudice to *paragraph (d)*, the time lines within which the digital service undertaking shall respond to complaints about different categories of harmful digital communications, including the harmful communications referred to in *sections 4 to 8* and, in the event that such a complaint is upheld, the time lines within which the digital service undertaking is to take down each category, shall, at least, be no less stringent than the time lines specified in the code of practice issued under *section 20*,
- (f) the digital service undertaking shall appoint a suitably qualified individual, who shall be an employee or agent of the digital service undertaking, as its digital safety officer for the purposes of this Part, and
- (g) the contact details of the digital safety officer shall be notified to the Commissioner.

Explanatory Note

Section 21 implements the recommendation in **paragraph 3.88** that digital service undertakings, including internet service providers and social media sites, must comply with specified National Digital Safety Standards.

Section 21 of the Bill therefore provides that the National Digital Safety Standards are:

- (a) the digital service undertaking's terms of use must contain a provision that prohibits end-users from posting harmful digital communications, including the harmful communications referred to in *sections 4 to 8*, or an equivalent provision;
- (b) the digital service undertaking must have a complaints scheme under which its end-users can request the take down, that is, the removal from the digital service undertaking's service, of harmful digital communications (including the harmful communications referred to in *sections 4 to 8*) that breach the service's terms of use;
- (c) the digital service undertaking's take down procedure must be made available to all affected individual persons free of charge;
- (d) the digital service undertaking's take down procedure must comply with the requirements of the Code of Practice on Take Down Procedure issued under *section 20* of the Bill;
- (e) the time lines within which the digital service undertaking must respond to complaints about different categories of harmful digital communications (including the harmful communications referred to in *sections 4 to 8*) and, in the event that such a complaint is upheld, the time lines within which the digital service undertaking is to take down each category, must, at least, be no less stringent than the time lines specified in the code of practice issued under *section 20*;
- (f) the digital service undertaking must appoint a suitably qualified individual, who must be an employee or agent of the digital service undertaking, as its digital safety officer for the purposes of *Part 3* of the Bill; and

(g) the contact details of the digital safety officer must be notified to the Digital Safety Commissioner.

These standards are derived from comparable provisions in the Australian *Enhancing Online Safety for Children Act 2015*.

Certificate of compliance with code of practice and National Digital Safety Standards

22.—(1) A digital service undertaking may apply in writing to the Commissioner, in such form as the Commissioner approves, for a certificate that it complies with the code of practice issued under *section 20* and with the National Digital Safety Standards in *section 21*.

(2) If the Commissioner is satisfied that the digital service undertaking complies with the code of practice issued under *section 20* and with the National Digital Safety Standards in *section 21* the Commissioner shall, in writing, issue a certificate of compliance to the digital service undertaking for the purposes of this Part.

(3) Where the Commissioner issues such a certificate, the Commissioner shall thereafter presume, until the contrary is established (including in the course of making a determination under *section 23*), that the digital service undertaking complies with the code of practice issued under *section 20* and with the National Digital Safety Standards in *section 21*.

(4) The Commissioner shall, from time to time, monitor compliance with the code of practice by each digital service undertaking to whom such a certificate has been issued, and each digital service undertaking shall not unreasonably refuse to cooperate with such compliance monitoring.

(5) If, following such a monitoring procedure, the Commissioner is satisfied, having heard and considered the views of the digital service undertaking, that it is not complying with the code of practice issued under *section 20* or with the National Digital Safety Standards in *section 21*, the Commissioner shall revoke the certificate of compliance issued to the digital service undertaking.

(6) The revocation referred to in *subsection (5)* shall be subject to such terms, if any, as the Commissioner considers appropriate, including the circumstances in which the digital service undertaking may re-apply for a certificate of compliance.

Explanatory Note

Section 22 implements the recommendation in **paragraph 3.89** concerning the effect of the Commissioner issuing a certificate that digital service undertakings, including internet service providers and social media sites, comply with the code of practice on take down procedure issued under *section 20* and with the National Digital Safety Standards in *section 21*.

Section 22(1) and (2) thus provide that digital service undertakings may apply to the Commissioner for such a certificate of compliance.

Section 22(3) provides that if the Commissioner issues a certificate of compliance he or she must then presume (until the contrary is established, including in the course of making a determination under *section 23* of the Bill), that the digital service undertaking complies with the code of practice issued under *section 20* and with the National Digital Safety Standards in *section 21*.

Section 22(4) to (6) provide that the Commissioner must, from time to time, monitor compliance with the code of practice by each digital service undertaking to whom such a certificate has been issued, and each digital service undertaking must cooperate with such compliance monitoring. If, following such a monitoring procedure, the Commissioner is satisfied, having heard and

considered the views of the digital service undertaking, that it is not complying with the code of practice issued under *section 20* or with the National Digital Safety Standards in *section 21* of the Bill, the Commissioner must revoke the certificate of compliance issued to the digital service undertaking. The revocation referred is to be subject to such terms, if any, as the Commissioner considers appropriate, including the circumstances in which the digital service undertaking may re-apply for a certificate of compliance.

The oversight and monitoring procedures of digital service undertakings by the Commissioner in *section 22* of the Bill are derived from comparable provisions in the Australian *Enhancing Online Safety for Children Act 2015*.

Appeal to Commissioner: investigation and direction

23.—(1) An individual who has sought to have specified communications concerning him or her removed using the complaints scheme and take-down procedure of a digital service undertaking referred to in *section 21* may, if the digital service undertaking did not take down the specified communications or did not comply with a take-down timeline specified in the code of practice issued under *section 20*, make an appeal to the Commissioner in such form as the Commissioner shall prescribe.

(2) The Commissioner shall investigate the appeal and, if satisfied, having considered the respective submissions of the individual and of the digital service undertaking, that the digital service undertaking has not complied with the code of practice issued under *section 20* or with the National Digital Safety Standards in *section 21*, shall make a determination that the appeal shall be upheld and shall issue a direction in writing to the digital service undertaking to remove the specified communications forthwith.

(3) Where the Commissioner upholds an appeal under *subsection (2)*, he or she shall also revoke any certificate of compliance issued to the digital service undertaking under *section 22*, and such revocation shall be subject to such terms, if any, as the Commissioner considers appropriate, including the circumstances in which the digital service undertaking may re-apply for a certificate of compliance.

Explanatory Note

Section 23 implements the recommendation in **paragraph 3.90** that the Digital Safety Commissioner should have jurisdiction to hear an appeal by an individual who has sought to have specified communications concerning him or her removed using the complaints scheme and take-down procedure of a digital service undertaking under *section 21*. The digital service undertaking, such as an internet service provider or social media site, is to be the first port of call, and the Digital Safety Commissioner is to be an appeal body.

Section 23(1) therefore provides that an individual who has sought to have specified communications concerning him or her removed using the complaints scheme and take-down procedure referred to in *section 21* may, if the digital service undertaking did not take down the specified communications or did not comply with a take-down timeline specified in the code of practice issued under *section 20*, make an appeal to the Commissioner in such form as the Commissioner is to prescribe.

Section 23(2) provides that the Commissioner must investigate the appeal and, if satisfied, having considered the submissions of the individual and of the digital service undertaking, that the digital service undertaking has not complied with the code of practice issued under *section 20* or with the National Digital Safety Standards in *section 21*, must allow the appeal and must issue a direction in writing to the digital service undertaking to remove the specified communications forthwith.

Section 23(3) provides that where the Commissioner upholds an appeal, he or she must also revoke any certificate of compliance issued to the digital service undertaking under *section 22*, subject to such terms, if any, as the Commissioner considers appropriate, including the circumstances in which the digital service undertaking may re-apply for a certificate of compliance.

Enforcement in Circuit Court of direction by Commissioner

24.—(1) Where a digital service undertaking refuses to comply with a direction issued by the Commissioner under *section 23*, the Commissioner shall apply to the Circuit Court, on notice to the digital service undertaking, for an injunction requiring compliance with the direction.

(2) The Court, having heard and considered the respective submissions of the Commissioner and the digital service undertaking, and if it is satisfied that the digital service undertaking has not complied with the code of practice issued under *section 20* or with the National Digital Safety Standards in *section 21*, shall by order issue an injunction directing the digital service undertaking to comply with the direction issued by the Commissioner under *section 23*.

Explanatory Note

Section 24(1) implements the recommendation in **paragraph 3.91** that, where a digital service undertaking refuses to comply with a direction issued by the Commissioner under *section 22*, the Commissioner should be empowered to apply to the Circuit Court for an injunction requiring compliance with the direction.

Section 24(2) provides that the Court, having heard and considered the respective submissions of the Commissioner and the digital service undertaking, and if it is satisfied that the digital service undertaking has not complied with the code of practice issued under *section 20* or with the National Digital Safety Standards in *section 21*, shall by order issue an injunction directing the digital service undertaking to comply with the direction issued by the Commissioner under *section 23*.

The Commission's Report recommends that, for the purposes of ensuring an appropriate level of oversight and regulation by the Digital Safety Commissioner of this area, it is not necessary to put in place any specific offence to ensure compliance with such an order of the Circuit Court. The Report notes, nonetheless, that if the Circuit Court issues an injunction after a hearing under *section 23*, failure by a digital service undertaking to comply with the injunction would constitute criminal contempt of court.

Powers of courts in intended civil proceedings

25. — (1) The Circuit Court or High Court may hear and decide an application by a person (in this section referred to as the intended applicant) for an order under subsection (2) related to civil proceedings which the intended applicant intends to begin before either Court and which concern harmful communications, including the harmful communications referred to in *sections 4 to 8*.

(2) The application referred to in subsection (1) is for an order (sometimes referred to as a *Norwich Pharmacal* order) directed at a person or, as the case may be, persons (in this section referred to as the third party or, as the case may be, third parties) to disclose either the name of another person (in this section referred to as the intended respondent) against whom the intended applicant intends to bring the proceedings referred to in subsection (1) or the address (which may be a digital address) of the intended respondent, or both the name and address.

(3) The court may, in its discretion, grant an order under subsection (2), subject to such terms, if any, as it considers suitable, if the intended applicant has established to the court on the balance of probabilities that there is a *prima facie* demonstration of wrongful activity by the intended respondent, and that the intended respondent has engaged in such wrongful activity through the third party or, as the case may be, the third parties, including through a digital service or services operated by the third party or, as the case may be, the third parties as a digital service undertaking or, as the case may be, as digital service undertakings.

(4) Before making an order under subsection (2), the court may, in its discretion, order (subject to such terms, if any, as it considers suitable) that the third party or, as the case may be, the third parties, serve notice on the intended respondent in order to allow the intended respondent to appear and to make representations to the court.

Explanatory Note

Section 25(1) and (2) of the Bill implement the recommendation in **paragraph 3.112** that the power to issue what is sometimes referred to as a *Norwich Pharmacal* order (named after an English case in which this order was first made) should be placed on a statutory footing, and that both the High Court and the Circuit Court should be empowered to make such an order. A *Norwich Pharmacal* order is an order requiring a person or persons to disclose the name of another person against whom the applicant intends to bring civil proceedings. In the type of cases with which this Report and Bill are concerned, this usually involves applying to an internet service provider, a social media site, or a telecoms company to reveal the name of a person who has posted harmful communications online but who has disguised his or her real identity. At present, a *Norwich Pharmacal* order can only be issued by the High Court, which the Report points out involves significantly more cost than would be the case if such an order could be applied for and made in the Circuit Court.

