Report of the

Internet Content Governance Advisory Group

May 2014

Roinn Cumarsáide, Fuinnimh agus Acmhainní Nádúrtha
Department of Communications, Energy and Natural Resources

Table of Contents

Foreword by the Chairperson

As Chairperson, I am pleased to present the following Report of the Internet Content Governance Advisory Group.

The Minister for Communications, Energy and Natural Resources, Pat Rabbitte TD, established the group to consider the existing national regulatory and legislative frameworks, and policy responses to issues of internet content governance, specifically in relation to online abuse and the accessing of potentially harmful content.

The internet offers profound opportunities to Irish society. However, as a free, open and global environment, it challenges many accepted norms and also creates evident risks to which society must respond.

Some 15 years ago, the Working Group on Illegal and Harmful Use of the Internet proposed a system of industry self-regulation combined with governmental support for education to address the opportunities and the risks that the internet affords. The system that subsequently developed has proved to be robust and capable of responding to online harms, particularly of an illegal nature.

Our focus, rather, is directed at the context in which the now pervasive use of the internet for media consumption, creation and sharing of content online, especially through the use of social media, may create challenges for all citizens, but especially for children and young people. Research shows that while most users' experience of the internet is positive, a minority is adversely affected or has suffered some form of online harm. Risks arise in relation to bullying and harassment that can take place in the many online communities in which young people participate. The internet is also host to much content that is negative or age-inappropriate and which may prove harmful to vulnerable young users or have adverse effects on their development.

How government should respond and what the most appropriate relationship should be between industry, online service providers, the State and citizens in relation to internet content is the subject of our report. We believe it is vital to build on Ireland's well-established foundation for internet safety while addressing the new reality of an almost fully converged environment for information, online communication and entertainment. This calls for both unique and tailored solutions as well as a review of extant law and government structures relating to internet content governance.

We outline a set of proposals that we believe will bring about better coordination of existing governance measures and that target guidance and support to where it is needed most. We also recommend the consolidation of national governmental capacity to manage the both the opportunities and inevitable risks that arise from convergence around the global internet.

The internet is a fluid, evolving environment, requiring policy makers, industry and relevant stakeholders to be flexible as they adapt to changing and emerging contexts. The internet does not now and will not stand still. We hope that the work of the Internet Content Governance Advisory Group will assist in shaping the governmental response, in the interests of all citizens, to an on going process of innovation, convergence and technological mediation.

Brian O'Neill *Chairperson*

List of Acronyms

IEDR	.ie Domain Registry
AUPs	Acceptable Use Policies
ASAI	Advertising Standards Authority for Ireland
AF	Audiovisual Federation
AVMSD	Audiovisual Media Service Directive
ATVOD	Authority for Television on Demand
BBFC	British Board of Film Classification
BAI	Broadcasting Authority of Ireland
COPPA	Children's Online Privacy Protection Act
DCYA	Department of Children and Youth Affairs
DCENR	Department of Communications, Energy and Natural Resources
DES	Department of Education and Skills
DoH	Department of Health
DJE	Department of Justice and Equality
eID	Electronic Identification
FSF	Freiwillige Selbstkontrolle Fernsehen Voluntary Self-Regulation of Television
FSM	Freiwillige Selbstkontrolle Multimedia-Diensteanbieter Voluntary Self-Regulation of Multimedia Service Providers
INHOPE	International Association of Internet Hotlines
ITU	International Telecommunication Union
IAB	Internet Advisory Board
ICRA	Internet Content Rating Association
ICANN	Internet Corporation for Assigned Names and Numbers
ISAC	Internet Safety Advisory Committee
ISPs	Internet Service Providers
ISPAI	Internet Service Providers Association of Ireland
IBEC	Irish Business and Employers Federation
ICIA	Irish Cellular Industry Association
IFCO	Irish Film Classification Office
ISSU	Irish Second-Level Students' Union
KJM	Kommission für Jugendmedienschutz (Commission for Youth Media Protection)

MNO	Mobile Network Operator
NAPD	National Association of Principals and Deputy Principals
NCCIS	National Council for Child Internet Safety
NCCA	National Council for Curriculum and Assessment
NEPS	National Educational Psychological Service
NICAM	Netherlands Institute for the Classification of Audiovisual Media
OiS	Office for Internet Safety
ODPC	Office of the Data Protection Commissioner
OCO	Office of the Ombudsman for Children
ODAS	On Demand Audiovisual Media Services
Euro-DIG	Pan-European Dialogue on Internet Governance
PEGI	Pan-European Games Information
PICS	Platform for Internet Content Selection
PRS	Premium Rate Services
PDST	Professional Development Services for Teachers
SIIC	Safer Internet Ireland Centre
SPHE	Social, Personal and Health Education
TIF	Telecommunications and Internet Federation
UKCCIS	UK Council for Child Internet Safety
UGC	User Generated Content

Terms of Reference

The Internet Content Governance Advisory Group was established by the Minister for Communications, Energy and Natural Resources, Pat Rabbitte TD, in December 2013. The terms of reference given to the group by the Minister were as follows:

Having regard in particular to:

- *The development of the internet as a platform for media consumption, creation and dissemination of content on a pervasive basis, and in particular the increased use and prominence of social media;*
- *The profound opportunities that the internet offers to society as a whole, and to children and young people in particular;*
- *Risks of bullying and harassment, particularly with regard to children online;*
- *The present national regulatory and legislative framework around electronic communications, internet governance and the sharing and accessing of material online;*
- *Recent proposals in other jurisdictions to request that ISPs block access 'by default' to certain age-inappropriate but otherwise legal material;*
- *The need to preserve the free and open nature of the internet, and to preserve freedom of speech and freedom of access to information online;*
- *The recent report of the Joint Oireachtas Committee titled 'Addressing the Growth of Social Media and Tackling Cyberbullying';*
- *Recent decisions taken at the ECHR on the issue of online commentary.*

The Taskforce is requested to consider the following and make recommendations to the Minister by 30th May 2014:

- *Whether the existing national regulatory and legislative frameworks around electronic communications, internet governance and the sharing and accessing of content online remain relevant;*
- *Whether other existing policy responses by the State remain sufficient in relation to dealing with any of these issues;*
- *What the most appropriate relationship should be between ISPs, online service providers, the State and citizens in relation to internet content that may be age-inappropriate and to bullying and harassment online.*

Acknowledgements

The group would like to acknowledge the co-operation of the many organisations, both public and private, and individuals whose assistance was invaluable in the preparation of this report. The group would also like to express its gratitude to Richard A. Browne and Áine McHugh (Department of Communications, Energy and Natural Resources) for their dedicated support throughout the process and making its work productive and efficient.

Membership of the Group

Dr Brian O'Neill, *Chairperson*
Head of Research, College of Arts and Tourism
Dublin Institute of Technology

Mary Aiken
Director of the CyberPsychology Research Centre
Royal College of Surgeons in Ireland

Mark Caffrey
President, Irish Second-Level Students' Union

Prof Joe Carthy
College Principal and Dean of Science, Director of the Centre for Cybersecurity and Cybercrime Investigation (CCI)
University College Dublin

Ronan Lupton
Barrister-at-Law, Chair, Association of Licensed Telecommunications Operators (ALTO)

Áine Lynch
CEO, National Parents Council (Primary)

Kate O'Sullivan
Vice-President Corporate Affairs, UPC Ireland

Summary of Recommendations

Institutional/structural recommendations

Revised role for the Office for Internet Safety

1. We recommend that that the Office for Internet Safety (OiS) should be reconfigured to deal exclusively with issues of law enforcement and illegal online content. It may be retitled or have its role reduced to an administrative function. It should be given clear terms of reference clarifying its role in providing oversight of the system of self-regulation for illegal internet content.
2. The OiS should include within its terms of reference an assessment of the industry self-regulatory code of practice.
3. The OiS should include within its remit oversight of the current voluntary blocking of illegal internet content undertaken by mobile network operators.

The National Council for Child Internet Safety

4. We recommend that the Internet Safety Advisory Committee (ISAC) be expanded and reconfigured as the National Council for Child Internet Safety (NCCIS). This council should act as the primary multi-stakeholder forum for internet safety strategy in Ireland. It should include representation from industry, relevant government departments, public bodies, civil society including youth representation and child protection interests.
5. Responsibility for the secretariat function for the council should be assigned to the Department of Children and Youth Affairs. The council should be chaired at ministerial or junior ministerial level to ensure that its work receives the appropriate level of political support.
6. The council should act as coordinator for the Safer Internet Ireland project, in particular its awareness-raising, education and helpline functions.
7. The council should establish working groups to deal separately with issues of research, education and industry safety implementation. Working groups reporting to the council should guide its work with the most up-to-date information available, informed by international best practice.
8. The council should seek to harness innovative technology, tools and educational approaches in promoting internet safety and standards of digital citizenship, advising all relevant stakeholder groups with regard to emerging risks and good practices in dealing with online abuse.
9. The council should foster close co-operation between stakeholders and in particular ensure the effectiveness of industry measures, as envisaged in Objective 3.19 of the National Policy Framework for Children and Young People. In particular, the participation on the council of leading internet companies located in Ireland and representative industry associations should be encouraged.
10. The council should collaborate with the implementation group for the Anti-Bullying Action Plan to coordinate stakeholder responses to all internet-related dimensions of bullying and abuse. It should also commission research on the most effective ways to counteract bullying and harassment and on the impact of exposure by minors to age-inappropriate content.

The Safer Internet Ireland Centre (SIIC)

11. We recommend that the Safer Internet Ireland project, currently co-financed by the European Commission, be enhanced to act as the Safer Internet Ireland Centre (SIIC). While it is envisaged that resourcing will continue to be available through the Connecting Europe Facility, it is important that government ensures that this vital public service is fully resourced.

12. The SIIC should operate through a common online platform and brand, and offer a helpline, educational resource and awareness-raising function for children and young people, for teachers and educators, and for parents. It should act as a one-stop portal designed to address the likely volume of enquires, aggregating available support content and serve as a directory/information resource for the general public.

13. Oversight of the SIIC should be undertaken by the National Council for Child Internet Safety, with advisory input as required from government departments such as the Departments of Communications, Energy and Natural Resources (DCENR), Education and Skills (DES) and Justice and Equality (DJE).

14. The SIIC should:

    - compile resources of best practices in dealing with online abuse and harassment for parents, teachers and young people;
    - plan and direct a national awareness campaign on effective measures to deal with the reporting cyberbullying and online abuse;
    - provide guidance to schools on incorporating in their anti-bullying policies best practice in relation to social media and online communication;
    - work with the Office of the Data Protection Commissioner (ODPC) to raise awareness of privacy issues in the sharing of content online and the most appropriate ways to deal with violations of privacy;
    - promote the Hotline.ie services for reporting illegal content, including racist speech and incitement to hatred.

Legislative measures

15. We recommend that the Communications Regulation (Amendment) Act 2007 be amended to include 'electronic communications' within the definition of measures dealing with the 'sending of messages which are grossly offensive, indecent, obscene or menacing'.

16. Further, we advise that the Minister for Communications, Energy and Natural Resources suggest that the Minister for Justice, in conjunction with the Attorney General and the High Court Rules Committee, establish a review of the suitability of current non-party discovery and disclosure rules of court, to bring current court discovery and disclosure processes in line with societal and technological norms.

Administrative/policy questions

Internet content governance

17. We recommend that DCENR be formally charged with coordinating internet content policy at government level in addition to its extant roles in dealing with these issues at an international level.
18. We also recommend the formation of a standing Inter-Departmental Committee to cover all aspects of internet governance.
19. The Department should take the lead in developing a high level media policy framework, dealing with the effects of technological change on media in general, and specifically on audiovisual and online media, including an on-going review of best/new practices in European and international jurisdictions that may help address the issue of availability of age-inappropriate content regarding minors.

On-Demand audiovisual media services

20. Responsibility for the implementation of the provisions of the Audiovisual Media Services Directive, presently vested in the On-Demand Audiovisual Media Services entity (or ODAS), should be assigned to the Broadcasting Authority of Ireland (BAI).
21. BAI and DCENR should also monitor the impact of measures to regulate restricted on-demand content in other jurisdictions, including the application of age-verification systems.

Dealing with cyberbullying and harassment

22. An inter-agency working group should be established by DES in conjunction with the National Council for Curriculum and Assessment (NCCA) to identify appropriate mechanisms to ensure that internet safety and digital literacy skills are taught as a core element of the curriculum at both primary and post-primary levels.
23. Supports for schools on the implementation of the Social, Personal and Health Education (SPHE) programme as part of the Primary and Junior Cycle curricula need to be updated to promote a positive, safer, and more effective use of technology by children.
24. Further support should be given to training directed at parents to make them aware of the risks of cyberbullying and how to deal with it. Training initiatives such as those developed by the National Parents' Council, should be further expanded and resourced.
25. We recommend that the Garda Síochána Schools "Respectful Online Communication" and "Connect with Respect" programmes, dealing with cyberbullying among other topics, be extended to include a learning resource for parents to explain the role of policing in relation to online abuse and harassment.

Dealing with accessing of age-inappropriate content

26. Internet service providers (ISPs) and mobile network operators (MNOs) should be encouraged to include parental control products and services as part of their consumer offering. In particular, ISPs and MNOs should provide advice and support about how to configure the different filtering solutions available, including those for portable internet-enabled devices, to assist parents in managing children and young people's internet access.

27. An awareness-raising campaign to encourage parents to make more use of the array of parental controls should be developed as a collaborative initiative of National Parent Councils, youth representative organisations, children's charities and industry. Awareness messages about parental controls should emphasise that they are not complete solutions but have a role to play in an overall digital parenting context.

28. The application of filtering on public Wi-Fi access points or hotspots is ultimately a decision for the provider concerned, taking into account the likelihood of children using Wi-Fi in that location for internet access. Terms of use should be prominently displayed at the point of access, stating clearly whether a service is a filtered one or not. A 'family-friendly' logo to designate the use of filtering of adult or other age-inappropriate content for public Wi-Fi access points should be developed.

29. Awareness-raising by relevant agencies and by industry should provide authoritative guidance and support targeted at specific groups of users likely to access potentially harmful content, e.g. teenage girls who may access pro-anorexia content, younger adolescents who may come across sexual or pornographic content, vulnerable children or those with psychological difficulties, etc.

30. Awareness-raising should also include the development of specific resources targeted at parents to make them aware of the current labelling systems, such as PEGI (Pan-European Games Information) and PEGI-Online for gaming content, as well as other emerging rating systems for online content.

Chapter 1: Introduction

"The internet is a resource for everyone. It provides all of us with new ways to interact, communicate, be creative and productive."[1]

1.1 Irish society and the internet

Irish society benefits enormously from the internet. It offers a wealth of opportunities to Irish citizens and creates new ways to communicate and share knowledge that can transform education, business and social, cultural and political life. The digital sector is of profound importance to the Irish economy; Ireland's reputation as a global hub for leading internet industries is an important factor in economic recovery. The digital sector contributes 4.4% to Ireland's GDP and supports 95,000 jobs both directly and indirectly.[2]

More importantly, the internet has transformed Irish society in many positive ways. Eight in 10 of all households in Ireland now have access to the internet at home. Over 60% of the population go online daily for email, to find information about goods and services, to engage in social networking and to access a variety of e-commerce and other services.[3] Young people in Ireland are to the fore in terms of internet adoption and use, enthusiastically embracing online opportunities. Findings from Growing Up in Ireland, the national longitudinal study of children, show that Irish households with children are more likely to be online than those without children.[4] According to EU Kids Online, the pan-European survey of 9-16 year-olds' internet use, Irish children's use of the internet at home is among the highest in Europe.[5] Young people engage in a wide range of creative, productive and communicative activities, using a great variety of technologies and devices for entertainment and online communication. The increasing trend towards an ever-younger age for online use underlines the fact that the internet is thoroughly embedded in all aspects of young people's lives in Ireland today.

Yet, alongside its many benefits, the internet also brings risks and the potential for harm, especially for children and young people. Increased risks of online bullying and harassment have been the subject of much public debate. The internet enables easy access to content that may be inappropriate for children or harmful for their development. It also raises concerns about the risk of children coming into contact with strangers, including predatory contact.

How to address such concerns and to ensure that the appropriate safeguards are in place has been the subject of policy debate since launch of the World Wide Web. Acknowledged to be a shared responsibility of government, industry, educators, civil society and users themselves,[6] governance arrangements need to adapt to changing conditions and emerging risks arising from pervasive internet use. Internet governance is, however, inherently complex, and especially so in relation to questions of online content.

---

1 DCENR. (2013). Doing More with Digital National Digital Strategy for Ireland Phase 1 – Digital Engagement. Dublin: Department of Communications, Energy and Natural Resources.

2 *Ibid.* p.2.

3 Information Society Statistics, Households 2013, CSO. Retrieved from http://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2013/.

4 McCoy, S., Quail, A. & Smyth, E. (2012). *Growing Up in Ireland. Influences On 9-Year-Olds' Learning: Home, School and Community. Report 3.* Dublin: Department of Children and Youth Affairs.

5 O'Neill, B., Grehan, S. & Ólafsson, K. (2011). *Risks and safety for children on the internet: the Ireland report.* LSE, London: EU Kids Online.

6 European Commission (2013). Safer Internet – Digital Agenda for Europe. Retrieved from http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids.

Freedom of expression and information on the internet, regardless of frontiers, are fundamental values espoused by the international community and propounded by bodies such as the Internet Governance Forum,[7] the Council of Europe[8] and the International Telecommunications Union (ITU).[9] At the same, protecting internet users, particularly young people, is recognised as vital to ensuring trust and confidence in the online environment.[10]

In 2013, the Oireachtas Joint Committee on Transport and Communications held a series of public hearings on the challenges facing individuals, families and communities arising from the use of social media, including the challenges posed by cyberbullying and online harassment. The Committee's report, *Addressing the Growth of Social Media and Tackling Cyberbullying*, made a number of recommendations for consideration by government regarding legislative and policy responses to online safety issues.[11] Responding to this report, the Minister for Communications, Energy and Natural Resources, Pat Rabbitte TD, established the Internet Content Governance Advisory Group to consider its findings, and in light of national and international debates on internet safety and content governance, requested that the group recommend how best to take forward legislative, regulatory and policy provision in this area.