Section 25(3) of the Bill, by referring to an application against a “third party or, as the case may be, third parties,” implements the recommendation in **paragraph 3.113** that a one-step procedure should apply to applying for such orders, so that only one application would be required which would apply, in the online context, to the website, social media company or a telecoms company.

Section 25(4) of the Bill implements the recommendation in **paragraph 3.114** that the person alleged to have posted the harmful communications should be given the opportunity of appearing and making representations to the court before the court makes a *Norwich Pharmacal* order.

Jurisdiction for Part 3

26. — (1) This Part applies to harmful communications, including the harmful communications referred to in *sections 4 to 8*, where —

(a) such harmful communications affect —

(i) an Irish citizen, or

(ii) a person ordinarily resident in the State,

and

(b) the means of communication used in connection with such harmful communications are within the control to any extent of —

- (i) an undertaking established under the law of the State, or
 - (ii) a company formed and registered under the Companies Act 2014, or
 - (iii) an existing company within the meaning of the Companies Act 2014.
- (2) Without prejudice to subsection (1), this Part also applies to harmful communications, including the harmful communications referred to in *sections 4 to 8*, where
- (a) such harmful communications affect —
 - (i) an Irish citizen, or
 - (ii) a person ordinarily resident in the State,
- and
- (b) where the means of communication used in connection with such harmful communications are within the control to any extent of an undertaking established under the law of another State and where a court established in the State would have jurisdiction to give notice of service outside the State in respect of civil proceedings to which such harmful communications refer.
- (3) For the purpose of this section, a person shall be deemed to be ordinarily resident in the State if he or she has had his or her principal residence in the State for the period of 12 months immediately preceding the act of harmful communication, including any harmful communication referred to in *sections 4 to 8*, concerned.

Explanatory Note

Section 26 of the Bill implements the recommendation in **paragraph 3.121** concerning the territorial scope of *Part 3* of the Bill, including the territorial scope of the take down procedure and of the Digital Safety Commissioner.

Section 26(1) of the Bill thus provides that *Part 3* applies to harmful communications, including the harmful communications referred to in *sections 4 to 8*, where (a) such harmful communications affect an Irish citizen or a person ordinarily resident in the State, and (b) the means of communication used in connection with such harmful communications are within the control of an undertaking or company established under the law of the State.

Section 26(2) of the Bill also provides that *Part 3* of the Bill could also have some extra-territorial effect, in connection with an Irish citizen or a person ordinarily resident in the State. This would be where the means of communication used in connection with such harmful communications are within the control of an undertaking established under the law of another State but where a court established in the State would have jurisdiction to give notice of service outside the State in respect of civil proceedings to which such harmful communications refer. This therefore corresponds with the approach taken in connection with the extra-territorial enforcement of civil proceedings generally, including under the “service out” procedures in Orders 11-11D of the *Rules of the Superior Courts 1986*.

APPENDIX B

**Report of consultations with young people concerning harmful internet
communications including cyber bullying**



May 2016

Index

Executive Summary

Section 1:

Introduction

- 1.1 Overview
- 1.2 About this report
- 1.3 Background
- 1.4 About the consultations
- 1.5 Recruitment of young people
- 1.6 Consultation methodology

Section 2: Policy and research context

- 2.1 Overview
- 2.2 Young people's participation in decision-making
- 2.3 Policies relating to children and young people's use of social and digital media
- 2.4 Children and young people's use of digital and social media in Ireland
- 2.5 Research on harmful internet communications
- 2.6 Cyber bullying
- 2.7 Research on cyber bullying
- 2.8 Parents, teachers and youth workers mediation of internet safety
- 2.9 Legislation related to cyber-bullying

Section 3: Consultation Findings

- 3.1 Overview

Theme 1: Catfishing/fake profiles and accounts/hacking

- 3.2 About catfishing/fake profiles and accounts/hacking
- 3.3 Impacts of catfishing
- 3.4 Recommendations related to catfishing
- 3.5 Key issues related to catfishing/hacking

Theme 2: Cyber bullying/trolling/anonymous activity

- 3.6 About cyber bullying/trolling
- 3.7 Impacts of cyber bullying/trolling
- 3.8 Recommendations related to cyberbullying
- 3.9 Key issues related to cyber bullying

Theme 3: Group chats

3.10 About group chats

3.11 Recommendations related to group chats

3.12 Key issues identified by young people relating to group chats

Theme 4: Hate speech/discrimination and racism

3.13 About hate speech/discrimination and racism

3.14 Key themes identified on hate speech/discrimination and racism

Theme 5: Pornography/revenge porn/inappropriate use of photos

3.15 About pornography/revenge porn/inappropriate use of photos

3.16 Recommendations on pornography/revenge porn/inappropriate use of photo

3.17 Key issues related to pornography/revenge porn/inappropriate use of photo

3.18 Experience of getting something taken down off the internet

Section 4: Summary of Key Findings

4.1 Overview

4.2 Key themes identified by young people

4.3 Theme 1: Catfishing/fake profiles and accounts/hacking

4.4 Theme 2: Cyberbullying/trolling/anonymous activity

4.5 Theme 3: Group chats

4.6 Theme 4: Hate speech/discrimination and racism

4.7 Theme 5: Pornography/revenge porn/inappropriate use of photos

4.8 Experience of getting something taken down off the internet

References

Appendix A: Consultation Methodologies

Appendix B: Consultation Evaluation Findings

Tables

Table 1: Would engaging in these activities related to catfishing/hacking on a once off basis make them illegal?

Table 2: Would engaging in these activities related to cyber bullying on a once off basis make them illegal

Table 3: Would engaging in these activities related to group chats on a one off basis make them illegal

Table 4: Would engaging in these activities related to hate speech/discrimination and racism on a one off basis make them illegal?

Table 5: Would engaging in these activities related to pornography, revenge porn and inappropriate use of photos on a one off basis make them illegal?

Executive Summary

This report documents the findings of a consultation process with young people on the issue harmful internet communications, including cyber bullying, conducted by the Department of Children and Youth Affairs (DCYA), in partnership with the Law Reform Commission. The consultations were part of a wider Law Reform Commission project involving the examination of the current law on personal safety and privacy, including cyber bullying.

In total, 70 young people aged 13-17 years took part in two consultations on the 27th and 28th April 2016 and were recruited primarily through Comhairle na nÓg around Ireland. Participants discussed the following questions: *'What online activity should be illegal?'* *'Would engaging in this activity on a once off basis make this illegal?'* and *'Have you any experience of getting something taken down off the internet?'*. Five key themes were identified by young people at the two consultation events:

- Theme 1: Cat Fishing/fake profiles and accounts/hacking
- Theme 2: Cyberbullying/trolling/anonymous activity
- Theme 3: Group chats
- Theme 4: Hate speech/discrimination and racism
- Theme 5: Pornography/revenge porn/inappropriate use of photos

Catfishing or “stealing someone’s identity by making a fake profile” was considered to be potentially very dangerous and to have serious impacts on people’s reputation and mental health. The majority of participants thought catfishing and identity theft should be illegal and suggested social networking sites should take more responsibility for this issue and young people should be better educated on catfishing and online safety in schools.

Cyber bullying or trolling was described as online activity which is generally anonymous and can include name calling, abuse, sharing of photos and personal information, online harassment and stalking. The impacts of cyber bullying were judged to range from mild to severe, including suicide. Participants thought

cyber bullying, particularly of vulnerable groups, should be illegal and suggested websites which facilitate anonymous activity should be banned. Young people called for more education on cyber bullying in schools.

Group chats were identified as a common online forum used for bullying, illegal activity and sharing of harmful content. Young people stated there should be better education in schools on the implications and legalities of sharing and receiving content through group chats and social networking websites should make it easier to remove personal content. Participants agreed that accounts which facilitate group chats on harmful topics should be illegal as well as posting abusive messages and sending photos without consent in these forums.

The consultations identified the Lesbian, Gay, Bisexual and Transgendered (LGBT) community, religions, ethnic minority groups, people with mental health issues, women, members of the Travelling community and people with disabilities are the main groups who are targets of online hate speech, discrimination and racism. Overall, young people felt strongly that online hate speech, discrimination and racism should be illegal.

In relation to pornography, the inadvertent exposure of children and young people to pornography adverts online was identified as a key issue. More regulations and monitoring of the advertising of pornography online, particularly on websites used by children and young people was recommended. Participants agreed that revenge porn should be illegal as it impacts people's reputation and mental health. Improving sex education in schools to cover issues such as sending and receiving nude photos and online safety was suggested.

Finally, only a very small number of young people had experience of getting something taken down off the internet. Generally, young people thought it was very difficult to get content taken down of the internet and argued that social networking websites should make it easier to report and remove content online.

Section 1: Introduction

1.1 Overview

This section of the report provides an introduction to the report and a background to the consultations.

1.2 About this report

This report documents the results of a consultation process with young people on the issue harmful internet communications, including cyber bullying, which was conducted by the Citizen Participation Unit of the Department of Children and Youth Affairs (DCYA), in partnership with the Law Reform Commission.

1.3 Background

The Law Reform Commission, in partnership with the Citizen Participation Unit of the Department of Children and Youth Affairs (DCYA), was interested in seeking the views of young people in connection with a Commission law reform project.

This concerned Project 6 in the Commission's 4th Programme of Law Reform, which involved an examination of the current law on personal safety and privacy, including cyber bullying. The project involved:

- an examination of the types of harmful behaviour involved in this area, including the impact that cyber bullying through social media has had;
- whether existing criminal law, notably the harassment offence in the *Non-Fatal Offences Against the Person Act 1997*, should be reformed because it does not appear to cover indirect harassment such as compiling harmful fake social media profiles;
- whether there is a case for a new criminal offence that would deal with a once-off upload of harmful, in particular intimate, images - sometimes referred to as an "upskirting" offence; and
- whether new legislation is required to provide for more effective, immediate, civil remedies such as "take-down" orders.

In 2014, the Law Reform Commission published a consultative *Issues Paper on the Law Affecting Personal Safety and Privacy, Including Cyber Bullying* (LRC IP 6-2014), in which it identified the main issues involved in this project and sought the views of interested parties. The Commission also engaged in an extensive consultative exercise since then, which included a public seminar in April 2015. The final report on this project, which will be published by the Commission in late 2016, will include its final recommendations for law reform.

1.4 About the consultations

Two consultations were run by the DCYA Citizen Participation Unit in the Aisling Hotel, Dublin, on 27th and 28th April 2016 with two groups of 13-17 year olds, comprising 70 young people in total. 36 young people attended the first consultation day and 34 young people attended the second consultation day. The focus of the consultations was on the experiences, concerns and needs of young people in connection with harmful internet communications, including cyber bullying.

1.5 Recruitment of young people

Young people were primarily recruited through Comhairle na nÓg (child and youth councils) around Ireland. A number of seldom heard young people were also recruited through Barnardos and the Irish Wheelchair

Association. Young people from the following 19 Comhairle na nÓg were represented at the two consultation events:

Day 1:

- Cork City Comhairle na nÓg
- Donegal Comhairle na nÓg
- Kerry Comhairle na nÓg
- Limerick Comhairle na nÓg
- Longford Comhairle na nÓg
- Mayo Comhairle na nÓg
- Monaghan Comhairle na nÓg
- Sligo Comhairle na nÓg
- Tipperary Comhairle na nÓg
- Waterford Comhairle na nÓg
- Wicklow Comhairle na nÓg

Day 2:

- Cavan Comhairle na nÓg
- Dublin City Comhairle na nÓg
- Galway City Comhairle na nÓg
- Galway County Comhairle na nÓg
- Leitrim Comhairle na nÓg
- Louth Comhairle na nÓg
- Meath Comhairle na nÓg
- Roscommon Comhairle na nÓg

1.6 Consultation methodology

The methodology for the workshops was designed by the DCYA Participation Support Team (see Appendix A). The consultation began with an introductory speech from representatives from the Law Reform Commission and the DCYA to explain the background to the consultation and outline issues such as child protection procedures at the consultations. Young people took part in an ice-breaker activity and were then divided up into separate groups and assigned to tables with an adult facilitator.

All young people then discussed the question, '**What online activity should be illegal?**' Young people were given four 'post-its' each to write down their ideas in relation to this question and were asked to stick the post-its on a designated wall in the room. One young person from each table volunteered to group the post-its into agreed topics, with support from facilitators.

The key topics which emerged at the first consultation were:

- Cat Fishing/fake profiles
- Trolling/bullying
- Hacking/group chats
- Porn/explicit images/revenge porn
- Anonymous activity

The key topics which emerged at the second consultation were:

- Fake accounts
- Cyber bullying including ask FM
- Hate speech (discrimination and racism)
- Inappropriate use of photos

Placemats relating to each of the topics identified in the open space session were assigned to the tables of young people. The consultation used a 'world café' methodology which involved young people discussing each topic and writing on the placemat and then moving tables to discuss the next topic. This allowed young people see what other young people have written on the topic on each placemat and add to it. After the young people had discussed each topic they carried out 'sticky dot voting', identifying what they considered to be the most important issues related to each topic. Young people were then given the opportunity to vote on each issue.

The top six issues from each table were then displayed on cards. Participants again visited each table and discussed: ***Would engaging in this activity on a once off basis make this illegal?*** After a short discussion, participants indicated agreement or disagreement by placing the appropriate coloured card in the envelope attached to each of the six issues. If their answer was yes, they placed a green card in the envelope, if no; they placed a red card in the envelope. Participants were given 30 of each colour at the beginning of the exercise. Finally, young people discussed the question, '***Have you any experience of getting something taken down off the internet?***'

Section 2: Policy and research context

2.1 Overview

This section of the report examines the policy and research context for conducting consultations with young people on the issue of harmful internet communications including cyber bullying.

2.2 Young people's participation in decision-making

Article 12 of the UN Convention on the Rights of the Child (UNCRC) (UN, 1989), which was ratified by Ireland in 1992, guarantees a commitment to ensuring the voices of children and young people are heard and their opinions are given due weight in accordance with their age and maturity in matters that affect them. Similarly, Article 24 of the EU Charter of Fundamental Rights (European Union, 2000), which outlines the fundamental rights protected in the EU, on 'The rights of the child', states children "may express their views freely" and "such views shall be taken into consideration on matters which concern them in accordance with their age and maturity."

Goal 1 of *Our Children – Their Lives: The National Children's Strategy* (Department of Health and Children, 2000), draws strongly on Article 12 of the UNCRC, stating that "children will have a voice in matters which affect them and their views will be given due weight in accordance with their age and maturity." In terms of current Irish policy, *Better Outcomes, Brighter Futures: The National Policy Framework for Children and Young People, 2014-2020* (Department of Children and Youth Affairs, 2014) also commits to children and young people having a voice in decisions that affect their lives across all five outcome areas of the policy framework.

The aim of the National Youth Strategy (DCYA, 2015a) is "to enable all young people to realise their maximum potential, by respecting their rights and hearing their voices, while protecting and supporting them as they transition from childhood to adulthood." Objective 10 of the strategy advocates that "young people's autonomy is supported, their active citizenship fostered, and their voice strengthened through political, social and civic engagement."

The National Strategy on Children and Young People's Participation in Decision-Making (2015-2020) (DCYA, 2015b), is guided and influenced by the UNCRC and EU Charter of Fundamental Rights. Its goal is to ensure that children and young people will have a voice in their individual and collective everyday lives. The strategy (DCYA, 2015b:20) defines children and young people's participation in decision-making as "the process by which children and young people have active involvement and real influence in decision-making on matters affecting their lives, both directly and indirectly." Objective 7 of the National Strategy on Children and Young People's Participation in Decision-Making commits to "mainstreaming the participation of children and young people in the development of policy, legislation and research".

The strategy also highlights the benefits of participation by children and young people in decision-making, for example, benefits for services include improved services, policies and research; benefits for children include increased self-confidence and communication skills and better educational outcomes; and benefits for society include active citizenship and social inclusion (DCYA, 2015b: 7).

2.3 Policies relating to children and young people's use of social and digital media

Children and young people's use of social and digital media is addressed in a number of national policies including:

- Better Outcomes Brighter Futures: The national policy framework for children and young people 2014 – 2020 (DCYA, 2014);
- The National Youth Strategy 2015-2020, (DCYA, 2015a);
- The National Digital Strategy (Department of Communications, Energy and Natural Resources, 2013) and;
- The National Digital Strategy for Schools 2015–2020 (Department of Education and Skills, 2015).

In relation to realising the potential of children and young people through the use of social and digital media, Better Outcomes Brighter Futures: The national policy framework for children and young people 2014–2020 (Department of Children and Youth Affairs, 2014), under Outcome 2 'Achieving full potential in learning and development', commits to:

"support and link existing partnerships, strategies and initiatives that aim to improve the decision-making capacity of children and young people through strengthening self-esteem, resilience, responses to social and interpersonal pressure, health and media literacy (including social media literacy)". (2014:70),

However, in relation to Outcome 3, 'Safe and protected from harm', the policy framework (2014: 79) recognises *"the complex and multifaceted nature of cyber-bullying"*. It highlights the important role of parents, teachers and the wider community in terms of *"creating a climate that does not tolerate or foster bullying (including cyber-bullying) or intolerance."* It also acknowledges the need for parents and teachers to protect their children in terms of online safety and provide guidance and support to young people to cope with this aspect of their lives.

"With the growing role of technology in children and young people's lives, parents need advice and information on how best to protect their children from harm online and in relation to social media and texting. Equally, children and young people need the guidance of teachers and parents to learn to manage and cope with this added dimension to modern life"(DCYA, 2014: 77).

Similarly, the policy framework recognises the importance of continuing to "promote best practice by social media providers with respect to privacy controls and reporting mechanisms for abuse/bullying so as to better protect children online" (2014: 82).

The National Youth Strategy (DCYA, 2015a:27) under outcome 2 – ‘achieving full potential in all areas of learning and education,’ identifies the promotion of “the use of new technologies and support acquisition of digital skills of young people” as an outcome.

The main goal of the National Digital Strategy (Department of Communications, Energy and Natural Resources, 2013) is “the optimal economic and social use of the internet by business, individuals and by Government.” Strand 3 of the Strategy (DCENR, 2013: 3) focuses on Education and eLearning and aims “to utilise ICT to its full potential across the education system including the use of the internet in learning”. While the strategy acknowledges the opportunities which digital use represents for learning and development among children and young people, it also highlights internet safety as an important issue and outlines the need for “new research on the nature and extent of children’s internet and social network use including issues of internet risks and safety for young people”.

The National Digital Strategy for Schools 2015 – 2020 (Department of Education and Skills, 2015) provides a rationale and a Government action plan for integrating ICT into teaching, learning and assessment practices in schools. The strategy (DES, 2015: 38) recognises that “central to promoting the autonomous, effective, and safer use of the internet by young people is a strong commitment to changing behaviour through a sustained information and awareness strategy targeting parents, teachers, and children and young people themselves.”

The strategy also acknowledges that some schools have not engaged in internet use because of concerns over internet safety. It highlights the importance of schools constantly reviewing their policies and procedures regarding acceptable internet use, internet safety, digital identity and data protection. One of the key recommendations of the strategy is to provide parents/guardians, students and teachers with information, advice and tools to promote safer, more responsible and more effective use of the internet, including developing additional resources on cyber-bullying awareness for teachers, for example through the Social, Personal and Health, Education (SPHE) curriculum.

2.4 Children and young people’s use of digital and social media in Ireland

Internet use is prolific among children and young people in Ireland. A recent study (O’Neill and Dinh, 2015: 4) found that 63% of children report using the internet several times a day. Smartphones are the most used device for internet access on a daily basis by 9-16 year olds (35%), followed by laptops (29%) and tablets (27%). Just under half (46%) of children access the internet from their own bedroom on a daily basis, with 22% saying they do so several times per day. There has been a significant increase in internet use in children’s own rooms among older teenagers (15-16 years), with over three quarters (77%) saying they go online in their own room compared with 43% in 2011.

In terms of social media use, the study (O’Neill and Dinh, 2015: 5) found that nine out of ten of all 15-16 year olds in Ireland have a profile on a social networking site and just under 40% of 11-12 year olds have a social networking profile, despite age restrictions set by many networks. Eight out of ten young people use

Facebook as their main social network profile and 10% use Twitter. Over one third of all 9-16 year olds (36%) have a profile on a media sharing platform with Instagram being the most popular (43%) followed by YouTube (34%) (O'Neill and Dinh, 2015: 5).

In terms of internet safety, Irish children have made a good progress in terms of increasing their online safety skills, for example blocking message from someone they don't want to hear from, deleting the record of which sites they have visited, etc. Over half (57%) of Irish children and young people claim to be able to use the internet safely (57%), however, 43% still say that they do not know how to use "report abuse" buttons on websites (O'Neill and Dinh, 2015: 5).

2.5 Research on harmful internet communications

The Net Children Go Mobile Report (O'Neill and Dinh, 2015: 5) found that 20% of children in Ireland had been bothered by something they saw on the internet in the past. This represents a doubling of the figure reported by EU Kids Online in 2011. A quarter (25%) of 13-14 year olds and 37% of older 15-16 year olds said they have experienced something that bothered them or wished they hadn't seen. Over a third (35%) of girls aged 13-16 had encountered some form of harmful online content such as hate messages (15%), anorexic or bulimic content (14%), self-harm sites (9%); sites discussing suicide 8% and sites where people share their experiences with drugs (7%).