1.2 Areas of focus

The Internet Content Governance Advisory Group has been asked to consider the emerging issues arising from pervasive access to online content, and its impact on society as a whole, and to take particular account of issues of online safety arising from children and young people's use of the internet. The issues concerned are extensive and wide-ranging: the internet affords access to content on a vast and unprecedented scale, outpacing long-established regulatory and legislative approaches to content regulation, as, for instance, for print publications, cinema, radio and television. Similarly, communication and social interaction has been transformed by the widespread adoption of social media platforms, leading to new challenges for legislators and policymakers in regulating conduct by citizens.

The Irish Constitution or *Bunreacht na hÉireann* provides the most logical frame of reference for many of the issues that the Internet Content Governance Advisory Group has had to consider. The Irish Constitution was, in many ways, ahead of its time in expressly conferring both numerated and unenumerated constitutional protections on the individual's good name and indeed protection of individual freedom of expression[12] and other rights.

The two most important Articles of the Constitution in this field are:

1. Article 40.3.1° which contains a guarantee by the State to defend and vindicate the personal rights of the citizen.
2. Article 40.3.2° which requires the State, by its laws, to protect and vindicate in particular certain personal rights, including the right to good name.

---

7 http://www.intgovforum.org/.

8 http://www.coe.int/t/informationsociety/.

9 http://www.itu.int/osg/csd/intgov/.

10 Safeguarding the open internet for all. (2013, 7). *Neelie Kroes Blog*. Retrieved from http://ec.europa.eu/commission_2010-2014/kroes/en/blog/open-internet.

11 Joint Committee on Transport and Communications. (2013). *Addressing the Growth of Social Media and Tackling Cyberbullying*. Dublin: Houses of the Oireachtas.

12 *Cornec v. Morrice* [2012] 1 IR 804; *Sullivan v. Boylan* [2012] IEHC 389; *Sullivan v. Boylan* (No. 2) [2013] IEHC 104.

The law that seeks to fulfil some of these Constitutional obligations is the law of defamation.

Defamation law, in effect, strives to find a constitutionally acceptable balance between the exercise of the right to freedom of expression guaranteed under Article 40.6.1° (i) of the Constitution and the obligation to protect and vindicate reputation provided by Article 40.3.2°.

The two Articles of the Irish Constitution referenced above, arise under the heading Fundamental Rights and are noteworthy in that: 40.6.1°(i) acknowledges *"the rightful liberty of expression, including criticism of Government policy"* for example of the media, and Article 40.3.2° which also pledges that the State, as part of its general obligation to defend and vindicate the personal rights of the citizen, will *"in particular, by its laws protect as best it may from unjust attack and, in the case of injustice done, vindicate the ... good name ... of every citizen"*.[13]

Importantly, and in light of the Supreme Court's decision in *McD. v. L.*,[14] it must be acknowledged that the European Convention on Human Rights (ECHR) is not, as such, directly effective in Irish law, but rather has effect only under the conditions actually specified in the European Convention of Human Rights Act, 2003. Additionally, as a consequence of the Supreme Court's decision in *Carmody v. Minister for Justice and Equality*,[15] the Irish Courts are first required to examine any question presented for resolution under the terms of the Constitution. It is only that in the event that the Constitution cannot avail the litigant who pleads or suggests that his or her constitutional rights have been infringed that the Court can then turn to a consideration of the position under the Act of 2003.

It is these constitutional rights, and by extension the European Convention rights (Articles 8 and 10), that have been brought into sharp focus coupled with the overarching requirement for balance, considering Ireland's now more diverse, plural and secular society. The deliberations and consultation process undertaken by the group has had to include consideration of the governance, operation and vindication of those constitutional rights that may be exercised or indeed infringed by means of, or over the internet.

Among the many areas of concern in relation to internet content governance, we focused our attention on the two substantive issues of: *conduct* or behavioural abuse online, in particular dealing with cyberbullying and harassment, and *content*, or possible harms arising from the accessing of harmful content, especially by young people.

As outlined in its terms of reference, the group then proceeded to address the following three questions:

1. Whether the existing national regulatory and legislative frameworks around electronic communications, internet governance and the sharing and accessing of content online remain relevant;
2. Whether other existing policy responses by the State remain sufficient in relation to dealing with any of these issues;
3. What the most appropriate relationship should be between ISPs, online service providers, the State and citizens in relation to internet content that may be age-inappropriate and to bullying and harassment online.

[13] See further, the discussion of the significance of this right in *Barrett v. Independent Newspapers* [1986] IR. 13;

[14] [2009] IESC 81

[15] [2009] IESC 71, [2010] 1 ILRM 157

In examining the above questions, we reviewed existing legislative and regulatory arrangements as well as policy responses to both substantive concerns in turn. Our examination, framed within a national context, sought to address if, where and how the State should be involved in contributing to safeguards for citizens when they go online. The group was conscious, however, that the national context is just one part of the equation and, given the global scale on which the internet is organised and the worldwide relationships it entails, we also take into account the wider international context in which internet governance, regulation and online safety are debated.

1.3 Content governance and the internet

The internet is a vast and intricate environment of networked technologies, communication links and operating systems that defies easy manipulation or control. Designed as a network to withstand destruction, it has a radically decentralised architecture, without any single point of control or coordination. Its underlying technology ensures that information and data of any kind seek the optimum route to their destination, leading one commentator to claim that its design is such that it 'treats censorship like damage and routes around it'.[16] Regulation of or control over the internet's infrastructure is, therefore, inherently complex and not amenable to easy technological, legal or political solutions.

Since its origins, the internet has been characterised as a large, self-regulating community, committed to values of freedom of expression and the free flow of information, with a high degree of resistance to external control.[17] But that is not to say that the internet is without regulation. Lawrence Lessig, renowned cyber-theorist and lawyer, described *laws, social norms, market and architecture or code* as the four key modalities shaping the online world.[18] No one dimension exerts complete control. Social norms play a major role in the conduct and regulation of online communities; yet, as Lessig argues, 'code' or architecture is a central determining factor, just as market forces and, increasingly, laws shape and determine the contours of online experiences.

The regulation of harmful and illegal material on the internet has been vigorously debated since the early years of the World Wide Web. Two competing approaches stand out.

In the first instance, there is the approach that treats the internet as essentially an extension to the traditional media environment, albeit in a new, interactive and converged form but to which equivalent standards and controls should apply. There have been notable efforts, such as the ill-fated Communications Decency Act (1996) in the United States, that have sought to apply traditional media content controls to the online environment. Among its provisions, the Act sought to make it an offence to knowingly transmit or display over the internet 'patently offensive' material where it would be viewable by persons under 18 years of age.[19] If the initial efforts at imposing direct content regulation proved to be ultimately unsuccessful, subsequent efforts have sought to apply some of the lessons from the traditional media world to the online world. These include classification and labelling schemes in the form of guidance to parents, age verification techniques and parental control tools as a means of controlling access to services and restricting how and when young people gain access to content online.

---

16 Walker, J. (2003). The digital imprimatur: How big brother and big media can put the internet genie back in the bottle. *Knowledge, Technology & Policy*, 16(3), 24-77.

17 Rheingold, H. (1993). *The virtual community: Finding connection in a computerized world.* Addison-Wesley Longman Publishing Co., Inc.

18 Lessig, L. (1999). *Code and Other Laws of Cyberspace.* New York: Basic Books.

19 Reid, A. S. (2005). The rise of third generation phones: The implications for child protection. *Information & Communications Technology Law, 14*(2), 89-113.

The second approach presents the internet as a very different domain to which traditional media norms do not apply. The internet, in this view, represents a new form of public space in which human rights and fundamental freedoms are pre-eminent. Accordingly, access to online content is something that should not be restricted or subject to censorship in any form, except in the case of clear illegality. The European Convention on Human Rights, specifically the right to freedom of expression (Article 10) and to freedom of association (Article 11), provides a foundation for this approach. The only restrictions on such freedoms are those prescribed by law and which are necessary for the prevention of crime, as in the case of distribution of illegal child abuse material or in a limited number of other cases.[20] The Group has noted in the case of *Yildirim v. Turkey*[21] the European Court of Human Rights acknowledged that: *"In view of the fact that legislation concerning the internet, which has to be seen against a background of rapidly changing new technologies, is particularly dynamic and fragmented, it is difficult to identify common standards based on a comparison of the legal situation in Council of Europe member States."* This remains a significant challenge, given Ireland's special role in the facilitation of the information society globally.

A further fundamental principle is that ISPs act only as 'mere conduits'[22] for content that is uploaded and shared by the millions of internet users who access their services. Internet service providers, in this sense, do not have any responsibility for the content carried on their networks, until such time as they are formally made aware of the nature and legality of that content, and are required, either by law, or by court order to remove same. Under the terms of the EU E-Commerce Directive (2000/31/EC),[23] providers are exempt from any liability for content they carry if they do not knowingly act to promote harmful or illegal material and act expeditiously to remove any such content once notified by competent authorities. An equivalent provision applies in the United States in the form of the Digital Millennium Copyright Act 1998, whereby immunity for internet intermediaries applies on the basis that responsibility for content lies with users rather than with service providers. Users decide on the suitability of content; the service providers' role is to provide innovative communications platforms and services.

In practice, the boundaries between the two positions have become blurred. Increasing convergence means that content is available across multiple platforms and potentially subject to different regulatory regimes. The European Commission's Green Paper (2013/231) *Preparing for a Fully Converged Audiovisual World*[24] highlights this dilemma

---

20 More specifically "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". Retrieved from http://www.echr.coe.int/Documents/Convention_ENG.pdf

21 Judgement of the European Court of Human Rights in *Yildirim v. Turkey*. Application no. 3111/10, judgment of 18 December 2012, at para. 31.

22 Article 12: *"1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:(a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.*

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

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."

23 Recital (42): *"The exemptions from liability established in this Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, which implies that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored."*

24 European Commission. (2013). Green Paper COM(2013) 231 final. Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0231:FIN:EN:PDF

and poses a series of questions around the challenges that arise in the governance of converged media in promoting values such as freedom of expression and the freedom of access, and in protecting minors in a converging audiovisual landscape.

1.4 State involvement and regulation

A related question arises as to the role of the state, if any, in the internet environment. Regulation of sectors such as broadcasting and telecommunications position the state as a central actor in providing oversight of the market and the maintenance of standards, but, arguably, a different relationship applies in relation to the internet. Legal scholars Brown and Marsden (2013) characterise three principal varieties of state involvement in internet regulation.[25] First, there is the view that self-regulation with minimal state involvement is the most effective approach to regulating a fast-paced dynamic sector such as the internet. A second approach is to provide for increased state involvement in internet regulation, whether directly in the form of legislative support (or control) of the internet within its jurisdiction or more indirectly through asserting increased influence through state regulatory agencies. The third approach is that of multi-stakeholder coregulation, wherein the role of civil society and other stakeholders involved in the internet arena is recognised and/or represented in decision-making processes.

Over the last decade, against a background of rapid technological development and growth in the digital economy, it is self-regulation that has tended to dominate, while direct state involvement is the exception rather than the norm. Self-regulation in the field of internet safety has received strong support in the European Union and elsewhere, and is sometimes credited with enabling the industry to identify targeted, proportionate and effective solutions to issues of global concern. Yet self-regulation rarely exists without some form of governmental oversight, and, more recently, self-regulatory schemes have incorporated a much greater degree of governmental involvement, partnering with industry to achieve desired outcomes and, in the case of Turkey, directly intervening to censor or block services the government may not approve of. In internet governance debates more generally, multi-stakeholder involvement is widely supported through such processes as the Internet Governance Forum,[26] the Internet Corporation for Assigned Names and Numbers (ICANN)[27] and the pan-European dialogue on internet governance, EuroDIG.[28] Similarly, internet safety policy development has relied on mechanisms for multi-stakeholder involvement ranging from the annual Safer Internet Forum,[29] representative bodies such as Ireland's Internet Safety Advisory Committee (ISAC)[30] and the UK's Council for Child Internet Safety (UKCCIS),[31] as well as forums facilitating youth participation.[32]

The term 'governance' itself, as used throughout this report, points to a shift that has taken place from viewing 'the state as the central actor and legislation as the main instrument, instead towards more heterogeneous regulatory structures'.[33] Internet content governance, for instance, encompasses the notion that there is not necessarily a single (state) regulator for defining content standards but that, alongside traditional approaches

25 Brown, I. & Marsden, C. T. (2013). *Regulating code: Good governance and better regulation in the information age.* MIT Press.

26 http://www.intgovforum.org

27 https://www.icann.org/

28 http://www.eurodig.org/

29 http://www.saferInternet.org/

30 http://www.Internetsafety.ie/website/ois/oisweb.nsf/page/aboutus-isac-en

31 https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

32 http://www.saferInternet.org/ireland

33 Katzenbach, C. (2013). Media Governance and Technology: From 'Code is Law' to Governance Constellations. In: Monroe Price, Stefaan Verhulst and Libby Morgan (Eds.). *Routledge Handbook of Media Law.* Abingdon, New York: Routledge, 399-418.

to legislation, various mechanisms of 'private law' – such as contracts, end-user agreements, and terms of service set by internet companies – as well as international norms and standards with regard to fundamental rights increasingly shape discourse regarding online content. This entails, as regulatory theorists point out, taking into consideration the plurality of actors and the flexible nature of the stakeholder coalitions needed to address what is a deeply embedded, rather than an external dimension, of contemporary life.[34]

1.5 From a safer to a better internet

It is now nearly two decades since the first policy parameters for the new converging media and information environment were set out.[35] In 1996, the European Parliament and Council called on the Commission to examine in-depth some of the key public interest issues – protection of minors, protection of human dignity, information security, protection of personal information – and to respond with appropriate policies to strengthen trust, security and public confidence in new audiovisual and information services. The European Commission's response – the *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services* (1996)[36] and the communication on *Illegal and Harmful Content on the Internet* (1996)[37] – lay the foundation for much subsequent policy implementation. It led to the development of the Safer Internet Programme at European level, and a variety of initiatives at national level to combat the most serious forms of online abuse and to monitor safety standards for content and services that may be potentially harmful for minors.

The change in emphasis from a *safer* to a *better* internet for children and young people[38] marks a new phase in which embracing digital opportunities for all is regarded as vital for prosperity and growth, as well as a healthy, functioning democracy, while attending to the need to ensure better provision for quality of content and robust support for safety standards. A benchmarking of safer internet policies for the European Commission positions Ireland among a group of countries that have achieved a good balance of complementary measures for implementing internet safety between the public and private sector, with an effective legal and policy framework to promote better internet strategies.[39] However, as pointed out in the report of the Joint Oireachtas Committee, lack of coordination between the different agencies responsible for implementing internet safety policy, combined with low public awareness of what they actually do, highlights the need to review at a more fundamental level the national approach to governance of online content and internet safety. The completion of the current phase of the Safer Internet Programme at European level and the call by the European Commission for member states to do more to support safer and better internet use also adds new urgency to the task.

---

34 Braman, S. (2004). Where has media policy gone? Defining the field in the twenty-first century. *Communication Law and Policy, 9*(2), 153-182.

35 European Commission (1994). *Europe and the global information society: Recommendations to the European Council (The Bangemann Report).* Brussels. Retrieved from http://www.echo.lu/eudocs/en/bangemann.html

36 European Commission (1996). *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services COM(96) 483.* Brussels: European Commission.

37 European Commission (1996). *Illegal and Harmful Content on the Internet COM(96) 487.* Brussels: European Commission.

38 European Commission (2012). *Communication on The European Strategy for a Better Internet for Children COM(2012) 196.* Brussels: European Commission. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF

39 O'Neill, B. (2014). *Policy Influences and Country Clusters. A Comparative Analysis of Internet Safety Implementation* (No. D6.3). London, LSE: EU Kids Online.

1.6 Public consultation

In order to inform its work, the Internet Content Governance Advisory Group launched a public consultation in January 2014. Members of the public were invited to comment on the central questions addressed by the group's terms of reference. Notices of the consultation were placed in national newspapers and supported by a social media campaign on Twitter. Members of the group participated in a series of public meetings and gave media interviews. A web presence for the group was established on the Department's website at www.dcenr.ie, with details of its terms of reference and membership as well as an online submission page. The Twitter account @CAGroup14 was also used for dissemination, especially during the consultation period.

A total of 59 responses to the public consultation were received (see Appendix I for list of individuals and organisation who made submissions). The group was impressed by the number of submissions made in a personal capacity as well as the response from industry. Among industry contributions were submissions from Eircom, Facebook, Internet Service Providers' Association of Ireland, Three Ireland and UPC. A wide range of stakeholder organisations and groups also participated, and made detailed and helpful submissions. Participation of two key stakeholder groups was notable: the National Parents' Council, represented on the group by its CEO, coordinated a survey of its members as part as part of the consultation process. The Webwise Youth Advisory Panel also convened a special meeting to prepare a submission. Further youth participation was also assisted by the inclusion on the group of the President of the Irish Second-Level Students' Union (ISSU).

To facilitate further consultation within the time constraints of the period during which the group met, a number of bilateral meetings were held with relevant government departments, agencies and industry representatives. Meetings were held with officials in the OiS, the Law Reform Commission, DES, DCYA, the Department of Health (DoH), and the Office of the Ombudsman for Children (OCO). Meetings were also held with representatives of Facebook, Google, Twitter and Three Ireland. Many of these organisations also made formal submissions in response to the public consultation. Had the group more time, further meetings could have been scheduled. However, the group was satisfied that it had gathered sufficient information from all relevant stakeholders to inform its deliberations.

The issues that the Internet Content Governance Advisory Group had to consider are inherently challenging. They include questions of internet governance, freedom of expression, safety and child online protection, cyberbullying and harassment, and access to content that may be harmful or age-inappropriate. While the group could have continued to explore these issues for many more months, our priority in keeping to the assigned schedule was to bring forward proposals that could be implemented within a relatively short time-frame. Conscious that the internet is an environment that does not stand still and continues to evolve at a rapid pace, the group considered it important to outline proposals that would contribute to better governance and safety, while considering emerging trends and new policy developments. Aware also that there are currently a number of on going online safety initiatives within the field, the group was concerned to ensure that its proposals added value to existing arrangements and made the best use of current resources.

1.7 Structure of the report

The report is organised into three main sections. Following the Introduction:

- Chapter 2 examines the principal contours of the current legislative and regulatory framework for internet content governance and online safety in Ireland, and makes recommendations for more effective coordination in light of convergence in the internet and audiovisual arena.
- Chapter 3 deals with online communication and the use of social media, and assesses responses to cyberbullying from a legislative and regulatory point of view.
- Chapter 4 examines access to content by minors that may be considered unsuitable or age-inappropriate and makes recommendations on the policy options available to the State.
- The Conclusion summarises the group's recommendations to government and outlines themes for further consideration in the form of a roadmap for future policy development.

Chapter 2: Internet content governance: regulatory and legislative frameworks

"Mutually respectful dialogues between all stakeholders on the future development of global internet governance are essential given the global economic and societal importance of the internet."[40]

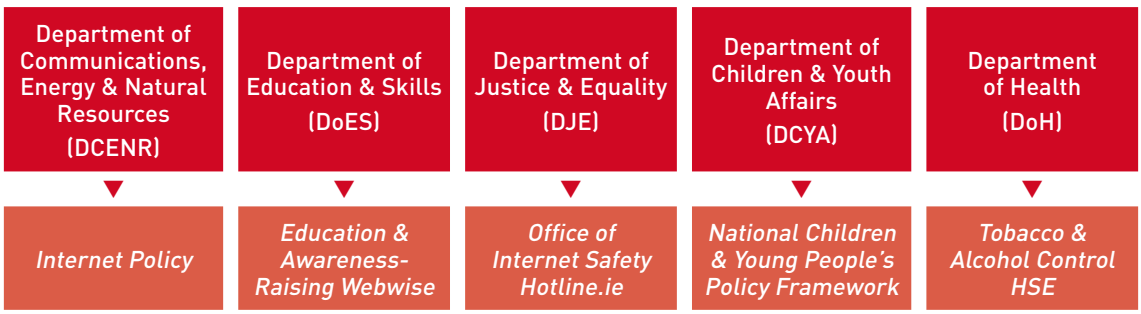
Consideration of issues relating to internet content governance and online safety in Ireland goes back to 1998 when the first Working Group on Illegal and Harmful Use of the Internet was established by the then Minister for Justice, Equality and Law Reform.[41] The report of the Working Group recommended a system of self-regulation by industry, incorporating a code of practice for internet service providers, a national hotline for the reporting of illegal content and an awareness programme to address concerns regarding illegal and harmful material online.

The Office for Internet Safety (OiS), based in the Department of Justice and Equality, and previously the Internet Advisory Board (IAB) (2000-2007), have been the principal vehicles for overseeing the regulatory system for internet safety in Ireland. However, activities relevant to internet content governance as well as online safety are also located in a number of government departments and agencies. The approach has been an evolutionary one, responding to issues as they arise, and consequently a variety of regulatory and legislative frameworks apply. With new developments in technology, this is an area that continues to expand. There is, therefore, a need to consider a more effective configuration of responsibilities and accountabilities. The following brief review presents an overview of existing arrangements for internet content governance and outlines recommendations for a reconfiguration of resources in this area.

2.1 Government departmental responsibilities

Currently, responsibility for internet safety falls primarily within the remit of the Department of Justice and Equality. However, the work of other government departments also has an important bearing on policy development and/or regulatory activity in this area. At least five areas stand out (Figure 1):

Figure 1: Government Departments with responsibility for aspects of internet safety



[40] Internet Policy and Governance: Europe's role in shaping the future of Internet Governance. (2014, February 12). European Commission. Retrieved from http://ec.europa.eu/digital-agenda/en/news/communication-internet-policy-and-governance

[41] 'Illegal and Harmful Use of the Internet'. First report, Working Group on Illegal and Harmful Use of the Internet. Department of Justice, Equality and Law Reform. Retrieved from http://www.internetsafety.ie/website/ois/oisweb.nsf/0/77B7FDAED19CE22F802574C5004E587D/$File/working%20group%20repor%20on%20illegal%20and%20harmful%20use%20of%20the%20internet.pdf

2.1.1 Department of Justice and Equality

The Department of Justice and Equality acts as host to the OiS. Evolving from the Internet Advisory Board (IAB), set up on the recommendation of the Working Group on Illegal and Harmful Use of the Internet (1998), the OiS was established in 2007. Its origins may also be traced to a period when there was a Minister of State for Children across a number of government departments (1994–2011). A minister who had previously held that post became Minister for Justice and obtained Government agreement to establish the Office for Internet Safety as an Executive Office in the Department of Justice.

The Office for Internet Safety (OiS) is described as taking 'a lead responsibility for internet safety in Ireland, particularly as it relates to children'.[42] Its primary emphasis is on combating online child abuse material. The OiS also engages in awareness-raising activities around the dangers for children on the internet and oversees the work of the Hotline.ie service, run by the Internet Service Providers Association of Ireland (ISPAI), to which reports are made about suspected illegal activity on the internet, in particular, child-abuse material.

In addition to the work of OiS, DJE has responsibility for civil and criminal law reform in areas that may have relevance for online safety. This includes provision for conduct that is illegal in and of itself offline, and therefore also illegal on the internet, such as fraud, harassment, child-abuse imagery, etc.

DJE is currently conducting a review of sexual offences legislation and is considering legislation for the transposition of Directive 2011/92/EU *on combating the sexual abuse and sexual exploitation of children and child pornography*.[43] Article 25 ('Measures against websites containing or disseminating child pornography') is dealt with in part by the current operation of the Hotline.ie service (the removal of websites under 'notice and takedown' procedures). The second part of the Article deals with blocking access to web pages containing or disseminating child pornography, which, it is proposed, will be dealt with by a new Garda initiative in cooperation with internet service providers in Ireland.[44] The group acknowledges that there may be a requirement for primary legislation giving effect to the Directive in its current form.[45]

2.1.2 Department of Communications, Energy and Natural Resources

DCENR deals with the internet and online activity from a number of perspectives, including internet security, telecommunications infrastructure, information society services and electronic communications services and broadband rollout. It also has a number of functions around broadcast and online media.

DCENR takes the lead responsibility for implementation in Ireland of the Digital Agenda, the EU's strategy to help digital technologies, including the internet, to deliver social and economic benefits for citizens.[46] Responsibility for telecommunications and broadcasting come within its remit. The Department manages the National Digital Strategy, encouraging use of the internet and use of digital technology. It has also set out a strategy to deliver high-speed broadband throughout Ireland through the National Broadband Plan.

---

42 http://www.Internetsafety.ie/

43 Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0093

44 Seanad Adjournment Debate, Progress being made in transposing Directive 2011/92/EU: Opening Remarks by Minister Kathleen Lynch on behalf of Alan Shatter TD, Minister for Justice, Equality and Defence. Retrieved from http://www.justice.ie/en/JELR/Pages/SP13000036

45 Demeyer, K., Lievens, E., & Dumortier, J. (2012). Blocking and Removing Illegal Child Sexual Content: Analysis from a Technical and Legal Perspective. Policy & Internet, 4(3-4), 1–23.

46 http://ec.europa.eu/digital-agenda/digital-agenda-europe

The Broadcasting and Media Divisions in the Department have responsibility for the policy and legislative framework to facilitate the provision of quality broadcasting services in Ireland, along with a number of other functions including aspects of internet and media governance. Media, at a global level, is widely understood to be in the advanced stages of a process termed convergence, whereby all extant media converge on a set of online services, either in parallel with or instead of their present means of communicating with an audience. The two divisions operating in this area, the Broadcasting Policy Division and the Cross-Media Division, are responsible for the ongoing development of broadcasting and media legislation, corporate governance of public service broadcasters, and a number of developing international policy issues at EU and Council of Europe level, and at bodies such as EuroDIG and the Internet Governance Foundation (IGF).

2.1.3 Department of Education and Skills

DES includes in its support services for the education sector a range of technology and internet services to schools. Content filtering is an integrated element of the Schools Broadband Programme. This is managed by the Professional Development Services for Teachers (PDST) team, working with DES and HEAnet.[47]

PDST is also a partner in the Safer Internet Ireland project (supported under the European Commission's Safer Internet Programme).[48] The Webwise Internet Safety Initiative of the PDST manage the awareness centre on behalf of the DES, and develop materials and programmes of awareness to ensure that children, teachers and parents understand the benefits and risks of the internet. Webwise and the Office for Internet Safety (OiS) are supported by the Webwise Youth Advisory Panel. Webwise also promotes Safer Internet Day in Ireland, the global awareness initiative to promote a safer internet for all users. DES has been supporting this initiative since 2004.

The DES has also been proactive in combating cyberbullying in schools. With the Department of Children and Youth Affairs, DES has developed the Action Plan on Bullying, delivering on a commitment in the Programme for Government to develop proposals to combat bullying in schools.[49] New anti-bullying procedures for primary and post-primary schools, which include cyberbullying and bullying via text messages, were published in September 2013. Awareness and prevention are key features of this policy that seek to build empathy, respect and resilience in pupils, and explicitly address the issues of cyber-bullying and identity-based bullying including, in particular, homophobic and transphobic bullying.

The National Educational Psychological Service (NEPS), also within the Department, has developed guidelines on social media use in responding to critical incidents in schools as part of its general guidance on mental health and well-being.[50]

The Department also oversees curriculum development and assessment through the National Council for Curriculum and Assessment (NCCA). It thus plays a central role in developing a curriculum that provides opportunities for digital literacy education and internet safety skill training through subjects such as Social, Personal and Health Education (SPHE).[51]

47 http://www.pdsttechnologyineducation.ie/en/Technology/Schools-Broadband/Content-Filtering/

48 http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids

49 http://www.education.ie/en/Publications/Education-Reports/Action-Plan-On-Bullying-2013.pdf

50 http://www.education.ie/en/Schools-Colleges/Services/Educational-Psychologist-NEPS-/Guidance-on-Social-Media-Use-and-Critical-Incidents-2014-.pdf

51 http://www.sphe.ie/

2.1.4 Department of Children and Youth Affairs

DCYA was established in 2011 to consolidate and coordinate policy and provision for children, young people and families. Responsibility for the Child and Family Agency and the Office of the Ombudsman for Children are included in its remit. Prior to 2007, responsibility for internet safety rested with the Minister of State for Children. The Department funds *Growing Up in Ireland*, the national longitudinal study of children.[52] The Department's National Strategy for Research and Data on Children's Lives 2011–16[53] aims to develop research capacity and to ensure policy is guided by comprehensive and up-to-date data.

The National Policy Framework for Children and Young People, published in April 2014, is a new initiative that places DCYA in a coordinating role across all of Government in relation to children.[54] The framework contains general principles that inform the Department's work and recognise the centrality and importance of digital media in children's lives. The framework deals with both the safety and well-being of children and young people through supporting better outcomes for children.

Three commitments in the framework are of particular relevance to the current report:

> **[2.11]** 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). (p.135)
>
> **[3.9]** Continue to promote best practice among retailers, the media and the entertainment industry with a view to interrupting the sexualisation and commercialisation of childhood; and where appropriate to introduce legislation and/or regulation to control or restrict inappropriate practices. (p.137)
>
> **[3.19]** Continue 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. (p.138)

Responsibility for the above lies, respectively, with DES, DCYA and DCENR. Implementation will be delivered under the coordination of DCYA, using its consultative bodies and interdepartmental processes.

2.1.5 Department of Health

DoH has, in response to parliamentary questions, addressed issues related to websites that promote the 'virtues' of, for example, anorexia and bulimia and which seem to be targeted primarily at young girls. Such website content comes under the heading of harmful content but, as these websites are often based in the United States and are not deemed to be illegal under US law, it is understood that action that could be taken against them in Ireland is limited.

In material supplied by DoH, the Department has expressed concern about alcohol marketing using digital media. It has argued that, because of its harmful effects, alcohol advertising should be considered 'inappropriate online material' when viewed by children and young people, and that they should be protected from it as far as legally and practically possible. Increased and improved surveillance of alcohol industry activities in digital media is necessary, it argues, for protecting the health and well-being of the population in general.[55]

---

52 http://www.growingup.ie/

53 http://www.dcya.gov.ie/viewdoc.asp?fn=%2Fdocuments%2FResearch%2FResearchDataStrat.htm&mn=nats&nID=1

54 http://www.dcya.gov.ie/documents/cypp_framework/BetterOutcomesBetterFutureReport.pdf

55 Material supplied by the Department of Health, Tobacco and Alcohol Control Unit.

2.2 Regulatory agencies and other public bodies

Aspects of regulatory responsibility for internet content – or activity that may be construed as having some relevance to the subject – are also to be found within the remit of a number of other, both state and non-state bodies. The following is not an exhaustive list and highlights only the more prominent examples (Figure 2).

Figure 2: Regulatory agencies/public bodies with an interest in content governance

2.2.1 Internet Safety Advisory Committee

The Internet Safety Advisory Committee (ISAC) is a forum established under the auspices of the Department of Justice and Equality. It comprises an independent chairperson, representation from industry, An Garda Síochána, child protection interests, relevant government departments and the Office of the Data Protection Commission as well as legal expertise. It acts rather as a stakeholder forum to advise the OiS and DJE. ISAC is modelled on its predecessor, the Internet Advisory Board (IAB), established in 2000 on the recommendation of the Working Group on Harmful and Illegal Use of the Internet. It acts as the national stakeholder forum for the purposes of the requirements of the EU-funded Safer Internet Ireland project.[56] During the operation of the IAB, the stakeholder forum undertook a wider range of functions.[57] In addition to monitoring the effectiveness of the industry's self-regulatory mechanisms and the workings of Hotline.ie, the IAB assumed responsibility for awareness-raising and fostering international links in the area of internet safety. The IAB also commissioned some of the first research studies of internet use by children in Ireland.[58] [59]

2.2.2 Broadcasting Authority of Ireland

The Broadcasting Authority of Ireland (BAI), established under the Broadcasting Act 2009, is the body responsible for regulating content across all broadcasting networks in Ireland. The definition of broadcasting services excludes 'audio or audiovisual services provided by way of the internet' (Pr.1, S.2). The latter services are included, however, in the definition of 'electronic communications network' and among the duties of public service broadcasting is the provision of broadcasting services over the internet (RTÉ s.114(4) (r).[60]

The BAI also has the ancillary function to promote media literacy, understood as bringing about a better public understanding of content published by broadcast and 'other electronic means' (Pr.1, S.2). This function includes undertaking, encouraging and fostering research and activities directed towards the promotion of media literacy, including the provision of support under the Broadcasting Funding Scheme.

---

56 ISAC, Office for Internet Safety, About Us (2008). Retrieved from http://www.Internetsafety.ie/website/ois/oisweb.nsf/page/aboutus-isac-en

57 Office for Internet Safety, Internet Advisory Board, Report 2000–2002. Retrieved from http://www.Internetsafety.ie/website/ois/oisweb.nsf/0/4FCD5CCF592A6BE4802574C5004DD850/$File/IAB%2000-02%20report.pdf

58 Amárach Consulting. (2001). *Research of Internet Downside Issues.* Dublin: Internet Advisory Board. Retrieved from http://www.internetsafety.ie/website/ois/oisweb.nsf/0/F970D473024C7B2E802574C5004DFB69/$File/am%C3%A1rach%20con.%20research%20of%20internet%20downside%20issues%20Aug%2001.pdf

59 Amárach Consulting. (2004). *The Use of New Media by Children.* Dublin: Internet Advisory Board. Retrieved from http://www.internetsafety.ie/website/ois/oisweb.nsf/0/57019ADDBBA5856F802574C5004E2882/$File/am%C3%A1rach%20con.%20the%20use%20of%20new%20media%20by%20children.pdf

60 McGonagle, M., & Brody, A. (2013). Ireland. In Sousa, H., Trützschler, W., Fidalgo, J. & Lameiras, M. (Ed.), *Media Regulators in Europe: A Cross-Country Comparative Analysis* (pp. 81–99). Braga, Portugal: CECS, University of Minho, p. 85.

2.2.3 Commission for Communications Regulation

The Commission for Communications Regulation, also known as ComReg, is the statutory body responsible for the regulation of the electronic communications sector (telecommunications, radio communications, and broadcasting transmissions) and the postal sector. It is the independent national regulatory authority for these sectors in accordance with EU law and comes under the remit of DCENR.[61] Among the objectives of ComReg set out in the Communications Regulation Act 2002 (Pr.2, S.12) is encouraging access to the internet at reasonable cost to consumers.

ComReg does not have responsibility for content as such. However, as of 2010, it is responsible for the regulation of Premium Rate Services (PRS), defined as the provision of content (other than broadcasting) through an electronic communications network, typically through a telephone number or short code and charged at a premium rate. PRS providers must be licensed and operate through a code of practice which defines standards of legality, decency and data protection as well as setting out specific provisions for individual categories of services including entertainment, competition, sexual entertainment services, chatline/dating services, and services targeted at children.[62]

2.2.4 Office of the Data Protection Commissioner

The Office of the Data Protection Commissioner (ODPC), established under the 1988 Data Protection Act, is responsible for upholding the rights of individuals under data-protection legislation and enforcing obligations under data controllers. The role of the ODPC takes on added importance with the location in Ireland of leading global internet companies. Under current European legislation, privacy complaints from across the EU about services of companies such as Google and Facebook are processed under Irish data-protection law. To date, the ODPC has undertaken two audits of Facebook International's compliance under EU data-protection provisions.