Almost half (47%) of older teenagers had seen sexual images online in the past 12 months compared to 11% of younger children. About half of older teenagers who had seen sexual images said they were upset by the experience. One in ten (10%) 13-14 year olds and 22% of 15-16 year olds reported having received sexual messages online and 4% reported being 'very' (1%) or 'a little' (3%) upset as a consequence. Finally, 22% of children reported having contact online with people they have never met face to face.

2.6 Cyber bullying

Cyber bullying can be described as "an extension of traditional bullying with technology providing the perpetrator with another way to abuse their target" (O'Moore, 2012) or "an aggressive, intentional act that is carried out by one or several people, using electronic devices against a victim who cannot easily defend him or herself" (www.tacklingbullying.ie). Methods of cyber bullying include; phone calls, text messages, emails, instant messaging using text, picture or video and on social networks such as Facebook, Twitter, Instagram, Snapchat etc. (www.tacklingbullying.ie).

According to the Action Plan on Bullying (Department of Education and Skills, 2013: 25), cyber bullying "can often take the form of identity based bullying such as racist or homophobic bullying" and because it is carried out using online technologies "it becomes increasingly difficult to deal with and goes beyond the traditional boundaries of the school environment". The effects of cyber-bullying can include stress, anxiety, anger, sleep problems, becoming withdrawn, depression, thoughts of suicide, aggressive behaviour, loss of confidence and self-esteem, loss of a sense of security, lack of motivation and energy, and alcohol,

drug or substance abuse (O'Moore and McGuire, 2014: 5).

2.7 Research on cyber bullying

An Irish study which investigated access and use, risks and opportunities of mobile internet use among children and young people (O'Neill and Dinh, 2015: 5) found that 22% of children had experienced either online or offline bullying. 13% of 13-14 year olds had been bullied on a social networking site, with girls being more likely to experience bullying than boys (26% of girls compared to 17% of boys).

The latest Irish Health Behaviour in School-aged Children (HBSC) Study (Gavin et al, 2015: 57-8) also identified significant gender difference in terms of cyber bullying. Overall, 17% of girls reported experiencing cyber bullying by being sent mean messages, wall postings or by a website created to make fun of them compared with 10% of boys. Similarly, 19% of girls reported being bullied by someone taking unflattering or inappropriate pictures of them without permission and posting them online compared with 11% of boys. Older children were also more likely to experience these types of cyber bullying compared with younger children.

2.8 Parents, teachers and youth workers mediation of internet safety

A recent study which examined parent's knowledge and usage of the internet and knowledge of their children's internet usage (O'Higgins Norman and McGuire, 2016: 22) found a low percentage of frequent parental supervision with regard to social networks (18%). The study also highlighted a comparative lack of use of basic preventative measures by parents in terms of online safety. For example, 29% of 13-14 year olds operated without a parental filter on their computer and 28% of 13-14 year olds and 38% of 15-16 year olds had access to a networked computer in a private place.

However, mediation of internet safety by teachers in Ireland has been found to be above the European average (O'Neill and Dinh, 2015: 6). The study reported that 81% of teachers had provided advice to children and young people in relation to using the internet safely, over three quarters (77%) had explained why some websites are good or bad and talked to children about their online activities.

A new study on the use of ICT, digital and social media in youth work conducted by the National Youth Council of Ireland (NYCI, 2016) found that 77% of youth workers use social and digital media in their work with young people. However, only 24% of youth workers stated they had received training in the use of social and digital media. The study calls for the development of a National Digital Plan for the youth work sector "to embed social and digital media in youth work practice" and to "provide information, advice and tools to promote safer, more responsible and more effective use of social and digital media."

2.9 Legislation related to cyber-bullying

Currently, there are no any laws which are related directly to cyber bullying. However, in some cases the following legislation can be applicable: the making of nuisance and malicious calls is a criminal offense under Section 13 (1) of The Post Office Amendment Act 1951. Under The Criminal Damage Act 1991, it is an

offense to damage property (Section 2), make threats to damage property (Section 3), and to gain unauthorised access of data (Section 5). The Non-Fatal Offences Against the Person Act 1997, Section 10, deals with harassment: when a person's acts intentionally or recklessly, seriously interferes with the other's peace and privacy or causes alarm, distress or harm to the other' (O'Moore and McGuire, 2014: 10)

Section 3: Consultation Findings

3.1 Overview

This section examines the key themes identified by young people at the consultation events. The key topics which were identified by young people at the two consultation events can be grouped into the following five themes:

- Theme 1: Cat Fishing/fake profiles and accounts/hacking
- Theme 2: Cyberbullying/trolling/anonymous activity
- Theme 3: Group chats
- Theme 4: Hate speech/discrimination and racism
- Theme 5: Pornography/revenge porn/inappropriate use of photos

Theme 1: Catfishing/fake profiles and accounts/hacking

3.2 About catfishing/fake profiles and accounts/hacking

Catfishing was described by participants as *"stealing someone's identity by making a fake profile" or "posing as other people without their prior consent"*. According to young people, catfishing can be used to lure someone into a relationship, ask for nude photos, bully people, get people into trouble and start fights. Catfishing or creating fake profiles was considered to be very easy as no identification is needed to set up an account and photos can be copied from other accounts. Participants felt social networking websites should take more responsibility in the area of fake accounts and make it more difficult for these types of activities to occur.

- *"Social media should take more responsibility when it comes to fake accounts. Make it harder to make fake accounts."*

Participants felt catfishing was very dangerous, in the sense that an older person could lure a child or young person into a relationship, meet up with them and then cause them harm, e.g. sexual assault, rape,

kidnapping. Young people thought a law on this issue was required due to the potentially serious consequences of identity theft and catfishing.

- *"Catfishing is incredibly easy to do and really dangerous. It is stealing someone's identity. It can affect the person who has been catfished and the person whose identity has been stolen. It can be used to start fights, kidnap people and make people believe they have relationships with fake people."*
- *"It's (catfishing) dangerous in the sense of older people being able to pretend they are the same age as you...especially when you think you know the person and meet up with them and they're not the person you thought. This could lead to sexual abuse."*

According to participants, one of the most common ways catfishing is used is to get nude photos of a person. Participants thought education on catfishing, online safety and the sending of nude photos should be introduced in primary and secondary schools to ensure young people's safety and raise awareness of the consequences of these activities.

- *"Educate girls/boys not to send nudes."*
- *"There should be an emphasis on awareness in schools about catfishing and online safety."*

3.3 Impacts of catfishing

Participants felt catfishing could have a very negative effect on both the person who has their identity stolen as well as the person who is targeted through the 'catfish'. They thought stealing someone's identity could cause damage to their reputation which could affect their future job opportunities. Bullying of people online using a fake profile could get the 'real person' into trouble as well as cause distress to both them and the victim, potentially resulting in mental health difficulties and even suicide.

- *"If the identity is stolen, this can greatly affect the reputation of the real person because catfishing isn't generally used positively."*

- *“Using someone else’s name and picture to bully people so the real person gets into trouble for bullying people.”*

3.4 Recommendations related to catfishing

Recommendations given by young people with regard to combating catfishing, hacking and the creation of fake profiles and accounts included:

- Social media users should be notified if someone views their account
- The reporting of fake profiles on social media should be taken more seriously
- Gardaí should have a database of IP addresses to investigate false accounts
- Proof of identity should be required when setting up a social media or email account
- Once a fake account is shut down the user shouldn’t be allowed to set up another account
- There should be a special identity number when setting up profiles on social media
- It should be easier to report fake profiles
- There should be classes on internet safety in schools

3.5 Key issues related to catfishing/hacking

The top issues which emerged from the consultations in relation to catfishing, hacking and fake profiles and accounts are detailed in Table 1 below. Participants were asked whether engaging in these activities on a one off basis should be illegal and voted on whether they agreed or disagreed with each statement. All (100%) young people thought identity theft should be illegal and almost all (97%) young people thought identity theft by creating fake profiles and taking someone’s pictures and personal information should be illegal. Catfishing should be illegal according to 94% of participants and catfishing to get nude photographs should be illegal according to 88% of participants.

Overall, 88% of young people thought hacking people’s accounts and messaging people to turn friends against you should be illegal. In the same way, 79% of young people thought using someone else’s name and picture so the ‘real’ person gets in trouble for bullying people should be illegal. Almost eight out of ten (79%) participants agreed that social networking websites should take more responsibility for stopping fake accounts.

Three quarters (75%) of participants agreed that taking pictures of teachers and making fake online accounts of them should be illegal. Just of half (52%) of participants thought users should be notified if someone views their online account. Only 22% of participants agreed that it should be illegal ‘for older people to pretend they are

younger and same age as younger people' whereas the majority (78%) disagreed with this statement. Finally, the majority (89%) of young people disagreed that people should need a licence to code.

Table 1: Would engaging in these activities related to catfishing/hacking on a once off basis make them illegal?

Activity	Agreed	Disagreed
Identity theft	33 (100%)	0 (0%)
Identity theft by creating fake profiles and taking someone's pictures and personal information	32 (97%)	1 (3%)
Catfishing	30 (94%)	2 (6%)
Hacking other people's accounts and messaging people to turn your friends against you	28 (88%)	4 (12%)
Catfishing someone to get nudes	28 (88%)	4 (12%)
Taking people's personal details, using it to Catfish, using images	29 (83%)	6 (17%)
Using someone else's name and picture so the real person gets in trouble for bullying people	26 (79%)	7 (21%)
Social media should take more responsibility for stopping fake accounts	26 (79%)	7 (21%)
Taking pictures of teachers and making profiles of them	24 (75%)	8 (25%)
Should be notified if someone else views your account	17 (52%)	16 (48%)
Should be illegal for older people to pretend they are younger and same age as younger people, e.g. minors	7 (22%)	25 (78%)
Licence to code	3 (11%)	25 (89%)

Theme 2: Cyber bullying/trolling/anonymous activity

3.6 About cyber bullying/trolling

Participants described cyber bullying or trolling as online activity which is generally anonymous and can include name calling, abuse, sharing of photos or personal information, online harassment and stalking. Cyber bullying can be a once off occurrence or happen over a period of time. Some participants made a distinction between cyber bullying and trolling. They felt trolling could sometimes be limited to posting satirical comments online, whereas cyber bullying was more personal and akin to offline bullying. The most commonly cited types of cyber bullying were posting photos of someone online without their permission and creating fake accounts to bully someone.

- *"Cyber bullying is like trolling, materials can be posted, nasty abusive comments, sharing photos without permission, stalking and spam, harassing. It can happen over a period of time and some material shared could really affect a person's life emotionally/job interviews."*

Social networking websites which allow for anonymous profiles and activities, such as ask.fm, were singled out by participants as being particularly prone to instances of cyber bullying. Some young people called for these types of anonymous websites to be banned or not to be allowed to be anonymous. However, some participants reported that ask.fm is not as popular as it was previously, and young people sometimes 'self-police' the website when harmful comments made against other young people.

- *"Ban anonymous profile website, e.g. ask.fm. Facebook and websites with private interaction should not be allowed be anonymous."*
- *"Ask.fm, a social media site where you can ask other users questions anonymously, is not as popular as it used to be. Young people are looking out for each other and sticking up for them on the comments."*

3.7 Impacts of cyber bullying/trolling

According to young people, the impacts of cyber bullying can range from harmless annoyance to embarrassment, hurt and humiliation. It can also have an impact on people's reputation, self-esteem, emotional well-being and mental health, and in some cases, lead to suicide.

- *"Cyber bullying can be a one off occurrence but what you post can change somebody's life forever. It's worldwide, can escalate and is there forever."*
- *"Cyber bullying can be one off as all online activity can never truly be erased. Lots of people will have access to the cyber bullies comments/actions so it's just like bullying in a big group. One comment/action can hurt somebody and ruin their reputation."*

3.8 Recommendations related to cyberbullying

- There should be a request of consent from a person who is being tagged or messaged

- Anonymous profiles should be not allowed on social networking sites
- There should be more education on online bullying in schools
- Age restrictions on Facebook, Instagram etc. should be more strictly regulated
- Social media users should be allowed to delete photos they are tagged in

3.9 Key issues related to cyber bullying

The top issues relating to cyber bullying identified by young people at the two consultation events are outlined in Table 2 below. Participants were asked to vote on whether engaging in these activities on a one off basis should be illegal. Almost all young people (94%) agreed that engaging in online racism, harassment and homophobia should be illegal. Overall, 89% of participants agreed that fake profiles used to target a certain person or those who are 'weak' should be illegal. Similarly, 88% thought being able to create fake accounts 'to post bad things or pictures of people' to target them should be illegal. Over three quarters (76%) of participants stated that posting comments that damage people's public image should be illegal. Over seven out of ten (72%) young people thought engaging in cyber bullying, even on a once off basis, should be illegal.

In relation to anonymous online activity, almost seven out of ten (68%) young people thought using the anonymous social networking site ask.fm should be illegal. Two thirds (66%) of participants thought it should be illegal not to take a person's photo down off the internet if they requested you to do so. Engaging in activity on gossip pages used for bullying should be illegal according to 64% of participants. Just over half (52%) of young people agreed that 'people don't get punished for the bullying they do as it is anonymous.' Overall, 45% of participants agreed being anonymous online on a public forum, e.g. social media, gossip girl pages, should be illegal whereas 55% disagreed with this statement. Similarly, 45% thought engaging in activities on anonymous profile websites should be illegal whereas 55% thought this type of activity should not be illegal.

In terms of hacking, 61% of participants thought Ddosing, a distributed denial-of-service (DDoS) attack, which occurs when multiple systems flood the bandwidth or resources of a targeted system, should be illegal. Almost half of participants (49%) agreed that proxies, (web proxies facilitate access to content on the World Wide Web and provide anonymity), should not be illegal, whereas just over half (51%) disagreed that proxies should be illegal, arguing that the only countries that block proxies are dictatorships and communist countries such as China.

Only 43% of young people agreed that putting up statuses and tweets to target people should be illegal, whereas 57% disagreed. Likewise, 42% agreed that posting photos of other people without their permission or consent should be illegal, while 58% disagreed. Just three out of ten (30%) young people thought sending personal abusive messages should be illegal whereas seven out of ten (70%) disagreed. Just over one quarter (26%) of young people agreed that creating videos or making comments to make fun of something

should be illegal while almost three quarters (74%) disagreed. Finally, just 26% of participants agreed that tagging a person without their consent should be illegal whereas 74% of participants disagreed.

Table 2: Would engaging in these activities related to cyber bullying on a once off basis make them illegal?

Activity	Agreed	Disagreed
Online racism, harassment and homophobia	29 (94%)	2 (6%)
Fake profiles used to target the weak/a certain person	31 (89%)	4 (11%)
Being able to create fake accounts to post bad things or pictures of people- used to target certain people	30 (88%)	4 (12%)
Comments that damage people's public image, e.g. framing, inappropriate videos/photos	25 (76%)	8 (24%)
Cyberbullying (even once off) should be made illegal	26 (72%)	10 (18%)
Ask.fm- a social media site where you can ask other users questions anonymously	28 (68%)	13 (32%)
To not take down a person's photo if they request it	19 (66%)	10 (34%)
Gossip pages (used for rumours/bullying)	21 (64%)	12 (36%)
Ddosing	28 (61%)	18 (59%)
People don't get punished for the bullying they do as it is anonymous	17 (52%)	16 (48%)
Proxies should not be illegal. Ireland is a democracy- the only countries that block proxies are dictatorships and communist countries like china	18 (49%)	19 (51%)
Being anonymous online on a public forum, e.g. social media, Gossip Girl pages	15 (45%)	18 (55%)
Anonymous profile websites, e.g. any website with private interaction	14 (45%)	17 (55%)
Putting up statuses and tweets etc. to target people	15 (43%)	20 (57%)
Posting photos of other people without their permission/consent	13 (42%)	18 (58%)
Sending personal abusive messages	10 (30%)	23 (70%)
Creating videos/making comments to make fun of something	9 (26%)	26 (74%)
Tagging a person without their consent	9 (26%)	25 (74%)

Theme 3: Group chats

3.10 About group chats

Group chat is a tool that allows a group of people to communicate with each other online. Group chats on social media websites such as Facebook messenger were singled out as online forums which can be used for bullying and illegal activity, for example sharing of explicit photos of young people under 18 years of age. Other anonymous websites which have a group chat or group forum function which is sometimes used for harmful communications that were singled out included Tumblr and 4chan. Groups on Instagram which promote eating disorders and self-harm were also highlighted by young people as negative online forums.

- *"Sending of nudes in Facebook messenger especially of minors."*
- *"Tumblr attacking people, telling them to go kill themselves."*

Some young people thought there should be better monitoring of groups chats, however others felt it was too difficult to monitor such online activity and suggested more emphasis should be placed on educating young people on the implications and legalities of sharing and receiving content online.

- *"Better education on laws in Ireland on illegal content sharing and receiving."*
- *"Better education. Instead of teaching people how to be victims teach them to deal with it."*

3.11 Recommendations related to group chats

Young people who use group chats made the following recommendations:

- Users should be able to report inappropriate group chats
- Users should have more control in terms of being added to group chats, e.g. a request should be sent to invite a user to a group chat which has to be approved
- If you remove yourself from a group chat it shouldn't be possible to be added again
- You should be able to remove other users from a group chat
- Screenshots should be banned on group chats and image messaging and multimedia apps such as Snapchat

3.12 Key issues identified by young people relating to group chats

Participants identified key issues relating to group chats which are outlined in Table 3 below. Young people voted on whether they agreed or disagreed if engaging in these activities on a one off basis should be illegal.

Almost all (97%) participants agreed that Twitter accounts and other website accounts that support self-harm and eating disorders should be banned. Just over nine out of ten (91%) young people agreed that posting abusive messages on websites such as 4chan (an image board website where users generally post anonymously) and Tumblr (a microblogging platform and social networking website which allows users to post multimedia and other content anonymously) should be illegal.

Over eight out of ten (84%) participants thought people should be allowed to remove personal information off Facebook and Google. Sharing images without consent should be illegal according to 82% of participants. Seven out of ten (70%) young people agreed that making fake accounts to talk to people on Facebook messenger should be illegal, whereas three out of ten (30%) disagreed. Finally, just over half (52%) of participants agreed that using screenshots, for example of sexting (sexually explicit photographs or messages sent online or by mobile phone), against people in group chats should be illegal, while just under half (48%) of participants disagreed.

Table 3: Would engaging in these activities related to group chats on a one off basis make them illegal?

Activity	Agreed	Disagreed
Ban Twitter and other sites accounts that support self-harm, eating disorders etc. e.g. accounts giving advice on how to “cut deeper”	31 (97%)	1 (3%)
Abuse of 4chan, Tumblr- attacking people, telling them to go kill themselves	30 (91%)	3 (9%)
You should be allowed take all of your private info off Facebook and Google	27 (84%)	5 (16%)
Lack of consent of images being shared	27 (82%)	6 (18%)
Making fake accounts to talk to people on Facebook messenger	21 (70%)	9 (30%)
Screenshots (of sexting for example) being used against people in groups chats	15 (52%)	14 (48%)

Theme 4: Hate speech/discrimination and racism

3.13 About hate speech/discrimination and racism

According to participants, the main groups who are targets of online hate speech, discrimination and racism are the Lesbian, Gay, Bisexual and Transgendered (LGBT) community, religions, ethnic minority groups, people with mental health issues, women, members of the Travelling community and people with disabilities. Participants argued that online hate speech, discrimination and racism should be blocked or banned by websites.

- *"Discriminating posts against members of the LGBT society should be blocked."*
- *"Racist comments or hurtful comments should be filtered out by social media platforms."*

Young people also felt that online posts, videos or websites created by terrorist organisations should be removed immediately from the internet and posts and websites that promote terrorism should be illegal.

- *"Isis and other Islamic terrorist groups have made a bad name for the Islamic faith so I think the videos they make about threats, beheadings and much more horrific things should be taken down immediately before the videos get seen or re-uploaded."*

Participants suggested there should be better monitoring of comments on YouTube and YouTube videos posted on social media sites such as Facebook should also be monitored and age rated.

- *"YouTube videos or videos on Facebook/Twitter/Instagram should be checked by Facebook and age rated."*

3.14 Key themes identified on hate speech/discrimination and racism

Participants who took part in the consultation events identified key issues related to hate speech, discrimination and racism and then voted on whether engaging in these activities on a one off basis should be legal or illegal (see Table 4 below).

Nine out of ten (90%) participants agreed that discriminative websites targeting religions should be illegal. Over eight out of ten (81%) young people thought posting videos or comments online to promote terrorism should be illegal, whereas 19% disagreed. In total, 79% of participants agreed that engaging in discrimination against the Lesbian, Gay, Bisexual and Transgendered (LGBT) community online should be illegal, while 21% disagreed. Similarly, 71% agreed that transphobic tweets and posts should be illegal. Just over seven out of ten young people agreed that discrimination against mentally ill people online should be

illegal whereas 28% disagreed. Over three quarters (76%) of participants disagreed that posting information online about people without their consent should be illegal while less than one quarter (24%) agreed with this statement.

Table 4: Would engaging in these activities related to hate speech/discrimination and racism on a one off basis make them illegal?

Activity	Agreed	Disagreed
Discriminative websites targeting religions	26 (90%)	3 (10%)
Posting videos/comments to promote terrorism	26 (81%)	6 (19%)
Discrimination against LGBT community	34 (79%)	9 (21%)
Discrimination against mentally ill	23 (72%)	9 (28%)
Transphobic tweets and posts	25 (71%)	10 (29%)
Posts about people without consent	8 (24%)	25 (76%)

Theme 5: Pornography/revenge porn/inappropriate use of photos

3.15 About pornography/revenge porn/inappropriate use of photos

The main issue identified by participants in relation to pornography was the inadvertent exposure of children and young people to pornography adverts online. Some young people gave examples of seeing adverts of pornography and dating websites on websites aimed at children or on sites where young people watch free films. They felt there should be stricter regulations in relation to online advertising to combat children and young people's exposure to inappropriate images and content. Some young people suggested the advertisement of pornography online should be made illegal, whereas others suggested introducing a watershed on this type of advertisement online, e.g. after 9pm.