The ODPC also has a role in awareness-raising for both individuals and companies regarding data-protection rights and privacy issues. Research conducted by the office indicates a low level of knowledge (and concern) among teenagers about online privacy. Accordingly, the ODPC has developed educational resources for the Junior Certificate CSPE (Civic, Social and Political Education) programme and has developed educational material for parents in conjunction with the OiS.[63]

2.2.5 Irish Film Classification Office

The Irish Film Classification (IFCO) does not have any remit for internet content, as such. However, this long-established body with vast expertise in providing content classification guidance is a potential resource in addressing related issues of online content. The role of the IFCO was first established under the Censorship of Films Act 1923 and expanded under the Video Recordings Act 1989. Its function is to provide parents with a reliable system of classification that protects children and young people from exposure to age-inappropriate content, has regard for freedom of expression and reflects the prevailing social values of the day.[64] The IFCO had a role in the development of the Internet Advisory Board; the Deputy Film Censor acted as chairperson of the IAB until 2006. In other jurisdictions, notably the British Board of Film Classification (BBFC) in the United Kingdom and the equivalent classification body NICAM in the Netherlands, film classification has been used as a basis for development of classification schemes for video game and online

[61] http://www.comreg.ie/about_us/roles_what_we_do.523.html

[62] Code of Practice for Premium Rate Services: https://www.comreg.ie/_fileupload/File/ComReg1229.pdf

[63] https://www.dataprotection.ie/ViewDoc.asp?fn=%2Fdocuments%2Fteens%2Fdefault%2Ehtm&CatID=88&m=t

[64] http://ifco.ie/

content. The IFCO also regularly conducts research into parental attitudes and concerns regarding age-related classification and is regarded as a trusted resource by parents and members of the public.[65] It has recently partnered with the equivalent film classification bodies in the UK and Netherlands, mentioned above, in developing rating systems for user-generated online content.[66]

2.3 Industry self-regulation

Self-regulation, whereby industry takes responsibility to regulate on behalf of government against internet abuses, was established on the recommendation of the 1998 Report of the Working Group on Illegal and Harmful Use of the Internet.[67] This comprised in the main a system of self-regulation of the internet service-provider industry to include a common code of practice and common acceptable use policies. It also recommended the establishment of a complaints hotline to investigate and process complaints about potentially illegal material on the internet. The trade association, the Internet Service Providers Association of Ireland, and the Hotline.ie service, therefore, act as the principal framework for managing harmful and illegal online content. Self-regulation also features in other areas of the media industry to which issues of internet content apply. These self-regulatory bodies are briefly reviewed below (Figure 3).

Figure 3: Self-regulatory bodies with relevance to internet content

2.3.1 Internet Service Providers Association of Ireland (ISPAI)

ISPAI, established in 1997 as the representative association of Irish ISPs, coordinated the industry's implementation of the recommendations of the Working Group on Illegal and Harmful Use of the Internet.[68] It developed the ISP Code of Practice and Ethics, and coordinates the resulting self-regulatory regime on behalf of the industry.

The Code of Practice and Ethics, adopted by the ISPAI in 2002, requires that ISP services and promotional materials must not:

> ...enclose content which is illegal, misleading, likely to incite violence or cruelty, racial hatred, prejudice, discrimination even if not illegal, is considered inappropriate or calculated to cause distress, anxiety, inconvenience to others.[69]

Furthermore, ISPs are required to adopt acceptable use policies (AUPs) that prohibit customers using ISPs services to:

> ...create, host, transmit material which is unlawful/libellous/abusive/offensive/vulgar/obscene/calculated to cause unreasonable offence. (Section 5.1.1)

---

65 IFCO. (2013). *Film Classification Survey – Parental Attitudes 2013.* Dublin: Irish Film Classification Office. Retrieved from http://www.ifco.ie/ifco/ifcoweb.nsf/lookupreports2/54C63DC5C04626FE80257BDE004DF327/$File/Film%20Classification%20Survey%20-%20Parental%20Attitudes%202013.pdf?openelement

66 Report presented to the CEO Coalition, 24 January, 2014 http://www.yourateit.eu/

67 Office for Internet Safety, 'Illegal and Harmful Use of the Internet' (2009). Retrieved from http://www.Internetsafety.ie/website/ois/oisweb.nsf/0/77B7FDAED19CE22F802574C5004E587D/$File/working%20group%20repor%20on%20illegal%20and%20harmful%20use%20of%20the%20Internet.pdf

68 ISPAI, 'About ISPAI'. Retrieved from http://www.ispai.ie/?page_id=9

69 ISPAI, 'Code of Practice'. Retrieved from http://www.ispai.ie/?page_id=11

AUPs must also include clauses to deal with third-party content that, while not necessarily illegal, may be 'considered inappropriate and deliberately calculated to cause unreasonable offence to others' (Section 5.1.2). ISPs also undertake to provide information about filtering software tools for content that users may deem unsuitable and to provide a link to the Hotline (see below) to report potentially illegal content. The Code of Practice also includes provision for a Complaints Procedure to deal with breaches of the Code by members of ISPAI.

2.3.2 Hotline.ie

Hotline.ie (the 'Hotline') was established in 1999 on the recommendation of the Working Group on Illegal and Harmful Use of the Internet.[70] It is operated by ISPAI and co-funded with support from the European Commission's Safer Internet Programme. The aim of the Hotline is to provide a secure and confidential service for members of the public to report anonymously content they may come across online and believe to be illegal. The Hotline forms a core part of the self-regulatory system in Ireland. Hotline.ie is a member of INHOPE, the international organisation of internet hotlines. It reports to the OiS, based in the Department of Justice and Equality.

The main focus of the Hotline is content that may be illegal under the Irish Child Trafficking and Pornography Act 1998, which makes it illegal for anyone to knowingly possess child pornography or to knowingly print, publish, import, export, manufacture or distribute child pornography. Other content that may be illegal and which can be reported using the Hotline includes racism, xenophobia or incitement to hatred; under the Irish Prohibition of Incitement to Hatred Act 1989, it is an offence for any person to distribute, publish, behave, display written material, words, behaviour, visual images or sounds if they are threatening, abusive or insulting and are intended or are likely to stir up hatred.

Material reported to the Hotline is assessed in the first instance by staff of the service and, if determined to be potentially illegal under relevant legislation, steps are taken to have it removed and duly notified to the relevant authorities. If the reported material is traced to a server located in Ireland, An Garda Síochána is notified and a 'take down' notice is issued to the ISP. If the material is traced to another country, details are forwarded to the relevant national hotline, if a member of INHOPE, and details provided to An Garda Síochána for transmission to the source country through international law-enforcement channels.

The Hotline also seeks to raise awareness of internet safety and security. It participates as a member in the Safer Internet Ireland project and provides general information about online safety, including filtering software.[71]

2.3.3 On-Demand Audiovisual Services (ODAS) Group

The Audiovisual Media Services Directive (AVMSD) (2010/13/EU) requires Member States to ensure that 'on-demand audiovisual media services receive similar treatment to television broadcasts when it comes to a range of human rights and intellectual property rights questions (Chapter III of the Directive), and also places a set of specific requirements on Member States around the operation of on-demand services (in Chapter IV). Member States have a significant degree of latitude in how they meet these requirements; in Ireland, the Directive was transposed by S.I. No. 258 of 2010 and S.I. No. 247 of 2012, with these requirements being met by way of a co-regulatory system. As such, on-demand audiovisual services made available within the jurisdiction of the Republic of Ireland, are covered by a self-regulatory framework called the On-Demand Audiovisual Services

[70] Hotline.ie, Irish Internet Hotline (2002). Retrieved from http://www.hotline.ie/

[71] http://www.hotline.ie/filteringsoftware.php

(ODAS) system. ODAS is a collaboration between IBEC's Audiovisual Federation (AF) and Telecommunications and Internet Federation (TIF), the BAI and the Advertising Standards Authority for Ireland (ASAI)[72]. Importantly, these on-demand services are not regulated by the BAI as such, but rather the regulator acts as a statutory backstop in cases where the initial complaint is not addressed to the satisfaction of the complainant. The BAI is responsible for approving the Code of Conduct, however.[73] Other jurisdictions, such as the UK, have taken a different approach and established a formal agency, the Authority for Television On Demand (ATVOD) to deal with these on-demand services.[74] ATVOD also works with the UK Council for Child Internet Safety in relation to online age verification and parental controls for connected TVs.

On-demand services now encompass a growing body of audiovisual content and television-like services, even if the number of providers originating within Irish jurisdiction remains low. It includes on-demand and catch-up television services for web and mobile platform delivery. Included within the definition of on-demand services is the feature that it is under the editorial control/responsibility of a service provider. As such, it does not include so-called user-generated content on media sharing platforms where editorial control lies with content creators.

2.3.4 Press Council of Ireland

The Press Council of Ireland was established in 2008 as a self-regulatory body, which, in conjunction with the Press Ombudsman, is designed to regulate the press according to an agreed set of ethical standards and principles and to handle complaints against print media. The Press Council and the Press Ombudsman are recognised under the Defamation Act 2009, which contains provisions about the council's composition and conduct, and the general scope of its code of practice.

The remit of the Press Council and Press Ombudsman primarily covers print-based media rather than its broadcast or online counterparts. However, with the rise of new forms of journalism and diverse news media outlets as well as major shifts in how people consume news, it is likely that press regulation will need to adapt further to changes underway in the media marketplace.[75] Currently, Journal.ie is the only online news platform covered by the Press Council. RTÉ's websites, as the online platforms of other broadcast outlets, are not subject to any regulatory regime.

2.3.5 Irish Cellular Industry Association

Mobile network operators in Ireland, licensed by ComReg, also operate a voluntary self-regulatory code of practice, coordinated by the mobile industry alliance, the Irish Cellular Industry Association (ICIA), comprising the mobile operators Meteor Mobile Communications, O2, Three and Vodafone.[76] The ICIA Code of Practice dates from 2006; a revised version is due to be launched later this year. Mobile network operators in Ireland are signatories of the European Framework for Safer Mobile Use by Younger Teenagers and Children (GSMA, 2007)[77]. Commitments of the Framework include an obligation to ensure that, where a service contains content that may be unsuitable for minors, the provider must provide suitable tools or controls to restrict its access, in relation to both

72 http://www.bai.ie/?page_id=2082

73 ODAS Code of Conduct. Retrieved from http://www.bai.ie/?page_id=2082

74 http://www.atvod.co.uk/

75 Foley, M. 'Holding Journalism to Account'. *Irish Times*, April 25, 2014. Retrieved from http://www.irishtimes.com/news/crime-and-law/holding-journalism-to-account-1.1773001?page=2

76 Irish Cellular Industry Association: http://www.ibec.ie/IBEC/BA.nsf/vPages/Business_Sectors~Telecommunications_and_Internet_Federation~irish-cellular-industry-association?OpenDocument

77 http://www.gsma.com/gsmaeurope/safer-mobile-use/european-framework/

a company's own-brand content and third-party commercial content. Mobile network operators also undertake to support appropriate classification of content for own and third-party content, using recognisable national schemes, where available, while supporting pan-European developments such as the PEGI labelling scheme for games and online content. The ICIA Code of Practice (2006) gave a commitment to establish an Independent Classification Body to implement a classification framework for content offered over mobile phones. Such a body, the code states, would provide a framework for classifying commercial content that is unsuitable for customers under the age of 18.[78] However, this has not yet been achieved and is one area where Ireland has been found not to be compliant with the European Framework.[79]

Three Ireland, in its submission to the group, notes this as a gap and recommends that a body such as ComReg or the BAI develop such a content classification and age rating system to which all access media for commercial content should adhere.[80]

2.3.6 .IE Domain Registry

The .ie Domain Registry (IEDR) is an independent private company, which since 1991 has managed the .ie country code Top Level Domain (ccTLD) namespace. Powers of regulation over the .ie namespace are vested with the Minister for Communications, Energy and Natural Resources while IEDR, in keeping with international practice, acts independently as a public service in the allocation of identifiably Irish domain names on the internet. All .ie domain registrations must adhere to specific naming and registration policies, included in which is the provision that a domain name 'must not be offensive or contrary to public policy or generally accepted principles of morality' (para 3.4).[81] While such a provision may be in the interests of preserving the reputational value of the .ie domain, it is relatively unusual in an international context. A recent review of .uk Registration Policy, for instance, recommended that Nominet, the equivalent domain registry body in the UK, as a private body should have no role in policing questions of taste or offensiveness on the internet.[82]

2.4 Recommendations

In reviewing the governmental arrangements in place contributing to implementation of safer internet policies, the group formed the view that there were many positive elements and examples of good practice in internet safety provision. The number of government departments and agencies with an interest in this area is extensive. A range of governance arrangements are in place in the private sector also, many of which have evolved to take account of increasing digitalisation and respond to particular issues. It is clear that there is a high degree of policy attention to encouraging users to gain the benefits of online opportunities, while also addressing public concerns over online abuses and potentially harmful content.

Effective strategies for internet safety, as recommended by the OECD, require a careful balance of public and private, legal and voluntary measures at various levels, based on shared responsibility between stakeholders, balancing the risks and opportunities afforded

78 ICIA. 'The Irish Mobile Operators Code of Practice for the Responsible and Secure Use of Mobile Services' 2006. Retrieved from http://www.ibec.ie/IBEC/BA.nsf/vPages/Business_Sectors~Telecommunications_and_Internet_Federation~icia-code-of-practice-04-05-2006?OpenDocument

79 PricewaterhouseCoopers (2009). 'European Framework for Safer Mobile Use by Younger Teenagers and Children – Implementation Report.' Retrieved from http://www.gsmeurope.org/documents/PwC_Implementation_Report.pdf

80 Submission from Three Ireland.

81 IEDR Naming Policy. Retrieved from https://www.iedr.ie/p30/naming-policy/

82 Lord Macdonald QC. *Review of .uk Registration Policy.* nominet, 2013. Retrieved from http://www.nominet.org.uk/how-participate/policy-development/current-policy-discussions-and-consultations/review-domain, p.2

by the internet and ensuring coherence and consistency at the policy level.[83] In our view, this balance is often achieved and is based on good cooperation between the various stakeholders involved.

However, the provision in this area is also somewhat fragmented, leading to a somewhat sub-optimal use of resources. What is lacking is an overarching strategic and policy framework to inform and coordinate the diverse elements of this evolving environment. Such fragmentation is not unusual given the speed at which the internet – and related safety concerns – have evolved in recent years. The European Commission, in its benchmarking of internet safety policies across member states, identified similar patterns in many other countries and, consequently, a diverse range of solutions to coordination of policy at the national level.

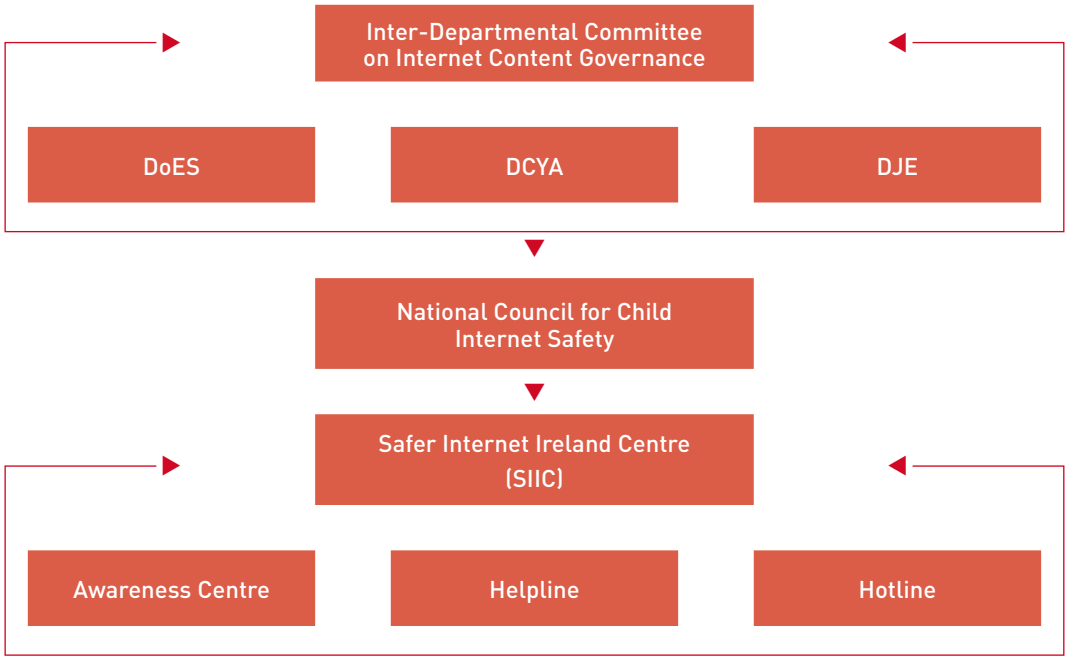
Our objectives in bringing forward recommendations relating to governance arrangements are to enhance capacity in an expanding field, while not disrupting what is currently proving to be effective or creating unrealistic expectations about what may be feasible.

We identify three main levels required for an effective regulatory and governance framework:

- A policy coordination function
- A framework for multi-stakeholder involvement
- A platform for implementation/delivery of internet safety

We believe that each of these elements exists within current arrangements though they may not be currently optimally deployed. Therefore, we recommend a reconfiguration of responsibilities as follows (Figure 4), with specific recommendations regarding the roles, responsibilities and reporting accountabilities for each of the actors involved.

Figure 4: Organisation chart



[83] OECD (2011). The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. Retrieved from http://dx.doi.org/10.1787/5kgcjf71pl28-en

2.4.1 Formal assignment of policy responsibility for internet content governance

We recommend that DCENR be formally charged with coordinating internet content policy at government level. This Department already implicitly covers some aspects of this role, and it is where primary expertise in relation to general internet governance issues reside.

Given the diverse nature of the issues involved, the Department will need to liaise with other relevant government departments to take account of issues relating to education, child protection, law enforcement etc. As such, a standing inter-Departmental Committee should be formed with representation from all Departments involved in related areas, meeting on a quarterly basis to cover all aspects of internet content governance. We do not recommend that the unit should replace the involvement of other government departments; rather, it should complement and add value by providing a holistic overview of an expanding and fast-moving field.

The Department should have assigned resources and expertise to take a policy lead on behalf of government on emerging issues for cross-media convergence, internet governance, content regulation and policy formation at the European and international level.