- *"Ads on kid's websites for porn and dating sites. Google should have more regulations for ads."*
- *"Pornographic adverts on movie sites like Putlocker should be illegal because young people watching things shouldn't see that. All porn adverts should be made illegal."*
- *"It's very awkward when your young sister is online and porn ads pop-up. You have to explain to parents that I'm watching a normal movie, not porn when they walk in and see a random ad for porn sites."*

The majority of young people felt that 'revenge porn', "the sexually explicit portrayal of one or more people distributed without their consent via any medium" (Citron et al., 2014), should be illegal. Young people also drew attention to the fact that intimate pictures could be used to blackmail a person into doing something they are not comfortable with or to embarrass a person after the break-up of a relationship. According to participants, the main impacts of revenge porn are on the reputation of the person and their mental health.

- *"Revenge porn is sending intimate pictures in a group chat or to their parties who aren't involved. Using intimate photos to blackmail you into doing things you are uncomfortable with. Posting private pictures after a break up to embarrass someone."*
- *"Leaking nude photos that were sent privately and a person is upset by them being shared should be illegal."*
- *"One picture/video can mess up your reputation in the future."*

3.16 Recommendations on pornography/revenge porn/inappropriate use of photos

The need for better sex education was raised by a large number of young people at both consultations. Many young people made recommendations in terms of improving and updating sex education in schools to cover issues such as the implications and legalities of sending and receiving nude photos, online safety and pornography addiction. A public awareness campaign in relation to online safety and sending of nude photos was also suggested by some young people. Educating parents about online safety was put forward as another recommendation.

- *"Sex education should be updated to include things like nudes and porn addiction. People should be told the legal and illegal side of sending explicit pictures both receiving and giving."*
- *"Make young people aware of the long term effect of making porn videos and sending nudes."*
- *"People aren't educated enough on online activity. People don't realise that if it's on the Internet in any capacity, it's out of your control completely. Some education on the Internet I believe is necessary."*

- *“Parents must take responsibility. Parents should know and protect their kids from such content and be involved in their child’s online activity. Without knowing about the Internet they leave their children vulnerable.”*

3.17 Key issues related to pornography/revenge porn/inappropriate use of photos

The key issues identified by young people in relation to pornography, revenge porn and inappropriate use of photos online are outlined in Table 5 below. Participants were asked to vote on whether they agreed or disagreed that engaging in these activities on a one off basis should be illegal.

All (100%) participants agreed that revenge porn should be illegal. Over nine out of ten (93%) participants agreed that using intimate photos to blackmail your partner into doing things they’re not comfortable with should be illegal. Overall, 85% of young people agreed that sharing of nude photos on group chat such as Facebook to bully either girls or boys should be illegal. Three quarters (75%) of participants thought the leaking, but not the sending, of nude photos should be illegal, while one quarter (25%) disagreed.

In relation to the inappropriate use of photos, 48% of young people agreed that using photos to hurt or slander someone should be illegal while over half (52%) of young people disagreed with it being illegal. Just over two in ten (23%) participants agreed that the distribution of someone’s photos without their consent should be illegal, whereas 77% disagreed with this statement.

In terms of exposure to pornography online, 84% of participants thought there was a lack of monitoring on social media sites and that there should be more regulations on the advertisement of pornography online, especially on websites aimed at children. Over eight out of ten (82%) young people agreed there should be restrictions on the advertisement of pornography online.

Almost three quarters (74%) of participants thought the advertisement of pornography should be made illegal, similar to tobacco advertising, while 26% disagreed. Similarly, 69% of participants thought the use of pornographic adverts on movies websites such as ‘Putlocker’ should be illegal as young people are being inadvertently exposed to pornographic images. Placing a time restriction on pornographic images being shown online, e.g. 9pm, was proposed as a recommendation at the consultations. However, only 31% agreed with this idea and the majority (69%) disagreed.

Table 5: Would engaging in these activities related to pornography, revenge porn and inappropriate use of photos on a one off basis make them illegal?

Activity	Agreed	Disagreed
Revenge porn- sharing nudes to get back at someone	33 (100%)	0 (0%)
Using intimate photos to blackmail your partner into doing things they’re not comfortable with	27 (93%)	2 (7%)
Group chats sharing of nude photos on Facebook chat used to	28 (85%)	5 (15%)

bully girls/boys		
Lack of monitoring on social media sites, especially private information. Adverts on kid's websites for porn and dating sites. Google should have more regulations for adverts. The law will have to be change constantly as technology advances	26 (84%)	5 (16%)
Porn adverts restricted	23 (82%)	5 (18%)
Leaking nudes, I don't think sending should be illegal but leaking should	24 (75%)	8 (25%)
Porn adverts should be illegal just like tobacco adverts	25 (74%)	9 (26%)
Pornographic adverts on movies sites like Putlocker should be illegal because young people watching things shouldn't see that	22 (69%)	10 (31%)
Using photos to hurt/slander someone	16 (48%)	17 (52%)
Time restriction before any of these images can be shown online e.g. after 9pm	10 (31%)	22 (69%)
Distribution of someone's photos without their consent	7 (23%)	23 (77%)

3.18 Experience of getting something taken down off the internet

Young people at both consultations were asked if they had any experience of getting something taken down off the internet. There were very few personal experiences reported of having content taken down off the internet. One young person said they had texted someone to take down a photo of them off the internet and another young person said her friend had been contact by a person she had posted a photo of on Facebook to ask them to remove it, which they did. Another young person said their friend was successful in getting 'hate groups' on Facebook removed through contacting the social networking website directly.

- *"I texted someone to take down a photo."*
- *"My friend posted up a group picture as her profile picture on Facebook. One person in the picture found it offensive so she reported it and messaged my friend say 'I find it offensive, can you take it down?' She took the photo down but got blocked from Facebook for ten days."*
- *"A friend reported hate groups on Facebook and it was removed. They contacted Facebook directly through the 'report buttons'."*

- *"My friend went to Guards over continuous cyber bullying."*

While a very small number of young people had personal experience of getting something taken down off the internet, participants at both consultations debated the issue and gave recommendations in relation to the topic. In general, young people thought it was very difficult to get something removed from the internet and agreed that social networking websites should make it easier to remove content.

Participants stated that Snapchat has no reporting system at all and only the user who posted a video can remove it, even if it is offensive, which they considered to be an ineffective system.

- *"Snapchat, it has to be the person who posted it can only take it down, e.g. of video of self-harming."*

Young people felt it was difficult to get abusive or explicit content removed from Facebook. They argued that the 'report abuse' function on Facebook does not work well as the threshold for removing content is too high.

- *"The 'report abuse' function on Facebook' doesn't work, standards are too high."*

Users of Instagram reported that the website had removed certain offensive hashtags in the past, but again, they felt the reporting function of the website was ineffective. Young people thought that a number of users had to report photos before they are removed.

- *"The Instagram report button doesn't really get anything changed."*

Some young people gave examples of Facebook and Instagram removing photos of transgendered people and lesbians kissing because they did not fit with their standards and policies which they did not agree with.

- *"Instagram/Facebook taking down pictures of topless women but not men, because of explicit image laws, e.g. transgender women case on Instagram!"*
- *"Facebook took down a picture of two girls kissing."*

Participants who use the website Yik Yak stated that if abusive or explicit content is reported on the site the post can still be seen by users but the person who posted it cannot which they considered to be an unhelpful system.

- *“Yik Yak, if you report to Yik Yak you stop being able to see the person but not the post.”*

Young people considered Tumblr to be “moderately better” than other social media websites in terms of their reporting systems and they thought providing a link to support websites when users look up harmful topics such as self-harm was a good idea. Participants who use Twitter gave examples of abusive tweets being removed directly by the website.

- *“Tumblr have a link to help sites if you look up something of concern, e.g. self-harm, thigh gap.”*

Finally, young people recommended that all social media websites should make it easier to report and take down content from the internet, Facebook should change the tagging function on their site so that tagging of another user in posts and photos must be approved first and that the Gardaí should have more access to social networking websites to investigate abusive content.

Section 4: Summary of Key Findings

4.1 Overview

This section of the report summarises the key findings from consultations with young people on the issues of harmful internet communications, including cyber bullying.

4.2 Key themes identified by young people

Five key themes emerged from the main topics identified by young people related to harmful internet communications including cyber bullying at the two consultation events:

- Theme 1: Cat Fishing/fake profiles and accounts/hacking
- Theme 2: Cyberbullying/trolling/anonymous activity
- Theme 3: Group chats
- Theme 4: Hate speech/discrimination and racism
- Theme 5: Pornography/vengeance porn/inappropriate use of photos

4.3 Theme 1: Catfishing/fake profiles and accounts/hacking

Key findings with regard to catfishing, fake profiles and accounts and hacking included:

- Catfishing or “stealing someone’s identity by making a fake profile” can be used to lure someone into a relationship, to ask for nude photos, to bully people, get people into trouble and to start fights.
- Young people considered catfishing to be potentially very dangerous if someone was lured into meeting up with a ‘catfisher’ and caused harm.

- Impacts of catfishing highlighted by young people included reputational damage, mental health difficulties and suicide.
- Participants argued that social networking websites should take more responsibility for stopping fake accounts.
- Young people thought there should be better education in schools with regard to the issue of catfishing and online safety.

In relation to catfishing, fake profiles and accounts and hacking, young people thought the following activities should be illegal:

- Identity theft (100%)
- Identity theft by creating fake profiles and taking someone's pictures and personal information (97%)
- Catfishing (94%)
- Catfishing to get nude photographs (88%)
- Hacking accounts and messaging people to turn friends against you (88%)
- Taking people's personal details, using it to Catfish, using images (83%)
- Using someone else's name/picture so the 'real' person gets in trouble for bullying (79%)
- Taking pictures of teachers and making fake accounts (75%)
- For older people to pretend they are younger and same age as younger people, e.g. minors (22%)

4.4 Theme 2: Cyberbullying/trolling/anonymous activity

Key findings related to cyber bullying, trolling and anonymous activity included:

- Cyber bullying or trolling was described by participants as online activity which is generally anonymous and can include name calling, abuse, sharing of photos and personal information, online harassment and stalking.
- Websites which allow for anonymous activity were singled out as being particularly conducive to cyber bullying.
- Potential impacts of cyber bullying highlighted by participants included annoyance, embarrassment, damage to reputation, negative impacts on self-esteem, emotional well-being and mental health as well as suicide.
- Young people suggested there should be more education on cyber bullying in schools.

With regard to cyberbullying, trolling/anonymous activity, participants agreed that the following activities should be illegal:

- Online racism, harassment and homophobia (94%)
- Fake profiles used to target a certain person or those who are 'weak' (89%)
- Fake accounts 'to post bad things or pictures of people' to target them (88%)
- Posting comments that damage people's public image (76%)

- Engaging in cyberbullying, even on a once off basis (72%)
- Anonymous social networking site ask.fm (68%)
- Not to take a person's photo down off the internet if they requested it (66%)
- Engaging in activity on gossip pages used for rumour and bullying (64%)
- Ddosing (61%)
- Proxies (51%)
- Being anonymous online on a public forum, e.g. social media, Gossip Girl pages (45%)
- Anonymous profile websites, e.g. any website with private interaction (45%)
- Putting up statuses and tweets etc. to target people (43%)
- Posting photos of other people without their permission/consent (42%)
- Sending personal abusive messages (30%)
- Creating videos/making comments to make fun of something (26%)
- Tagging a person without their consent (26%)

4.5 Theme 3: Group chats

Key findings identified by young people regarding group chats included:

- Group chat is a tool that allows a group of people to communicate with each other online.
- According to young people, group chats are an online forum which is commonly used for bullying, illegal activity and the sharing of harmful content.
- Participants acknowledged that group chats are difficult to monitor and suggested young people should be better educated on the implications and legalities of sharing and receiving content through group chats.
- Young people felt it should be easier to remove personal content from social networking websites and the internet in general and for users to have more control in group chats.

In relation to group chats, participants agreed that the following activities should be illegal:

- Twitter accounts and other website accounts that support self-harm and eating disorders should be banned (97%)
- Posting abusive messages on websites such as 4chan and Tumblr (91%)
- Sharing images without consent (82%)
- Making fake account to talk to people on Facebook messenger (70%)
- Using screenshots, for example of sexting (sexually explicit photographs or messages sent online or by mobile phone) against people in group chats (52%)

4.6 Theme 4: Hate speech/discrimination and racism

Key findings from the consultations on the theme of hate speech, discrimination and racism included:

- The Lesbian, Gay, Bisexual and Transgendered (LGBT) community, religions, ethnic minority groups, people with mental health issues, women, members of the Travelling community and people with disabilities are the main groups who are targets of online hate speech, discrimination and racism.
- Participants felt strongly that online hate speech, discrimination and racism should be blocked or banned by all websites.

Regarding hate speech, discrimination and racism, young people agreed that the following activities should be illegal:

- Discriminative websites targeting religions (90%)
- Posting videos or comments online to promote terrorism (81%)
- Engaging in discrimination against the Lesbian, Gay, Bisexual and Transgendered (LGBT) community online (79%)
- Discrimination against mentally ill people (72%)
- Transphobic tweets and posts (71%)
- Posting information online about people without their consent (24%)

4.7 Theme 5: Pornography/revenge porn/inappropriate use of photos

The key findings identified by participants in terms of pornography, revenge porn and the inappropriate use of photos included:

- The inadvertent exposure of children and young people to pornography adverts online was identified as the key issue relating to pornography.
- Participants would like to see more restrictions on the advertisement of pornography online in general, more monitoring of the advertisement of pornography on social media sites and more regulations on such advertising on websites aimed at children and young people.
- The majority of young people agreed revenge porn should be illegal and stated the main impacts of this activity were on a person's reputation and mental health.
- A large number of young people made recommendations in relation to improving and updating sex education in schools to cover issues such as the implications and legalities of sending and receiving nude photos and online safety in general.
- Other recommendations made by young people included running a public campaign on the topic of online safety and sending nude photos and educating parents.

Participants agreed the following activities related to pornography, revenge porn and inappropriate use of photos should be illegal:

- Revenge porn (100%)
- Using intimate photos to blackmail your partner into doing things they're not comfortable with (93%)
- Sharing of nude photos on group chat such as Facebook to bully girls or boys (85%)
- Leaking, but not the sending of, nude photos (75%)
- Advertisement of pornography (74%)

- Use of pornographic adverts on movies websites such as 'Putlocker' (69%)
- Using photos to hurt or slander someone (48%)
- The distribution of someone's photos without their consent (23%)

4.8 Experience of getting something taken down off the internet

- A very small number of young people had personal experience of getting something taken down off the internet.
- Examples mainly related to young people contacting another young people directly to ask them to remove content rather than getting content removed through a website.
- In general, young people felt it was very difficult to get content taken down off the internet and suggested that social networking websites should make it easier for this to happen.

References

Citron, Danielle Keats; Franks, Mary Anne (2014). "Criminalizing Revenge Porn". *Wake Forest Law Review* 49 (2): 345–392.

Department of Children and Youth Affairs (2015a) *National Youth Strategy 2015- 2020*. Dublin: Government Publications.

Department of Children and Youth Affairs (2015b) *National Strategy on Children and Young People's Participation in Decision-Making*. Dublin: Government Publications.

Department of Children and Youth Affairs (2014) *Better Outcomes, Brighter Futures: The National Policy Framework for Children and Young People, 2014-2020*. Dublin: Government Publications.

Department of Communications, Energy and Natural Resources (2013) *National Digital Strategy*. Dublin: Government Publications.

Department of Education and Skills (2015) *National Digital Strategy for Schools 2015 – 2020*. Dublin: Government Publications.

Department of Education and Skills (2013) *Action Plan on Bullying: Report of the Anti-Bullying Working Group to the Minister for Education and Skills*. Dublin: Government Publications.

Department of Health and Children (2000) *Our Children – Their Lives: National Children's Strategy, 2000-2010*. Dublin: Government Publications.

European Union (2000) *Charter of Fundamental Rights* (2000/C 364/01).

Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Gavin, A., Keane, E., Callaghan, M., Molcho, M., Kelly, C. & Nic Gabhainn, S. (2015). *The Irish Health Behaviour in School-aged Children (HBSC) Study 2014*. Dublin: Department of Health & Galway: Health Promotion Research Centre, National University of Ireland, Galway.

National Youth Council of Ireland (NYCI) (2016) *Screenagers International Research Project: Using ICT, Digital and Social Media in Youth Work, National Report of the Republic of Ireland*. Dublin: NYCI.

O'Neill, B. & Dinh, T. (2015) *Net Children Go Mobile: Full findings from Ireland*. Dublin: Dublin Institute of Technology.

O'Higgins Norman, J. and McGuire, L. (2016) *Cyberbullying in Ireland: A Survey of Parents Internet Usage and Knowledge*. Dublin City University: ABC, National Anti-Bullying Research and Resource Centre.

O'Moore, M. and McGuire L. (2014) *Cyber Bullying: Key Facts*. Dublin City University: ABC, National Anti-Bullying Research and Resource Centre.

Available at: <http://www.tacklebullying.ie/assets/resources/Parents/Cyberbullying%20Brochure2.pdf>

O' Moore, M. (2012) "Cyber-Bullying: the situation in Ireland" *Pastoral Care in Education: an international journal of personal, social and emotional development*. London: Routledge.

United Nations (1989) *UN Convention on the Rights of the Child*. Geneva: United Nations.

Appendix A: Consultation Methodologies

Consultations with young people on cyber crime

Aisling Hotel, 27 and 28 April 2016

11:15 Introduction and Icebreaker

11:30 Open Space Question

What online activity should be illegal?

4 post-its for each young person. 6 young people volunteers group post-its into agreed themes, with support from facilitators.

**12:00 Placemats on the themes identified in the open space session,
with the question:**

What do you mean by this?

12:15 World Café (4 moves with 8 minutes per move)

12:45 Sticky dot voting on the most important themes identified
Participants vote at each table

1:00 Lunch

1:45

Top 6 themes from each table are displayed on cards

Participants again visit each table and discuss:

Would engaging in this activity on a once off basis make this illegal?

After a short discussion, participants indicate agreement or disagreement by placing the appropriate coloured card in the envelope attached to each of the 6. If their answer is yes, they place a green card in the envelope, if no, they place a red card in the envelope.

Participants are given 30 of each colour at the beginning of the exercise.

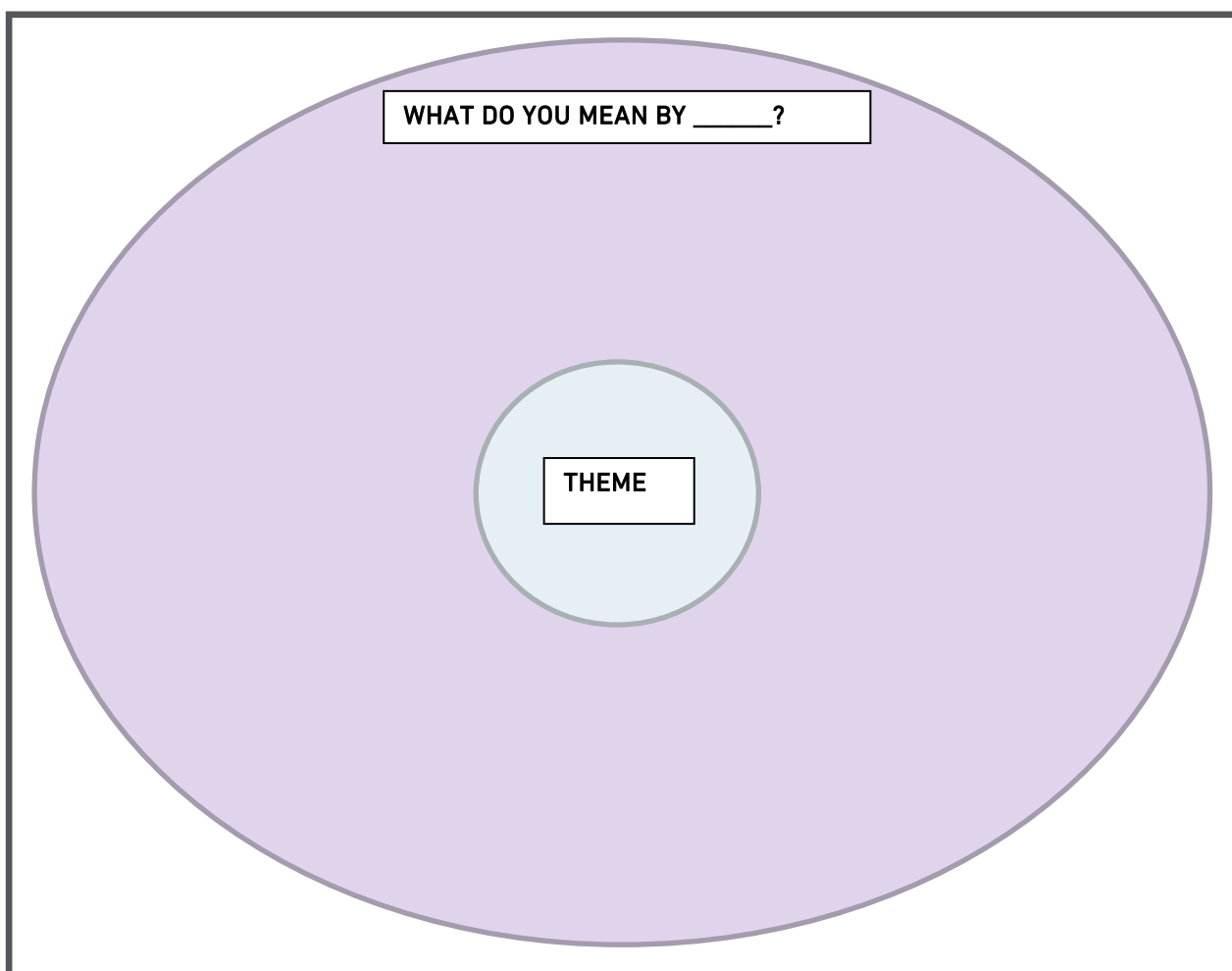
Participants spend 15 minutes at each table before moving to the next table.