We accept that the development of any national strategy on converged media will have to wait until the completion of a revision of AVMSD. However, this does not preclude the development of an outline policy framework on these issues, building on the current National Digital Strategy (Phase 1) dealing with digital engagement. We recommend that such a policy framework be brought forward within 12 months and be published for public consultation. This framework document should set out national policy priorities for online and converged media, including the full range of providers of such services (including for example premium rate services as currently provided for under the regulatory regime managed by ComReg).

Protection of minors and due regard for the safety standards that should exist within the communications environment will be one major consideration in the formation of such a strategy. There are, however, other substantial issues to be considered, including the appropriate structure of media regulation more generally, the advantages of adopting a fully converged regulatory model for all of telecommunications, broadcasting and online audiovisual content; issues of media pluralism and diversity; as well as placing the various self-regulatory arrangements of audiovisual and commercial content on a statutory footing.

2.4.2 A revised role for the Office for Internet Safety

The primary role of the OiS in overseeing the operation of the self-regulatory system for combatting online child sexual abuse is an extremely important one. As it deals with questions of law enforcement and illegality, its location within the Department of Justice and Equality is entirely appropriate and helps to secure the robustness of Ireland's internet safety provision.

We recommend that consideration should be given to changing its title as appropriate to its administrative function and responsibilities for illegality on the internet. In order to provide clarification of its role, the Department of Justice and Equality should assign clear terms of reference, identifying its function in monitoring and supervising the system of industry self-regulation.

The full transposition of Directive 2011/92/EU will aid the OiS in discharging its function. We anticipate that Article 25 dealing with blocking access to web pages containing or disseminating child abuse material may require additional primary legislation to give effect to the Directive in its current form.

2.4.3 The National Council for Child Internet Safety

We recommend the establishment of a National Council for Child Internet Safety to act as the primary multi-stakeholder forum for internet safety strategy in Ireland. We believe the Department of Children and Youth Affairs is the most appropriate location for such a council and will facilitate the coordination and support for those elements of the National Policy Framework for Children and Young People dealing with the role of digital media in children and young people's lives. In order to give effect to the new council, the existing Internet Safety Advisory Committee should be expanded and reconfigured for this purpose. The representation of the council should include representation from industry, relevant government departments, public bodies, civil society including youth representation and child protection interests. The participation of leading internet companies located in Ireland on the council should also be encouraged.

As with the equivalent UK Council for Child Internet Safety (UKCCIS) – for which the OiS provided an early model – NCCIS should be chaired at ministerial, or junior ministerial level, to ensure that its work receives the appropriate level of political support. We envisage the council and the Department of Children and Youth Affairs as the coordinator of the Safer Internet Ireland project (awareness-raising, education and helpline functions) with appropriate administrative support supplied by the Department.

The council's membership, reflecting industry, civil society, academia and government, may wish form to working groups, to deal separately with issues of research, education and industry safety implementation, thereby guiding the council's work with the most up-to-date information available, and informed by international best practice. The council, in conjunction with the Safer Internet Ireland project, should also seek to harness innovative technology, tools and educational approaches in promoting internet safety and standards of digital citizenship, advising all relevant stakeholder groups with regard to emerging risks and good practices in internet safety.

2.4.4 The Safer Internet Ireland Centre (SIIC)

The Safer Internet Ireland project currently plays a crucial role in the delivery of internet safety. Through its combination of helplines, awareness node and hotline services, it provides essential support for education, awareness-raising and support. We believe this role should be expanded and better integrated to act as the Safer Internet Ireland Centre (SIIC). This should act as a single portal and resource for internet safety delivery. The Safer Internet Ireland project is currently co-financed by the European Commission and may continue to receive funding under the Connecting Europe Facility (CEF). However, it is important that government ensures that this vital public service is fully resourced.

In order to ensure better integration, the SIIC should operate through a common online platform and brand, and offer a helpline, educational resource and awareness-raising function for children and young people, for teachers and educators, and for parents. It should act as a one-stop portal designed to address the likely volume of enquires, aggregating available support content and serve as a directory/information resource for the general public. It should seek to compile resources of best practices in dealing with online abuse and harassment for parents, teachers and young people; plan awareness campaigns dealing with cyberbullying and online abuse; provide guidance to schools on incorporating in their anti-bullying policies best practice in relation to social media and online communication; and raise awareness of privacy issues in the sharing of content online.

Chapter 3: Online abuse, cyberbullying and harassment

Bullying and harassment is not something that began with the internet. However, internet technologies have added a new dimension to a complex and challenging societal problem. Cyberbullying is an umbrella term given to a variety of forms of bullying and harassment that take place in the virtual realm. Its effects can be devastating, as several high-profile cases attest. Because of its persistent nature, it may be far more harmful than its offline equivalent. Social media can facilitate the circulation of inappropriate or threatening messages, offensive videos or photos, often anonymously, meaning that bullying can be persistent, silent and seen by a potentially unlimited audience. As a result, the perception that users, especially young people, can be bullied online with impunity has given rise to widespread public concern.

In 2012, the Office of the Ombudsman for Children published a consultation on the problem of bullying in schools.[84] Following a commitment in the Programme for Government, the Department of Education and Skills, with the Department of Children and Youth Affairs, established an Anti-Bullying Working Group to explore what could be done to tackle bullying, especially homophobic bullying. The report of the working group, the 'Action Plan on Bullying', outlines measures to encourage schools to develop comprehensive new anti-bullying procedures.[85]

The report of the Joint Oireachtas Committee on Transport and Communications devotes substantial attention to the problem and makes a number of recommendations to tackle bullying.[86] The Sixth Report of Dr Geoffrey Shannon, the Special Rapporteur on Child Protection (2012), also addresses bullying in the context of social networking and cyberbullying.[87] The Law Reform Commission has, following an undertaking by the Minister for Justice and Equality to examine legislation in the area, initiated a review of legislation under the heading of 'Crime affecting personal safety, privacy and reputation including cyberbullying'.[88]

Terms of reference for the Internet Content Governance Advisory Group require it to address risks of bullying and harassment online, particularly with regard to children, and to assess whether existing national regulatory and legislative frameworks as well as policy responses are sufficient in dealing with the issue. Without wishing to duplicate or unnecessarily overlap with efforts undertaken elsewhere, the focus of this section of the report is to assess governance arrangements in place from an internet safety perspective, and to advise on legislative and policy responses to an emerging and complex problem.

84 Office of the Ombudsman for Children (2012). *Dealing with Bullying in Schools: A consultation with children & young people.* Dublin: Office of the Ombudsman for Children.

85 Anti-Bullying Working Group (2013). Action Plan on Bullying. Dublin: Dept. of Education and Skills.

86 Joint Committee on Transport and Communications (2013). *Addressing the Growth of Social Media and Tackling Cyberbullying.* Dublin: Houses of the Oireachtas.

87 Shannon, Dr Geoffrey (2013). *Sixth Report of the Special Rapporteur on Child Protection.* Dublin: Department of Children and Youth Affairs.

88 Development of Fourth Programme of Law Reform. Retrieved from http://www.lawreform.ie/welcome/7-development-of-fourth-programme-of-law-reform.384.html

3.1 Scope of potential harm

3.1.1 Cyberbullying and Harassment

Bullying has been defined as 'as repeated aggression – whether it be verbal, psychological or physical – that is conducted by an individual or group against others'.[89] The research literature identifies bullying as an aggressive act incorporating three main characteristics: the act is intentional; it involves a power imbalance between aggressor and victim, and it is repetitive in nature and repeats over time.[90] This has been adapted to the online domain as constituting 'wilful and repeated harm inflicted through the use of computers, cell phones and other electronic devices'.[91]

In the DES Anti-Bullying Procedures for Primary and Post-Primary Schools,[92] bullying is defined as 'unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time'. These procedures make clear that this definition includes cyber-bullying and identity-based bullying (such as homophobic bullying and racist bullying). Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or other private messaging, do not fall within the definition of bullying and are dealt with, as appropriate, in accordance with the school's code of behaviour. However, in the context of this policy, placing a once-off offensive or hurtful public message, image or statement on a social network site or other public forum 'where that message, image or statement can be viewed and/or repeated by other people' is identified as constituting bullying behaviour.

Considered by some to be a continuation of its offline equivalent, the effects of cyberbullying are thought to be especially pernicious since it is not confined to a single location, and leaves the victim with no respite as it invades the private space of the home. Because of always-on connectivity, cyberbullying can happen at any time. An increasingly privatised internet experience, brought about by the use of mobile devices, means that online bullying may also be hidden from parents and guardians. Perpetrators, in many circumstances, can also remain largely anonymous or pseudonymous.

Harassment, by contrast, is often identified as referring to a wider group of offensive behaviours or unwanted conduct based on discrimination or malice.[93] Cyberbullying is a subset of harassment, frequently understood to have a youth dimension, and refers to acts of aggression between youths in an online setting, while harassment more usually refers to offensive behaviours and unwanted contact relating to adults.

We appreciate that there is a continuum between offline and online behaviours and that this contributes to the complexity of developing effective responses and remedies. However, the focus of the Internet Content Governance Advisory Group is on the technology-mediated forms of aggression and abuse. In taking into account the very wide range of potential online abuses, the group concentrated its discussion on forms of cyberbullying and harassment such as:

---

89 DCYA (2011). *Children First: National Guidance for the Protection and Welfare of Children.* Dublin: Department of Children and Youth Affairs, p.61.

90 Levy, N., Cortesi, S., Gasser, U., Crowley, E., Beaton, M., Casey, J. & Nolan, C. (2012). *Bullying in a Networked Era: A Literature Review.* Berkman Centre for Internet and Society, p.8.

91 Hinduja, Sameer & Justin W. Patchin (2009). *Bullying beyond the Schoolyard: Preventing and Responding to Cyberbullying.* London: Corwin Press, p.5.

92 DES. (2013). *Anti-Bullying Procedures for Primary And Post-Primary Schools.* Dublin: Department of Education and Skills. Retrieved from http://www.education.ie/en/Publications/Policy-Reports/Anti-Bullying-Procedures-for-Primary-and-Post-Primary-Schools.pdf

93 Employment Equality Act 1998.

- Hurtful or harmful messages sent by email, mobile phones, instant messaging (IM), social networking websites, apps, and other online technologies
- Harmful or offensive pages set up on social networking sites or on websites, containing content intended to cause hurt and offence to individuals
- Offensive or inflammatory comments, often posted anonymously, on public websites or online communities for the purpose of causing upset and harm
- Misuse of personal data, e.g. through posting images or videos without consent, with the intention of causing embarrassment or hurt or stealing another person's online identity in order to cause reputational damage

3.1.2 Incidence of cyberbullying

Research acknowledges that cyberbullying rarely occurs in isolation and that it is more likely to be part of a pattern of repeated abuse or harassment that continues from the schoolyard or workplace to online communication platforms. Estimates of its prevalence vary. Overall, one in five 9-16 year-olds report being bullied either online or offline in the past 12 months, according to EU Kids Online, with 6% saying the bullying happened on the internet.[94]

There is some evidence to suggest that incidence of cyberbullying is on the rise. For instance, a 2012 survey of Irish secondary schools found that 18% of 12-16 year-olds (15.7% boys and 23.6% girls) reported some involvement in cyberbullying, either as victim or bully.[95] In its submission to the public consultation, the National Association of Principals and Deputy Principals reported findings that 16% of second-level students had been bullied in the past 12 months, up from 12% in the previous year.[96] This rising trend is explained, in part, by increased internet use: the more time young people spend online across multiple devices, the more likely they are to encounter cyberbullying.[97] The proliferation of mobile connected devices also plays a part: the European Commission's Net Children Go Mobile project found that, among younger teenagers (13-14 year-olds) in Ireland, bullying on social media platforms had overtaken that of face-to-face bullying.[98]

3.1.3 Impact of cyberbullying

Research evidence points to the fact that the impact of cyberbullying is the most severe of online risks. While many risks go relatively unnoticed or are not treated as a major concern for young people, this is rarely the case with cyberbullying. The OCO, in its 2012 consultation, found that bullying and related problems of stereotyping and stigma, as well as identity-based bullying, were matters of significant concern to children.[99] EU Kids Online has also reported on the striking impact of online bullying; over half of all victims say they were fairly or very upset by the experience. Younger children, girls and low socio-economic status groups were found to be the most severely affected.[100]

---

94 Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. (2011). *Risks and safety on the Internet: The perspective of European children. Full Findings.* London, LSE: EU Kids Online, p.63.

95 O'Moore, M. (2012). Cyber-bullying: the situation in Ireland. *Pastoral Care in Education, 30*(3), 209-223, p.213.

96 NAPD National Survey on Cyberbullying, 2014. Submission from the National Association of Principals and Deputy Principals.

97 Görzig, A. & Frumkin, L. (2013). Cyberbullying experiences on-the-go: How social media can become distressing. *Cyberpsychology*, 7(1). Retrieved from http://www.cyberpsychology.eu/view.php?cisloclanku=2013022801

98 O'Neill, B. & Dinh, T. (2014). *Net Children Go Mobile: Initial findings from Ireland.* Dublin: Dublin Institute of Technology, Centre for Social and Educational Research. Retrieved from http://www.netchildrengomobile.eu/reports/

99 Office of the Ombudsman for Children (2012). Dealing with Bullying in Schools: A consultation with children & young people. Dublin: Office of the Ombudsman for Children.

100 O'Neill, B. & Dinh, T. (2013). *Cyberbullying among 9-16 year olds in Ireland.* Dublin: Dublin Institute of Technology, p.7.

3.1.4 Anonymity and cyberbullying

Anonymity is sometimes identified as a factor in contributing to the particularly harmful nature of cyberbullying. Online anonymity is, as such, a double-edged phenomenon. It is, at once, a cornerstone of the fundamental right to free speech, celebrated for the role it has played in mobilising against political oppression, as, for example, in the so-called Arab Spring.[101] Yet anonymity may also create conditions that facilitate online abuse.[102] Anonymity is often held to have a disinhibiting effect,[103] enabling perpetrators to behave in anti-social, offensive and abusive ways.[104] In cases of youth-related bullying, what has made online bullying so insidious and pernicious is the ability for bullies to act under anonymous cover. Anonymity can also be secured via fake social media accounts, allowing bullies to impersonate others online, pretending to be either their victim or a 'friend' of their victim, a factor which may contribute to victims feeling utterly "socially isolated, manipulated or betrayed".[105]

Some social media applications make a special feature of the ability to participate and post anonymously. 'Ask and answer' service applications, popular among teens and others, for instance, offer anonymous posting options and have been associated with cases of cyberbullying. Newer applications and services continue to evolve and exploit the appeal of anonymous posting and sharing of online content. All this creates safety concerns for educators and child welfare interests and raises ethical issues about the apparent endorsement of covert risk-taking behaviour by young people.

Several consultation submissions called attention to the role of anonymity in online bullying, arguing that anonymity in an online context should be regulated, controlled or even banned. Allowing anonymous posting, and bogus or fictitious names, it was claimed, provides bullies with the opportunity and cover to launch attacks on their victims that they would be reluctant to mount should they be obliged to reveal their correct identity.

3.1.5 Inflammatory messages

Anonymity is also linked to the practices of 'trolling' or 'flaming' in which offensive and sometimes inflammatory messages are targeted at an online community with the intention of disrupting communication for the entertainment value of provoking a response.[106] Exploiting the ability to post anonymously or pseudonymously, such practices, originally confined to online discussion and usenet groups, popular in the 1990s, have become more commonplace with the proliferation of online communities and social media platforms.[107] They have become so prevalent across online discussion groups, comments sections and user-generated review sections on websites that many online providers have considered the need to introduce more stringent – and costly – moderation on discussion lists or to abandon user comments altogether.[108]

---

[101] Khondker, H. H. (2011). Role of the New Media in the Arab Spring. *Globalizations*, 8(5), 675–679.

[102] As argued by the Minister for Communications, Energy and Natural Resources, Pat Rabbitte TD, in his presentation to the Joint Oireachtas Committee, 6 March 2013.

[103] Peter, J., Valkenburg, P. M. & Schouten, A. P. (2006). Characteristics and Motives of Adolescents Talking with Strangers on the Internet. *CyberPsychology & Behavior, 9*(5), 526–530.

[104] Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior, 7*(3), 321–326.

[105] See Net Addiction: http://www.netaddiction.co.nz/bullying.html

[106] Herring, S., Job-Sluder, K., Scheckler, R. & Barab, S. (2002). Searching for Safety Online: Managing "Trolling" in a Feminist Forum. *The Information Society, 18*(5), 371–384.

[107] Bishop, J. (Ed.). (2013). *Examining the Concepts, Issues, and Implications of Internet Trolling: IGI Global*. Retrieved from http://www.igi-global.com/chapter/psychology-trolling-lurking/74111

[108] Carroll, Jim, 'Cleaning up the wild west: how to deal with internet comments'. *On the Record Blog. The Irish Times*, 7 May 2014. Retrieved from http://www.irishtimes.com/blogs/ontherecord/2014/05/07/cleaning-up-the-wild-west-how-to-deal-with-internet-comments/

A number of submissions to the public consultation called attention to the challenges for editorial management and moderation of user-contributed content, arguing that it should not be possible to publish material on an online platform without the real name and contact details of the author being attached.

The Journal.ie in its submission, called attention to the lack of provision within the Defamation Act, 2009 for user-generated content. The legal defence that Host publishers often rely upon is the fact that they post-moderate discussions: comments are posted automatically and are not vetted in advance of online publication (and often only on foot of complaints from publication subjects). Post-moderation (or no-moderation) qualifies a publisher as merely Hosting[109] the information or content rather than being the originator of the publication and therefore making the Host arguably not legally responsible for any statements made. However, publishers do become liable for this content if they have moderation or a post-moderation process in place whereby staff review posts in any way – whether that be for quality, taste, defamation or for other criteria. If, therefore, a Host puts any kind of moderation or previewing process in place to detect or limit cases of cyber-bullying or defamation for instance, this would make them liable for any publications or comments that were not spotted as part of the previewing or post moderation process, or insofar as the Host may have failed to takedown the offending publication on receipt of valid notice from the subject or complainant. This acts as a deterrent to publishers in establishing any processes at all – by ignoring their comments section, they can avoid the substantial financial risk of a defamation action.[110] The task of moderation or previewing each and every post to a Host content provider site would be next to impossible to resource, thereby making pre-moderation, moderation or preview, the exception rather than the norm. This well understood principle has in recent months come under scrutiny as a result of a decision in the European Court of Human Rights.[111]

3.1.6 Online hate speech

Incitement to hatred in an internet context, or hate speech, is a form of online abuse that poses further challenges for policy. It straddles the boundary between free and 'protected' speech and criminal incitement to hatred.[112] Regulating hate speech in a global and cross-jurisdictional context has proved a particular challenge, highlighting the limitations of unilateral legislation or intervention. There has thus been a preference for international collaboration between governments, industry and civil society.[113] Yet hate speech is not confined to extremist websites; recent cases related to popular sites such as Twitter and Facebook highlight a growing trend of online abuse and relatively effortless expressions of hatred on popular social media platforms. In Ireland, the publication of an 'obnoxious and revolting' Facebook page against Travellers in 2009 was the first case of its kind brought under the Incitement to Hatred Act 1989.[114] Internationally, the successful prosecution of two individuals for sustained abuse and harassment on Twitter of feminist and journalist Caroline Criado-Perez has focused attention on the widespread misogynistic abuse that many women, well-known and otherwise, encounter online.[115]

---

[109] Hosting as defined by Article 14 of 2000/31/EC and Regulation 18 of S.I. 69 of 2003, The E-Commerce Directive.

[110] Submission by Journal.ie to the consultation.

[111] Case of Delfi AS v. Estonia. http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{"itemid":["001-126635"]}

[112] Leets, L. (2001). Responses to Internet Hate Sites: Is Speech Too Free in Cyberspace? *Communication Law and Policy, 6*(2), 287–317.

[113] Banks, J. (2010). Regulating hate speech online. *International Review of Law, Computers & Technology, 24*(3), 233–239.

[114] Facebook Traveller rant was a "once-off" (2012, December 1). *Independent.ie*. Retrieved from http://www.independent.ie/irish-news/courts/facebook-traveller-rant-was-a-onceoff-26777448.html

[115] Cockerell, J. (2014, January 24). Twitter "trolls" Isabella Sorley and John Nimmo jailed for abusing feminist campaigner Caroline Criado-Perez. *The Independent*. Retrieved from http://www.independent.co.uk/news/uk/crime/twitter-trolls-isabella-sorley-and-john-nimmo-jailed-for-abusing-feminist-campaigner-caroline-criadoperez-9083829.html

The Immigrant Council of Ireland (ICI) has reported that racist online speech accounts for just over 10% of all cases reported to it in 2013.[116] In its submission to the Oireachtas Justice Committee, ICI argued that it is unacceptable that individuals and groups can go online to spread messages of hate with no fear of prosecution, because internet servers are based in another country. In response, it has called for the ratification of European Convention on Cybercrime to ensure a robust response to online racism, as well as reporting of racism on the Garda Pulse system to enable more detailed statistics of incidences of racism.

NASC, the Immigrant Support Centre, in its submission, similarly argued that legislative and policy reform is necessary to curb racist and xenophobic expressions that occur on the internet.[117] Current legislation, including the Prohibition on Incitement to Hatred Act, 1989 and the Equality Acts, it argues, were put in place before the development of social media networks, which can serve to propagate expressions of racism and xenophobia, and – it is claimed – are difficult to prosecute. Retention of evidence and appropriate means of investigation to secure successful prosecutions are also areas of concern. NASC, therefore, calls for the development of guidelines and training to tackle such issues and to aid understanding of how the current legislation applies to online racism.

3.1.7 Misuse of personal data

Invasion of privacy and the abuse or misuse of personal data also frequently feature as an aspect of abuse in online contexts. Social media allow people to share large amounts of personal information, including contact, biographical and other identifying details, as well as images and videos of themselves, family and friends. There are particular concerns that, due to lack of skills or immaturity, young people may be vulnerable to online abuse or reputational damage. In 2011, EU Kids Online found that nearly 10% of 11-16 year-olds had been victims of personal data misuse, the most common of which was somebody gaining access to their account and pretending to be them.[118]

Abuse or misuse of personal information arises in a number of contexts:

- Identity theft or impersonation through unauthorised access to a user's account, whether through hacking or lost or stolen password
- Being tricked or cheated online to reveal personal information (phishing scams)
- Posting data, including images and videos, and tagging others, without consent

Serious privacy violations may occur through the non-consensual posting of private, false, humiliating, shameful or other harmful content.[119] The posting of embarrassing content is reputedly commonplace in cases of cyberbullying; it featured in the case of the so-called 'Star Wars Kid' video, one of the first demonstrations of the way content can spread virally online and the harmful consequences that can ensue.[120] The serious harm that can arise from posting content online has been underlined very directly in instances where, with frightening speed, indecent images of a minor may spread across social networks.

---

[116] Immigrant Council of Ireland (2014, March 21). National Action Plan Needed to Combat Racism. Retrieved from http://www.immigrantcouncil.ie/media/press-releases/811-national-action-plan-needed-to-combat-racism

[117] NASC, Irish Immigrant Support Centre. Submission to the consultation.

[118] Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. (2011). *Risks and safety on the Internet: The perspective of European children. Full Findings.* London, LSE: EU Kids Online, p.99.

[119] Law Reform Commission (2014, January). Scoping Paper (Draft). Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying. Dublin: Law Reform Commission.

[120] Campbell, M. A. (2005). Cyber Bullying: An Old Problem in a New Guise? *Australian Journal of Guidance and Counselling, 15*(01), 68–76.

In everyday practice, social norms regarding breaches of netiquette and non-consensual sharing of content continue to evolve. Companies are placing increasing emphasis on making terms of use or community guidelines more accessible and visible to their users. Awareness-raising has also continued to educate young people about posting publicly, using slogans such as 'ThinkB4UClick' to instil greater awareness of privacy, digital footprint and acceptable online use.[121]

From the perspective of responding to and dealing with instances of cyberbullying, one of the key issues that arises is the taking-down of offending or hurtful material. A number of submissions to the public consultation expressed frustration at the lack of a satisfactory response to requests for taking down material which users (or their parents or guardians) had found hurtful or damaging. Submissions from Comhairle na nÓg, Galway and the Webwise Youth Advisory Panel suggested an independent reporting mechanism to aid members of the public – be they a young person, teacher, youth worker or other responsible adult – in processing complaints. One submission proposed enhanced powers for the Office of the Data Protection Commissioner (ODPC) to provide an alternative mode of administrative redress, instead of court proceedings, whereby the ODPC would pursue a complaint with internet companies on a complainant's behalf. Clear criteria would be needed to prevent such a process from being overloaded by frivolous queries.

3.2 Legislative and policy responses

3.2.1 The current legal position

Existing legislation was deemed by the Minister for Justice and Equality to be adequate for the offences of bullying and harassment, but its applicability to cyberbullying has been referred to the Law Reform Commission. Its review is ongoing.

Under existing legislation, bullying and harassment are covered under the following provisions:

i. Non-Fatal Offences Against the Person Act, 1997

Section 10 of the Non-Fatal Offences Against the Person Act, 1997 deals with the offence of harassment. Section 10 of the Act prohibits the harassment of a person 'by any means' by 'persistently following, watching, pestering, besetting or communicating with him or her'. As noted by the Special Rapporteur on Child Protection, the explicit reference to communication with a victim 'by any means' suggests that this provision is well suited to the kind of circumstances that arise in cases of cyberbullying. However, the limited number of prosecutions taken may suggest difficulties in investigating complaints of cyberbullying.[122]

ii. Communications Regulation (Amendment) Act 2007

The Communications Regulation (Amendment) Act 2007, Section 13 amends a pre-existing offence under the Post Office (Amendment) Act 1951 with reference to the use of the **telephone** system by anyone who:

a) sends by telephone any message that is grossly offensive, or is indecent, obscene or menacing, or (b) for the purpose of causing annoyance, inconvenience, or needless anxiety to another person–(i) sends **by telephone** any message that the sender knows to be false, or (ii) persistently makes telephone calls to another person without reasonable cause.[123]

---

[121] ThinkB4UClick, Junior Certificate CSPE Resource, NCTE and Irish Council for Civil Liberties. Retrieved from http://www.thinkb4uclick.ie/

[122] Shannon, Dr Geoffrey. (2013). *Sixth Report of the Special Rapporteur on Child Protection*. Dublin: Department of Children and Youth Affairs, p.96.

[123] The Communications Regulations (Amendment) Act 2007 substitutes (under Schedule 1, Part 2 of the Act) a new section 13 into the Post Office (Amendment) Act 1951 to replace the existing section 13. In the amended section, 'message' is taken to include a text message sent by means of a short message service (SMS) facility – Section 13 (5).

This section was noted by the Special Rapporteur on Child Protection to be especially restrictive in addressing messages by telephone only, excluding electronic communications or social media. The Minister for Communications, Energy and Natural Resources also acknowledged this gap in legislative provision in his presentation to the Joint Oireachtas Committee on Transport and Communications.[124]

iii. Prohibition of Incitement to Hatred Act, 1989

The Prohibition of Incitement to Hatred Act, 1989 provides for the offence of online hate speech and prohibits preparation or publication of any materials leading to incitement to hatred against any group of persons 'on account of their race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation'. Section 1(1) defines *broadcast* as 'the transmission, relaying or distribution by wireless telegraphy ...or by wireless telegraphy in conjunction *with any other means of communications*' (emphasis added). As such, the definition may be taken to include communication by the internet.

NASC, the Irish Immigrant Support Centre, indicated in its submission, and previously to the Joint Oireachtas Committee on Transport and Communications,[125] that clarification is needed that the Act also applies to racist acts, as acts constituting incitement to hatred. It has also argued that ratification of the Council of Europe Additional Protocol to the Convention on Cyber Crime[126] would help to combat racist material on the internet.

In addition to the above categories of offences under Irish criminal law, civil law protection is also afforded under data-protection and defamation legislation.

iv. The Data Protection Acts, 1988 & 2003

The Data Protection Acts (1988 and 2003) give individuals rights and afford them with certain key protections while creating obligations and imposing responsibilities on data controllers.[127] In this sense, the placing of personal information about a person online, including the posting, without consent of images or videos, will be a breach of the Data Protection Act (DPA). Research conducted by the Office of the Data Protection Commissioner would appear to show, particularly among young people, a low level of awareness and understanding of privacy legislation and its application to the online world.[128] Digital Rights Ireland, accordingly, has called for greater resourcing of the Data Protection Commission, arguing that were it better funded it would be better able to help ensure that privacy rights could be properly and promptly vindicated by the average citizen.[129]

v. Defamation Act 2009

The 2009 Defamation Act provides that a defamatory statement, or 'a statement that tends to injure a person's reputation in the eyes of reasonable members of society', can be published by any means, including via the internet. Defamation law thus provides a comprehensive range of remedies for plaintiffs in cases of defamation online or on any

---

[124] Joint Committee on Transport and Communications. (2013). *Addressing the Growth of Social Media and tackling Cyberbullying.* Dublin: Houses of the Oireachtas, p.34.

[125] *ibid.* p.36.

[126] Council of Europe (2003). *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.* Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm

[127] Office of the Data Protection Commission. A Guide to your rights. Retrieved from http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/rights/RightsPlainEnglish.htm&CatID=16&m=r

[128] The i in online. Children and Online Privacy Survey. (2011). Retrieved from http://www.dataprotection.ie/viewdoc.asp?m=t&fn=/documents/teens/document1.htm

[129] Digital Rights Ireland. Submission to the Joint Committee on Transport and Communications.

medium. It is also the case, as noted by Digital Rights Ireland, that Irish courts have long taken the view that the crude and vulgar abuse often found online is not necessarily defamatory.[130]

The E-Commerce Directive 2000/31/EC transposed into Irish law by S.I. 68 of 2003, and the Defamation Act, 2009, deal with the issues of user-generated content and with the liability for Hosts. Online service providers and publishers maintain exemption from liability for defamatory content on the basis that they are acting as Hosts for information and are therefore not liable for the content of messages until such time as they are made aware of the unlawful or problematic nature of the content, in the same way that telephone companies and ISPs are exempt by virtue of the protection afforded to them as "mere conduits". The Defamation Act, 2009 does not discriminate between the form that a publication takes. Once it is published, and not removed from a Host provider (as defined) liability can attach to the Host.[131] At the same time, in the case of publishers who engage in moderation of content on their services, they retain the Hosting defence, if they operate a notice and take-down procedure on receipt of a complaint about offending content.

vi. Children First Bill 2014

Elements of the *Children First: National Guidance for the Protection and Welfare of Children (2011)* are in the process of being placed on a statutory footing.[132] Section 9 of the Children First Guidance deals with bullying in schools and in 9.4.5 states that 'Serious instances of bullying behaviour should be referred to the HSE Children and Family Services'.[133]

3.2.2 Soft law

Given the sensitive nature of the subject matter and the vulnerable age of many victims and perpetrators, the approach of soft law, in contrast to criminal codes or hard approaches, is increasingly preferred as a means of dealing with online abuse.[134] Soft law refers here to the range of self- and co-regulatory measures developed at national and European level as a means of tackling online abuses. A number of frameworks brokered both by industry groupings and by the European Commission are relevant in this regard.

The *Safer Social Networking Principles for the EU* is an agreement entered into in 2009 by the major social networking providers in Europe in consultation with the European Commission and a number of children's charities.[135] The principles set out good-practice recommendations for social networking providers to enhance safety. The framework entails a set of commitments around the provision of services in which age-appropriateness and safety are valued as primary objectives. Thus, signatories undertake to raise awareness of safety issues and acceptable-use policies to users (Principle 1); to provide easy-to-use mechanisms to report content or conduct that violates the Terms of Service (Principle 4), and to encourage users to employ a safe approach to personal information and privacy (Principle 6).

130 Digital Rights Ireland. Submission to the public consultation.

131 *Mulvaney v. Betfair* [2011] 1 IR 85 – High Court holds that hosting defence is available to chatroom operators. http://www.tjmcintyre.com/2009/05/mulvaney-v-betfair-high-court-holds.html

132 http://www.oireachtas.ie/viewdoc.asp?DocID=25898&&CatID=5

133 DCYA. (2011). Children First: *National Guidance for the Protection and Welfare of Children*. Dublin: Department of Children and Youth Affairs. Retrieved from http://www.dcya.gov.ie/viewdoc.asp?fn=/documents/Publications/ChildrenFirst.pdf

134 Brenner, S. W., & Rehberg, M. (2009). Kiddie Crime – The Utility of Criminal Law in Controlling Cyberbullying. *First Amendment Law Review, 8*, 1. See also: Bauer, T. (2014). The Responsibilities of Social Networking Companies: Applying Political CSR Theory to Google, Facebook and Twitter. *Critical Studies on Corporate Responsibility, Governance and Sustainability, 6*, 259–282.

135 European Commission (2009). Safer Social Networking Principles for the EU. European Commission. Retrieved from http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf

The *European Framework for Safer Mobile Use by Younger Teenagers and Children*, a self-regulatory initiative of the European mobile industry, is also important in this regard.[136] Developed in conjunction with the High-Level Group on Child Protection, set up by Commissioner Viviane Reding in 2006, the framework has underpinned the rollout of national self-regulatory codes of conduct on safer mobile use in EU member states, represented in Ireland by the code of practice of the Irish Cellular Industry Association.[137] In addition to providing for a range of content control measures, mobile operators undertake to raise awareness and provide advice to parents on safer use of mobile services, and ensure customers have ready access to mechanisms for reporting safety concerns.

The *ICT Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU* was signed in 2012 by a coalition of manufacturers and network, connectivity and online providers as an overarching framework for implementation of safety principles in all aspects of design and delivery of content and service provision, where use by children and young people is likely.[138] Its provisions include undertakings by participating companies to provide clear and simple processes whereby users can report behaviour that breaches the service's terms and conditions, to implement appropriate procedures for reviewing user reports, and to support methods to educate users in safer online use. Relatedly, the CEO Coalition for a Better Internet for Children, a coregulatory initiative sponsored by European Commission Vice-President Neelie Kroes, has among its objectives the initiation of concerted industry action on the development of simple and robust reporting tools to counter online abuse.[139]

Submissions from a variety of industry groups argue that existing legislation and current industry measures, as provided under various self-regulatory frameworks, are adequate to deal with the challenges posed by online abuse, cyberbullying and harassment. In particular, it is argued, compliance with user terms and conditions and greater awareness of how to report breaches of community guidelines represent the most effect way for online communities to regulate themselves. Self-regulation has been supported by the Irish Government and initiatives such as the European Commission's Safer Internet Programme as the most appropriate approach to internet safety. To be successful, however, self-regulation requires adoption across the sector as well as ongoing evaluation of its effectiveness. Evaluation studies to date have, on the whole, endorsed actions taken by industry but have also called for more inclusiveness (given that not all companies participate), more transparency with regard to reporting, and commitment to innovation in safety standards.[140] [141]

[136] GSMA (2007). European Framework for Safer Mobile Use by Younger Teenagers and Children. Retrieved from http://www.gsma.com/gsmaeurope/safer-mobile-use/european-framework/

[137] ICIA Code of Practice (2006). Retrieved from http://www.ibec.ie/IBEC/BA.nsf/vPages/Business_Sectors~Telecommunications_and_Internet_Federation~icia-code-of-practice-04-05-2006/$file/ICIA+Code+of+Practice.pdf

[138] ICT Coalition (2012). Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU. Retrieved from http://www.ictcoalition.eu/

[139] CEO coalition to make the Internet a better place for kids. Retrieved from http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids

[140] O'Neill, B. (2014). *First report of the implementation of the ICT Principles.* Brussels: The ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU. Retrieved from: http://www.ictcoalition.eu/

[141] Donoso, V. (2011). Assessment of the Implementation of the Safer Social Networking Principles for the EU on 14 Websites: Summary Report. European Commission.