3:00

Discussion on the following question in the same groups

Have you any experience of getting something taken down of the internet?

3:15

Evaluation and Close**PLACEMAT:**

Appendix B: Consultation Evaluation Findings

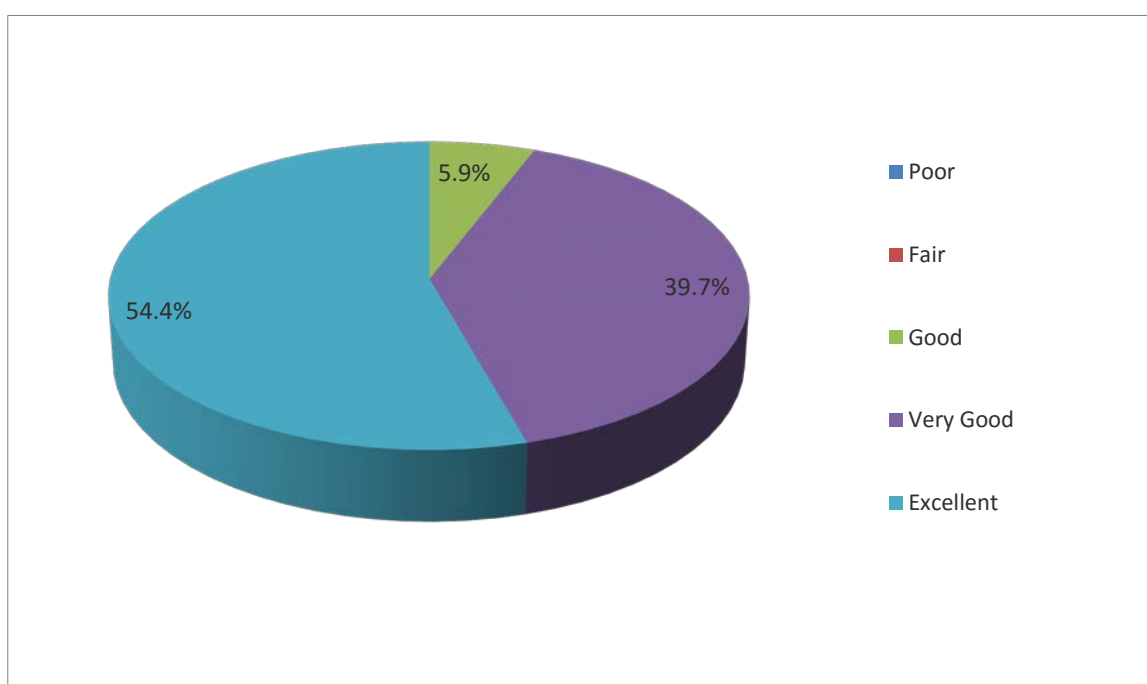
Introduction

Young people who participated in the consultation events completed evaluation forms on the day to see how they rated the consultations overall, the organisation of the consultations, the consultation sessions, the venue and food, what was the best thing about the consultations and what they would change about them.

Rating of consultation days

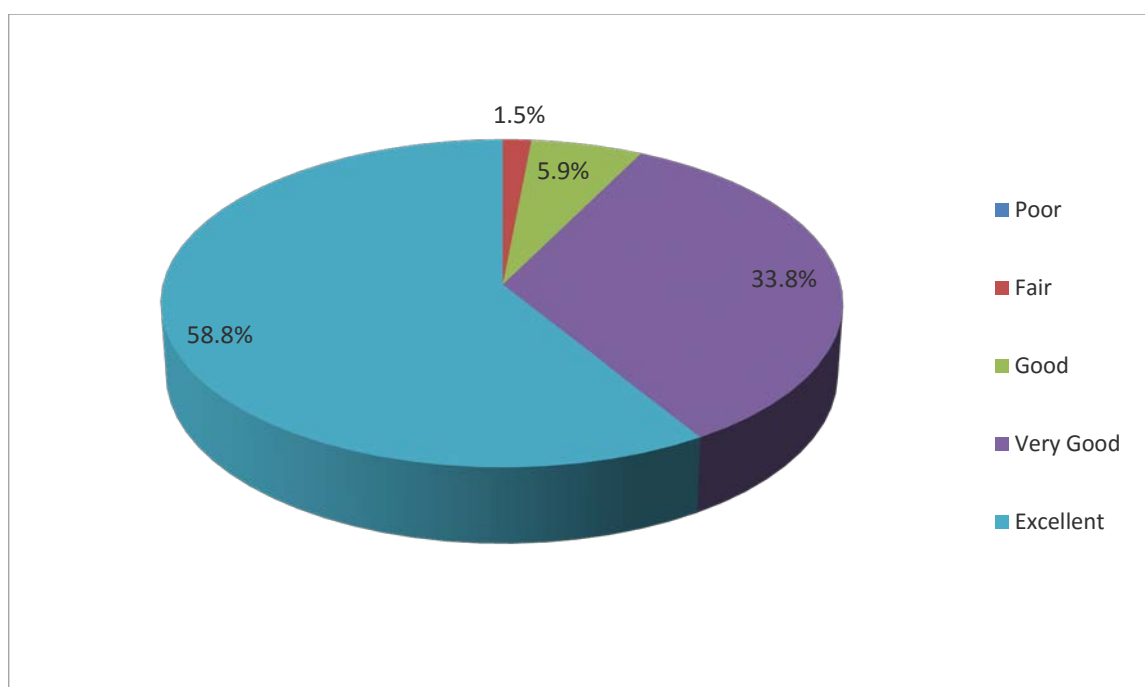
Participants were asked to rate the consultation days overall. As can be seen in Figure 1 below, over half (54.4%) of young people rated the consultations as excellent, almost four in ten (39.7%) rated them as very good and 5.9% rated them as good. No participants rated them as fair or poor.

Figure 1: How would you rate the consultation days overall?



Organisation of consultation days

In relation to the overall organisation of the consultation days, over half (58.8%) of participants rated it as excellent, one third (33.8%) rated it as very good, 5.9% as good and 1.5% as fair. No young people rated the organisation of consultations as poor (see Figure 2 below).

Figure 2: How would you rate the organisation of the consultation days?

Rating of sessions within the consultation days

Young people were asked to rate the different sessions during the consultation days. As can be seen from the table below, the most popular session was the world café workshop on themes with six out of ten (60.3%) young people rating it as excellent, 25% as very good and 14.7% as good. Voting on the themes was the next most popular session, with over half (54.4%) of young people rating it as excellent, 30.9% as very good, 13.2% as good and 1.5% as fair.

The next best rated session was the open space session with 37.9% of participants rating it as excellent, 45.5% as very good, 13.6% and 3% as fair. The next most popular session was the discussion on young people's experience of getting something taken down off the internet, with 36.8% rating it as excellent, 38.2% as very good, 22.1% as good and 2.9% as fair. Finally, just over one third (34.8%) of participants thought the introduction and games were excellent, 39.4% very good, 18.2% good, 4.6% fair and 3% poor.

Participant's ratings of consultation day sessions

	Excellent	Very Good	Good	Fair	Poor	Total
World café workshop on themes (changing tables)	60.3%	25%	14.7%	0%	0%	100%

Agreeing/disagreeing with top 6 themes at each table and voting	54.4%	30.9%	13.2%	1.5%	0%	100%
Open-space (post-its)	37.9%	45.5%	13.6%	3%	0%	100%
Discussion on experience of getting something taken off the internet	36.8%	38.2%	22.1%	2.9%	0%	100%
Introduction and games	34.8%	39.4%	18.2%	4.6%	3%	100%

Venue and food

Three quarters (75%) of young people thought the venue was excellent, 20.6% very good, 2.9% good and 1.5% fair. Just over half of young people (51.5%) rated the food as excellent, 28% as very good, 13.2% as good, 4.4% as fair and 2.9% as poor.

The best thing about the day

Participants at the consultation events were asked what they considered to be the best thing about the day. The majority of young people said the best thing about the day was the group discussions. What participants enjoyed most about the group discussions included having the opportunity to express their opinions, having their opinions and voices listened to, heard and valued, hearing other young people's opinions, learning more about the topic and making a difference by having an input into decision-making.

- *"I thoroughly enjoyed the opening discussions/debates. I felt my opinion was being taken on board and valued."*
- *"Learning more about cyber-crime, being given the opportunity to express my views."*
- *"Discussion with the group, I enjoy hearing about other people's opinions on different topics."*
- *"Knowing that the work we did will hopefully shape a better future for young people."*

According to participants, the next best thing about the day was meeting new people and socialising with other young people.

- *"I really enjoyed getting to meet/get to know more people who shared similar interests as me."*
- *"Socialising with various other Comhairle groups/members."*

Other aspects of the day that young people considered to be the best things about the consultations included the food, the world café method, the voting session, the introduction/games and the location and the facilitators.

- *"The food was excellent, organisation was top notch and the day was very enjoyable."*
- *"It was great to move tables."*
- *"The agree/disagree section was very enjoyable."*
- *"The intro - when we came in - scones, tea, the games, etc."*
- *"Just to say the location was great as it was really close to all the train/bus stations."*
- *"The adults at the tables supervising were very helpful and really cared for our opinions. Thank you for such a lovely day."*

What would you change about the day?

Young people who attended the consultations were asked what, if anything, they would have changed about the day. Changes related to the methodologies used at the consultation events were the most commonly suggested modifications. With regard to the voting process, a number of young people thought some of the statements they voted on were unclear, did not link to being legal/illegal and there were too many options to vote on.

- *"The idea of what's illegal as some of them didn't link."*
- *"Voting process - too many options."*

In terms of the world café methodology, young people would have liked more time for discussions. Participants would also have liked to spend more time on the open space session to suggest topics. Some young people thought the topics discussed on the day were repetitive. Finally, some young people would have liked other methods of getting their points across on the day and one person would have liked a more anonymous way of communicating their opinions to avoid embarrassment.

- *"I would have given longer time at the tables during the world cafe workshops on themes."*
- *"I would give more time to suggesting topics in the morning."*
- *"Some topics were quite repetitive."*
- *"More anonymous; so you can feel comfortable expressing your opinion."*

Other aspects of the days participants would have changed included having more ice-breakers in the smaller groups to get to know each other better, the air conditioning in the room which was considered to be too hot, having a larger open space, a better selection of food, more time to talk and socialise with other young people, a longer lunchtime and more emphasis on fun.

- *"More ice breakers possibly peer led. Smaller ice-breakers in the smaller groups."*
- *"The temp in the room - a bit too hot."*
- *"Bigger room space."*
- *"The food could have been 10 times better."*
- *"I would give the young people more chance to talk also a longer lunchtime so people can go outside for some fresh air."*