3.2.3 Education and awareness raising

The reliance on soft law and self-regulatory approaches as the primary means of dealing with bullying and harassment online has created an ever more important need to develop levels of digital literacy and awareness among users. If, as is claimed, the range of existing measures is sufficient: that legislative provision for both criminal and civil prosecution in relation to the most serious kinds of abuses is adequate; that industry processing and response to reports of abuse is effective; and that there is sufficient legal protection for industry providers in handling content, then a priority for policy has to be a major emphasis on awareness-raising and user education.

The Anti-Bullying Working Group in its report recommended 'securing implementation of existing legislative requirements rather than seeking to introduce new legislation' as the preferred approach to dealing with online abuse.[142] It rejected an overtly legislative route, arguing that 'additional criminal sanctions against children and young people' are not the way forward.[143] Instead, it recommends the implementation of awareness and prevention programmes in schools that build empathy, respect and resilience in pupils; and explicitly address the issues of cyber-bullying and identity-based bullying including, in particular, homophobic and transphobic bullying.

Research has found relatively low levels of awareness or take-up among members of the public in relation to remedies for online abuses. Privacy regulation is poorly understood and relatively few complaints to the Office of the Data Protection Commissioner deal with online privacy violations. Reporting mechanisms, such as Hotline.ie, to which any form of abusive content suspected to be illegal may be reported, are greatly underused. There is little public awareness, for instance, that illegal content refers not only to serious forms of child-abuse material but also content that involves racism and xenophobia, incitement to hatred, or financial scams, any of which may also be reported.[144]

Multi-stakeholder action, including the Insafe network of Safer Internet Centres, in conjunction with industry groups have, as a result, focused efforts on promoting greater visibility of reporting tools, support helplines, and resources and trusted sources of information on dealing with abuse. For Safer Internet Day 2014, Webwise, on behalf of the national Safer Internet Centre, coordinated a nationwide campaign to encourage young people to do something positive to help combat online bullying, with the key message that bullying affects everyone and that everyone has a role in doing something about it.[145]

An Garda Síochána runs education programmes in both primary and secondary schools, providing practical information about such topics as crime prevention and personal safety and substance abuse. The programme is provided to 5th class primary-school students and as part of the second-level Social, Personal & Health Education Junior Cycle module.[146] In 2012, as part of Safer Internet Day, An Garda Síochána launched a new initiative, 'Respectful Online Communication', addressing personal safety using new media. The aim of the resource pack is to enhance the social skills of communication, cooperation and conflict resolution, fostering respect for others online, and equipping children with the skills to deal effectively with cyberbullying.[147]

---

142 Anti-Bullying Working Group (2013), p. 73.

143 *Ibid.* p.70.

144 Online Racism Unreported. Retrieved from http://www.hotline.ie/library/online-racism-10042012.pdf

145 Safer Internet Day in Ireland. Retrieved from http://www.saferInternetday.org/web/ireland/home

146 Garda Síochána Schools Programme. Retrieved from http://www.crimecouncil.gov.ie/schoolsprogramme.html

147 Launch of Respectful Online Communication Programme on 6/2/2012. Retrieved from http://www.garda.ie/Controller.aspx?Page=8737

3.3 Recommendations

In responding to the difficult and challenging area of online abuse, harassment and cyberbullying, the group is cognisant of initiatives currently underway, such as the review of legislation by the Law Reform Commission and the continuing rollout of the Action Plan on Bullying. Our recommendations, therefore, focus on the wider aspects of policy response to cyberbullying and harassment, noting areas where some immediate progress may be made.

3.3.1 Legislative reform

The group agrees with the view that existing legislation is, for the most part, adequate to deal with offences of bullying and harassment. A review of the suitability of the Non-Fatal Offences Against the Person Act, 1997 in relation to cyberbullying is ultimately a matter for the Law Reform Commission. The group also concurs with the view of the Special Rapporteur on Child Protection that the Act is sufficient to cover the offence but that its implementation requires further investigation. A majority of the group also supported the position adopted by the Anti-Bullying Working Group that additional criminal sanctions – as, for instance, currently under consideration in New Zealand – are not appropriate as a means of tackling a complex social problem. However, it may be prudent to monitor the effectiveness of any initiative over time should it be found that a new approach or methodology is more effective.

The group is of the view that the Communications Regulation (Amendment) Act 2007 should be amended to include 'electronic communications' within the definition of measures dealing with the 'sending of messages which are grossly offensive, indecent, obscene or menacing'. Pending a full review of provision in this area by the Law Reform Commission, such an amendment would close a gap that has been identified in the legislation, will support victims of abuse, and will strengthen the capacity of An Garda Síochána to deal with reports of offences under the Act.

Due consideration should be given in the wording of any such legislation to address the concern put forward by Digital Rights Ireland that amending the Act would place an impossible burden on internet providers by making all online content subject to an offensiveness test.

The group also took the view that, with regard to the Prohibition of Incitement to Hatred Act 1989, 'electronic communications', including transmission via the internet, is adequately covered in the meaning of 'transmission, relaying or distribution by wireless telegraphy or by any other means' (emphasis added). Accordingly, no amendment is recommended. However, awareness-raising in relation to Hotline.ie as a mechanism to report content that may be illegal under the Act is strongly encouraged. Furthermore, appropriate classification by An Garda Síochána of reports of online abuse, including racism and incitement to hatred, on the Pulse system is recommended to facilitate more detailed crime reporting.

The group noted during its consultation and deliberations, that national Court procedures for pre and post action tracing of publishers and perpetrators of online crimes and torts appears to be both expensive, lacking detail and out of date in this jurisdiction.

The group notes that in cases where victims of tortious (Defamation, Copyright infringement, etc.) or criminal activity online (Harassment, Coercion, Endangerment, Identity Theft, etc.), the only recourse appears to be to the High Court in cases of tortious online activity, and to the law enforcement authorities in cases of criminal online activity.

In recent years, the requirement for parties to apply to the High Court for non-party discovery and disclosure orders, more commonly referred to as *Norwich Pharmacal* Orders (inherent jurisdiction court applications),[148] has become far more necessary than ever before.[149]

The group notes that unlike the United Kingdom,[150] the Irish Rules of the Superior Courts are very limited for any party seeking originating non-party discovery and disclosure of online information. This is outside of any uncodified rules adapted and applied by the division of High Court vested with supervision of such applications.

The group notes the limitations of Order 31, Rule 29 of the Rules of the Superior Courts, and that the Order only appears to contemplate non-party discovery and disclosure, in circumstances where some related or connected proceedings are already extant. This situation is out of synchronisation with more modern communications, and can create both delays and expense for those affected by such torts or crimes.

The group notes that the requirement for court ordered non-party discovery and disclosure operates to protect the ISP, Host or internet intermediary from a concomitant confidence, privacy and data protections actions, and also operates to compel the information requested (Internet Protocol – IP address, and subscriber account information) in circumstances where that information, or that data would not normally be compellable under Data Protection or E-commerce or other pre-existing legislation.

The group recommends, therefore, that three new Superior Court Rules be contemplated and brought by the Minister for Communications, to the Minister for Justice, the Attorney General, and the High Court Rules Committee. This is in order to aid victims of online tortious activity, and albeit purportedly anonymous online publication.[151]

The three new proposed Court Rules are:

1. A Rule dealing in detail with the issue, origination, procedure and costs of orders seeking **Disclosure before proceedings start**;
2. A Rule dealing in detail with the issue, joinder, origination, procedure and costs of orders seeking **Orders for disclosure against a person not a party** (seeking to enhance and modernise the pre-existing Order 31, Rule 29 of the Rules of the Superior Courts);
3. A Rule dealing in detail with the issue, joinder, origination, procedure and costs of orders seeking **Orders for disclosure against a person not a party to an action and not currently known**.[152]

The group would like to see such orders being made available to litigants in lower jurisdictions than the High Court, e.g., the Circuit Court, in order to save on delay, expense and effort. This may be a matter contemplated in the forthcoming work of the Law Reform Commission.

---

[148] *Norwich Pharmacal v. Customs & Excise* [1974] A.C. 133; *The Rugby Football Union v. Consolidated Information Services Limited* (formerly Viagogo Limited) [2012] UKSC 55

[149] *EMI Records (Ireland) Limited & Ors. v. Eircom Limited & Ors.* [2005] 4 IR 148.

[150] *English Civil Procedure Rules & Practice Directions*: Part 31 – Disclosure and Inspection of Documents – Rules: 31.16; 31.17; 31.18.

[151] *McKeogh v. John Doe & Ors.* [2012] IEHC 95

[152] A protective Order/issue of proceedings, allowing for Statute of Limitations considerations, complex tracing and the for issue of proceedings in the Central Office of the High Court, or other relevant court offices, as against parties currently unknown, but hosted online.

3.3.2 Role of Safer Internet Ireland Centre and National Council for Child Internet Safety

The group believes that an expanded role for the Safer Internet Ireland Centre (SIIC) and National Council for Child Internet Safety (NCCIS), as recommended in Chapter 2, can play a crucial role in implementation of safety measures to counteract bullying and harassment. The central role envisaged for each will allow for better coordination of existing efforts, both at the level of service delivery (SIIC) and in relation to policy coordination (NCCIS).

We recommend that the NCCIS undertake the following actions to deal with online bullying and harassment:

- Building on the participation of leading internet companies, the council should foster close co-operation between stakeholders with particular reference to ensuring the effectiveness of industry measures, as envisaged in Objective 3.19 of the National Policy Framework for Children and Young People.
- Industry measures in this context refers to availability and effectiveness of reporting mechanisms; notice and takedown procedures for harmful content; response times in relation to complaints received regarding cyber bullying and harassment; implementation of best practice with respect to privacy controls; and, the availability of appropriate educational resources and materials on industry platforms for adults and for young people.
- The council should collaborate with the implementation group for the Anti-Bullying Action Plan to coordinate stakeholder responses and advise with regard to emerging risks and good practices in dealing with online abuse to all internet-related dimensions of bullying and abuse. It may also wish to commission research on the most effective ways to counteract bullying and harassment.

The Safer Internet Ireland Centre should:

- Compile resources of best practices in dealing with online abuse and harassment for parents, teachers and young people
- Plan and direct a national awareness campaign on effective measures to deal with the reporting cyberbullying and online abuse
- Provide guidance to schools on incorporating best practice in relation to social media and online communication in schools' anti-bullying policies
- Work with the ODPC to raise awareness of privacy issues in relation to sharing of content online and the most appropriate ways to deal with violations of privacy
- Promote the availability of Hotline.ie reporting services for illegal content, including racist speech and incitement to hatred

3.3.3 Supporting education and awareness raising

Effective education and awareness-raising is central to effective strategies to deal with cyberbullying and harassment. The group supports the full implementation of the Action Plan on Bullying and welcomes the wide-ranging measures that have been adopted to develop school policies and actions to deal with bullying and harassment.

The following additional measures are recommended to support education on internet-related dimensions of bullying:

- An inter-agency working group should be established by DES in conjunction with the National Council for Curriculum and Assessment (NCCA) to identify appropriate mechanisms to ensure that internet safety and digital literacy skills are taught as a core element of the curriculum at both primary and post-primary levels with the focus on promoting positive, safer, and more effective use of technology by children.
- The Digital Media Literacy short course developed by the NCCA for the proposed new Junior Cycle provides an excellent example of a programme that allows students to develop their fluency in online communication by giving them opportunities to explore and discover the information and knowledge accessible online to pursue their interests and solve problems that are relevant to their lives. In studying digital media, students learn to use digital technology, communication tools, and the internet to engage in self-directed enquiry.
- Further support should also be given to training directed at parents to make them aware of risks of cyberbullying and how to deal with it. Training initiatives such as those developed by the National Parents' Council, should be further expanded and resourced.
- The Garda Síochána Schools Programmes for primary and post-primary, dealing with cyberbullying among other topics, should be extended to include an equivalent resource for parents to explain the role of policing in relation to online abuse and harassment.

Chapter 4: Harmful and age-inappropriate content

The apparent ease with which young people can access or stumble across unsuitable or harmful content online has given rise to much concern. Just as the internet offers extraordinary resources and a wealth of valuable information and knowledge, so too it contains content that may be offensive, harmful or simply inappropriate for younger users. Content that is restricted, or even banned, in traditional media outlets, may be easily accessed on the internet. Negative content, including much that is user-generated and shared online, comprises a vast array of material that includes adult pornography and other content that may be upsetting, offensive or harmful for young people. Commercial online content and direct marketing strategies to children is another area that has given rise to concern, amidst fears that young people are being targeted and subject to unfair commercial pressures, without parental consent or even knowledge.

How to manage or restrict access to content that may harmful for young people's development – or that users simply do not wish to see – is a topic that has been debated since the development of the World Wide Web. Striking the right balance between preserving online freedom of expression and restricting access to harmful content is a difficult and challenging task. Internationally, a number of different strategies have been pursued, yet there is neither consensus on the best approach nor whether solutions in one jurisdiction may be suitable or appropriate in another. Clearly, cultural context plays a major role in determining community standards in matters of taste, decency and social acceptability. The interconnected nature of the internet, however, is such that social and cultural values inevitably collide, creating new dilemmas for policy and for internet content governance.

The group's terms of reference included consideration of recent proposals, as for instance in the UK, to request that ISPs block access 'by default' to certain kinds of material that may be age-inappropriate or potentially harmful but otherwise legal. In examining this area, the group took into account current regulatory approaches in Ireland as well as some established strategies promoted by the European Commission such as access controls for age-inappropriate content, policies governing classification and labelling, parental controls and filtering, and age verification techniques. Our conclusions and recommendations in this area focus on internet content governance measures to support youth online protection as a public policy objective.

4.1 Harmful and age-inappropriate content

4.1.1 Adult Content

The ease with which young people can access online pornographic content is a topic that has garnered much media attention and, as submissions to the public consultation illustrate, has caused some public disquiet. In addition, sensationalist media coverage of youth and pornography has tended to contribute to a 'technopanic', amplifying concerns about the harmful effects of age-inappropriate content on young people's development, especially in relation to their attitudes to sexuality.[153]

[153] Thierer, A. (2013). Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle. *Minnesota Journal of Law, Science & Technology*, 14, 311–385.

Levels of exposure to pornographic content by teenagers are such leading some researchers to describe it as a normative experience.[154] Surveys in the US and in Europe both point to approximately half of older teenagers (aged 15-16) accessing pornographic content online.[155] Health professionals and child welfare specialists have warned of the dangers of early exposure to sexual content for children and young people who may be ill-prepared and emotionally immature.[156] For some, exposure is voluntary in that they actively seek it out. However, according to US researchers, for over a third, the exposure was unwanted.[157] Accounts of how upsetting or harmful such exposure may be vary. According to EU Kids Online, of those who have seen sexual or pornographic images online, one in three were upset by the experience and, of those, half were either fairly or very upset by what they saw.[158] More generally, exposure to sexually explicit content is associated with distorted and instrumental attitudes to sex, early sexualisation and with gendered notions of women as sex objects.[159] [160]

Sexually offensive content, as well as the portrayal of violence in the media, have historically provided a justification for introducing regulation of content that may be harmful to minors.[161] Concerns about the impact of indecent content are not new: indeed, there is a legacy of moral concern regarding threats posed by new media forms and the appropriate kinds of regulation required to protect children from harmful influence.[162]

Censorship of the media on the grounds of obscenity is still a feature of the legal system in Ireland, even if largely inactive.[163] As in other jurisdictions, legislation dealing with film and literature, such as the *Censorship of Films Acts, 1923-1992* and the *Censorship of Publications Acts, 1929-1965*, provides the principal basis for regulation or censorship of material that is obscene, blasphemous or contrary to public morality. In some jurisdictions, such as South Africa, that legislation has been extended to include publication on the internet, requiring film-like classification and regulation of all audiovisual content, regardless of the medium in which it is transmitted.[164]

There is no equivalent legislation in Ireland for internet content. Under European audiovisual regulatory rules, so-called restricted content, such as adult or 'hardcore pornography', is banned from terrestrial television but may be available online or through an on-demand, television-like service, subject to controls that would prevent young people gaining access (Article 12 of the AVMSD). In Ireland, On-Demand Audiovisual Media Services (ODAS) acts as the principal mechanism for regulation of online audiovisual content. Under the 2010 regulations giving effect to the AVMSD, operators of on-demand

---

[154] Sabina, C., Wolak, J., & Finkelhor, D. (2008). The Nature and Dynamics of Internet Pornography Exposure for Youth. *CyberPsychology & Behavior, 11*(6), 691–693.

[155] Wolak, J., Mitchell, K., & Finkelhor, D. (2007). Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users. *Pediatrics, 119*(2), 247–257.

[156] Ross, C. C. (2012, August 13). Overexposed and Under-Prepared: The Effects of Early Exposure to Sexual Content. *Psychology Today.* Retrieved from http://www.psychologytoday.com/blog/real-healing/201208/overexposed-and-under-prepared-the-effects-early-exposure-sexual-content

[157] Kimberly J., Mitchell, Lisa Jones, Finkelhor, D., & Wolak, J. (2014). Trends in Unwanted Exposure to Sexual Material: Findings from the Youth Internet Safety Studies. *3rd Youth Internet Safety Survey.* Retrieved from http://www.unh.edu/ccrc/

[158] Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *Risks and safety on the Internet: The perspective of European children. Full Findings.* London, LSE: EU Kids Online.

[159] Peter, J., & Valkenburg, P. M. (2010). Processes Underlying the Effects of Adolescents' Use of Sexually Explicit Internet Material: The Role of Perceived Realism. *Communication Research, 37*, 375–399.

[160] Zurbriggen, E. L., Collins, R. L., Lamb, S., Roberts, T.-A., Tolman, D. L., Ward, L. M., & Blake, J. (2007). Report of the APA Task Force on the Sexualization of Girls. *American Psychological Association*: Washington, DC Available Online at http://www.Apa.Org/pi/wpo/sexualizationrep.pdf. Retrieved from www.apa.org/pi/wpo/sexualization.html

[161] Heins, M. (2008). Not in *Front of the Children: Indecency, Censorship, and the Innocence of Youth* (2nd Revised edition edition.). New Brunswick, N.J: Rutgers University Press.

[162] Oswell, D. (2008). Media and Communications Regulation and Child Protection: An Overview of the Field. In S. Livingstone & K. Drotner (Eds.), *International Handbook of Children, Media and Culture* (pp. 469–486). London: Sage.

[163] Carolan, E. (2010). *Media Law in Ireland.* Haywards Heath, West Sussex U.K.: Bloomsbury Professional.

[164] Watney, M. (2008). Regulation of Internet Pornography in South Africa. Retrieved from http://www.isrcl.org/Papers/2005/Watney.pdf

audiovisual media services are required to develop codes of conduct, in co-operation with the BAI, and other relevant bodies (s.13(1)).[165] The code contains the provision that content unsuitable for children, or that 'might seriously impair' their physical, mental or moral development, can only be made available in a way that ensures that minors will not normally hear or see such on-demand audiovisual media services.[166] However, the ODAS code covers only on-demand content services originating within the Republic of Ireland, and has no effect on online content from outside the jurisdiction.

4.1.2 Other potentially harmful content

The internet, in contrast to most other media, allows for the sharing of content on an unprecedented scale. Almost anyone who is connected to the internet can make all kinds of material available to a large number of people. User-generated content now constitutes a vast array of material that is non-institutional and non-professional in nature that may be shared among peers and online communities, and may promote values, activities or knowledge that could be unsuitable for children.[167] So called 'negative' user-generated content comprises material that may be offensive or harmful, and includes websites or content that promote self-harm, drug-taking or alcohol abuse, as for instance in the recent phenomenon of 'neknominations';[168] so-called 'pro-ana' and 'pro-mia' websites promoting pro-anorexia or bulimia as lifestyle choices; websites containing racism, hate speech, or anti-LGBT (lesbian, gay, bisexual and transgender) attitudes; extremist political radicalisation; and websites that contain frightening, violent or gory content. Concern has also been raised about the phenomenon of 'sexting' (the self-production of indecent content by minors), involving the sharing between users of sexually explicit messages or photos online or via mobile devices.[169] [170]

EU Kids Online found that a quarter of Irish young people, aged 11-16, had come across harmful online content: 16% had encountered hate messages; 11% had seen anorexic/bulimic sites; 9% had accessed self-harm sites as well as sites about drug taking, and 4% had seen websites discussing suicide.[171] 11% also report having received a sexual message or 'sext' online or on a mobile device.[172] In the same research, young people spoke about the content that upset them most, listing pornographic as well as violent content among their top internet concerns. The latter includes a range of violent, aggressive or gory online content involving cruelty, abuse of animals and killings.[173] A number of submissions to the public consultation raised concerns about the prevalence of harmful online content; the ISPCC noted in its submission the many calls to its Childline service from children who were distressed and confused by what they had seen online.[174]

---

[165] Statutory Instrument no 258 of 2010 ("SI") entitled European Communities (Audiovisual Media Services) Regulations 2010. Retrieved from http://www.bai.ie/wordpress/wp-content/uploads/SI-258-2010.pdf

[166] ODAS Code of Conduct for media service providers of on-demand audiovisual media services. Retrieved from http://www.bai.ie/?page_id=2082

[167] Livingstone, S. (2014). Risk and harm on the Internet. In A. B. Jordan & D. Romer (Eds.), *Media and the Well-Being of Children and Adolescents*. Oxford University Press.

[168] McMahon, C., & Aiken, M. (2014, February 5). #neknomination: the internet has changed drinking games. *The Conversation*. Retrieved from http://theconversation.com/neknomination-the-internet-has-changed-drinking-games-22786

[169] Aiken, M., Moran, M., & Berry, M. J. (2011). Child abuse material and the Internet: Cyberpsychology of online child related sex offending. Presented at the 29th Meeting of the INTERPOL Specialist Group on Crimes against Children, Lyons. Retrieved from http://www.interpol.int/Crime-areas/Crimes-against-children/internet-crimes

[170] Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2012). Prevalence and characteristics of youth sexting: a national study. *Pediatrics, 129*(1), 13–20.

[171] O'Neill, B., Grehan, S., & Ólafsson, K. (2011). *Risks and safety for children on the Internet: the Ireland report.* LSE, London: EU Kids Online, p.40.

[172] *Net Children Go Mobile: Initial findings from Ireland*, p.22.

[173] Livingstone, S., Kirwil, L., Ponte, C., & Staksrud, E. (2013). *In their own words: What bothers children online?* LSE, London: EU Kids Online.

[174] Submission from ISPCC.

Harmful user-generated content poses a difficult dilemma for policy makers and for online service providers. Content that may be harmful but not illegal falls within the realm of soft law, or governance at the level of terms of service providers' terms of use and community guidelines, as well as being a matter for parental regulation and mediation. As mere conduits, internet service and platform providers typically do not have responsibility for user-created and shared content on their networks, unless advised of material that is either illegal or that contravenes their terms of service. In relation to content that is not illegal, the principal response of industry has been to implement reporting mechanisms whereby users are encouraged to flag or report content that may in breach of the community guidelines of the service.

4.1.3 Pro anorexia/bulimia sites

Bodywhys, the Eating Disorders Association of Ireland, called attention in its submission to the many 'pro-ana' and 'pro-mia' websites and online communities that promote eating disorders (ED), predominantly anorexia (pro-ana) and bulimia (pro-mia), as lifestyle choices.[175] Most of these websites and groups are open to the public although some are password-protected or invitation-only.

Researchers have pointed to difficulty in establishing clear link between effects of viewing pro-ana and pro-mia websites and harmful behaviour. Whilst some academics point to causal links between viewing pro-ED content and the escalation[176] of harmful behaviour, others note that online communities may be seen by some ED sufferers as a support mechanism and may even provide valuable information[177] to researchers and clinicians studying the development and treatment of these disorders.

Bodywhys recommends that 'pro-ana/pro-mia' websites should be recognised as having a serious negative impact on users and be monitored accordingly. The submission from the Webwise Youth Advisory Panel also referred to pro-anorexia content, finding 'gruesome and grotesque images' that promote self-harm and anorexia to be among the most upsetting online content.[178] Efforts to restrict or block these platforms have had limited success, however, as Bodywhys notes in its submission. Possible alternatives may be including a click through to a safe alternative or cycling recovery messages as banner advertisements on these types of sites.

Further research on new and emerging platforms particularly photo sharing applications such as Tumblr, Flickr, Pinterest etc. would assist in understanding the impact of this online content, as the increasing availability of private groups, accounts and message options on social media services may reduce the visibility but not the activity of pro-ED groups online.

4.1.4 Extremism and radicalisation

The use of the internet for radicalisation and recruitment by political extremists and terrorists is an area of online risk that national governments and the European Union have begun to address. Whilst various types of extremism are considered problematic across the EU,[179] a particular focus has been placed, following a number of atrocities, on Islamic extremism. In the UK, the *Prime Minister's Task Force on Tackling Radicalisation and Extremism* made a number of recommendations on countering extremist narratives and ideology online, including working with industry to remove content that is illegal under UK law and developing more effective filtering of extremist content.[180]

---

175 Submission from Bodywhys, the Eating Disorders Association of Ireland.

176 Talbot, T. S. (2010). The effects of viewing pro-eating disorder websites: a systematic review. *The West Indian Medical Journal, 59*(6), 686–697.

177 Casilli, A. A., Pailler, F., & Tubaro, P. (2013). Online networks of eating-disorder websites: why censoring pro-ana might be a bad idea. *Perspectives in Public Health, 133*(2), 1–2.

178 Submission from Webwise Youth Advisory Panel.

179 Such as Nazism and Holocaust denial which are illegal in a number of countries including Germany, Austria and France.

180 Prime Minister's Task Force on Tackling Radicalisation and Extremism. (2013). *Tackling extremism in the UK*. London: Cabinet Office.

While most governments have focused on technical solutions in attempting to remove or block radicalising material, there are limitations and difficulties with this approach.[181] Many of those promulgating extremist ideas online are technically sophisticated and have the capacity to work within the guidelines of the rapidly evolving social media and other platforms available, and, as such, much offending material could be considered legal. In some cases research has indicated that blocking and filtering may be counterproductive[182] as evidence indicates that it is unlikely that radicalisation occurs online only.[183] A recent European Parliament report has also urged caution in the implementation of counter radicalisation strategies that may impact negatively on internet users' rights.[184]

4.2 Commercial content, marketing and advertising

An area receiving growing attention in discussion of online safety is the risk that young people may be the target of unfair marketing techniques and commercial exploitation. The internet is increasingly a thoroughly commercialised environment, where many apparently free apps and services are supported by advertising and marketing based on the profiling of users through the data they share online. Critical literacy or awareness of the commercial interests involved in web-based services is reputedly low, particularly among young people.[185] In the course of their internet use, young people may therefore be pressurised to purchase products or agree transactions for services through in-app purchases. They may be exposed to advertising or direct marketing for products that are unhealthy or unsuitable for their age. They may also be induced into environments that promote gambling.

In the United States, the Children's Online Privacy Protection Act (COPPA), enacted in 1998, restricts websites or online services from collecting personal information from children under the age of 13.[186] The impact of COPPA is global given that most popular web-based services either originate in the United States or include US citizens as customers. COPPA places strict conditions on marketing to children, outlines where verifiable parental consent must be obtained and places responsibilities on providers in relation to the privacy protection of children. Because of its stringent requirements, many website operators and social media providers, both in the United States and internationally, choose to limit their services to over-13s. The enactment of the legislation was primarily the result of concern regarding unfair marketing and advertising techniques, and lobbying by a wide coalition of interests concerned about the commercialisation of childhood.[187] Children under the age of 13 are deemed too young to be able to consent to the information practices of websites; however, advertising, including advertising targeted at children, is not prevented on web services intended for a general audience or for users over the age of 13.

Concern about online commercial marketing of unhealthy products also featured in a number of submissions to the public consultation. The Irish Heart Foundation in its submission argued that the online marketing to children of food and drinks high in fat,

Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/263181/ETF_FINAL.pdf

181 International Centre for the Study of Radicalisation and Political Violence (ICSR). (2009). *Countering Online Radicalisation A Strategy for Action*. London: The Community Security Trust. Retrieved from http://icsr.info/wp-content/uploads/2012/10/1236768491ICSROnlineRadicalisationReport.pdf

182 Hussain, G., & Saltman, D. E. M. (2014). *Jihad Trending: A Comprehensive Analysis of Online Extremism and How to Counter it*. London: Quilliam Foundation. Retrieved from www.quilliamfoundation.org

183 Rogan, H. (2006). *Jihadism Online – A study of how al-Qaida and radical Islamist groups use the Internet for terrorist purposes*. Norwegian Defence Research Establishment. Retrieved from http://rapporter.ffi.no/rapporter/2006/00915.pdf

184 Directorate General For Internal Policies, European Parliament. (2014). *Preventing and countering youth radicalisation in the EU*. Retrieved from http://www.europarl.europa.eu/studies

185 Livingstone, S. (2009). *Children and the Internet: Great expectations, challenging realities*. Cambridge: Polity Press, p.76.

186 Children's Online Privacy Protection Act of 1998, 5 U.S.C. 6501–6505. Retrieved from http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

187 Montgomery, K. C. (2007). *Generation digital: politics, commerce, and childhood in the age of the internet*. Cambridge, Mass.; London: MIT.

sugar and salt (HFSS) raises concerns regarding exposure to unhealthy and potentially harmful behaviours. Concern was also expressed about the widespread online advertising of alcohol products and the impact that such activity has on Irish young people.[188] Such advertising and interactive digital marketing techniques may include SMS, social networking sites, product review websites, wikis, blogs, chat-rooms, advergames, and websites hosting user-generated content such as video, photos and consumer reviews.

The Advertising Standards Authority for Ireland (ASAI) is the independent self-regulatory body for the advertising industry. Its Code of Standards for Advertising, Promotional and Direct Marketing relates to all media, including print, radio, television, cinema, outdoor and the internet. The aim of the ASAI code is to ensure that members' commercial communications are all 'legal, decent, honest and truthful'.[189] In 2009, the code was extended to include digital marketing on advertisers' own websites as well as advertising placed with third-party platforms. In 2013, this was further extended to include advertisers' pages on social media.[190] Commercial communication for on-demand content under the ODAS code must also comply with the relevant provisions for broadcast commercial communication; for instance, the advertising of tobacco and alcohol to minors is prohibited.

Currently, the BAI regulates the advertising of unhealthy foods to children on broadcast media. For non-broadcast media including the internet, the self-regulated ASAI code applies.[191] However, the Irish Heart Foundation believes that the relevant sections of the ASAI code relating to the marketing of food and beverages to children are weak. In contrast to the statutory rules for television advertising that require advance clearance of advertisements, the ASAI only investigates complaints made about potential breaches of the code after the advertisement in question has been seen by the public.

4.3 Policy responses

4.3.1 Age restriction and age verification

Blocking access to restricted content through the use of age verification techniques is one solution that has been proposed by policy makers. Under the AVMSD, services offering material that might seriously impair- under-18s must be restricted by appropriate measures to ensure that children don't gain access.

The UK video-on-demand regulator, ATVOD, classifies adult pornography as restricted material and regulates services located in the UK accordingly. However, given that most adult content sites, including so-called free access 'tube sites', are located outside the UK, the regulator has thus far been powerless to act. In a further measure designed to restrict access to pornography, ATVOD has proposed cutting the flow of revenue to such sites providing free access unless they put in place appropriate age-verification techniques.[192]

The difficulties of implementing an effective age-verification scheme are substantial. Electronic identification (eID) is one of the tools advocated to ensure greater security and safety in carrying out electronic transactions online.[193] The introduction of eID schemes

[188] This was raised in both the submission from the Irish Heart Foundation and material supplied by the Department of Health's Tobacco and Alcohol Control Unit.

[189] Code of Standards for Advertising, Promotional and Direct Marketing, 6th edition. Retrieved from http://www.asai.ie/code.asp

[190] ASAI 33rd Annual Report 2013-14. Retrieved from http://www.asai.ie/news.asp?nid=97

[191] Code of Standards for Advertising, Promotional and Direct Marketing in Ireland. Retrieved from http://www.asai.ie/ASAI%20CODEBOOK_REVISED_2012.pd

[192] Peter Johnson, Chief Executive Officer, ATVOD. Industry standards and collaboration for a safer environment. *Westminster eForum Keynote Seminar: Childhood and the Internet – safety, education and regulation*. 29 January 2014.

[193] E-identification. Retrieved from http://ec.europa.eu/digital-agenda/en/e-identification

has proved complex and challenging. However, one sector in which age verification has been determined to be more effective is in the area of online gambling. A study led by the Oxford Internet Institute is currently seeking to draw lessons from the gambling industry and to explore the nature, efficacy and cost of the measures in place as a basis for applying similar strategies to other kinds of content classified as unsuitable for minors.[194]

An area that has provoked calls for better age verification is underage use of social networking sites. Most popular social networking platforms, such as Facebook, require users to be 13 to sign up for an account. Yet many younger children, sometimes with parental support, are active on social networking sites, having entered a false age to register. In Ireland, some 40% of 11-12 year-olds have a profile on a social networking site, despite age restrictions.[195] Among the potential risks faced by underage users are inadequate privacy protection and inappropriate advertising due to a wrong age being entered. Facebook, in its submission to the group, outlined some of the measures it has applied to prevent underage registration and to identify and remove accounts of those under 13. The Joint Oireachtas Committee in its report also called for greater parental vigilance in the absence of more effective age-verification techniques.

4.3.2 Content classification and rating systems

The use of content classification and ratings systems has also often been advocated as a way of minimising the impact of harmful online content.[196] Rating systems extend the notion of film-like classification to internet content, and build on the success of applying ratings and descriptive labels to video games. A number of systems were developed in the early years of the internet, receiving support from industry and from the European Commission; they were modelled on the implementation of a V-chip for television in the US in the mid 1990s.[197] Such systems enable website creators to provide metadata or labels, in machine-readable form, based on established or recognised classification. Rating systems are integrally linked to filtering tools and are used as the basis for blocking access to any content specified as unsuitable. Early versions were built into browser software (e.g. Internet Explorer) as well as third-party filtering products. However, the lack of take-up by content producers and the fact that most internet content, unlike film and television, is not classified led to systems such as those developed by the Internet Content Rating Association (ICRA) or the Platform for Internet Content Selection (PICS) being abandoned.[198]

An area where classification has proved more successful, and has won wide industry and regulatory support, is video games content. The PEGI (Pan-European Games Information) system was developed by the Interactive Software Federation of Europe, the industry trade association, with the support of the European Commission.[199] It provides a set of standard age classifications and eight content descriptors for violence, fear, sex, drugs, bad language, gambling, discrimination, and whether online gameplay is possible.[200] PEGI is now used throughout Europe, mostly on a voluntary basis, but is required under consumer legislation in the Netherlands and UK. PEGI Online, an addition to the PEGI system,

---

194 Effective Age Verification Techniques: Lessons to be Learnt from the Online Gambling Industry. Oxford Internet Institute. Retrieved from http://www.oii.ox.ac.uk/research/projects/?id=102

195 O'Neill, B. & Dinh, T. (2012). *Social Networking Among Irish 9-16 year olds.* Digital Childhoods Working Paper No. 3. Dublin: Dublin Institute of Technology, Centre for Social and Educational Research.

196 Staksrud, E. & Kirksæther. (2013). Filtering & Content Classification. In B. O'Neill, E. Staksrud & S. McLaughlin (Eds.), *Towards a Better Internet for Children?: Policy Pillars, Players and Paradoxes.* Nordicom.

197 Price, M. E. (1998). *The V-chip debate: content filtering from television to the Internet.* Mahwah, NJ ; London: Lawrence Erlbaum Associates.

198 Archer, P. (2012). 'ICRAfail. A Lesson For the Future'. Retrieved from http://philarcher.org/icra/ICRAfail.pdf

199 See http://www.pegi.info/

200 De Haan, J., van der Hof, S. & Pijpers, R. (2013). Self-regulation. In B. O'Neill, E. Staksrud & S. McLaughlin (Eds.), *Towards a Better Internet for Children? Policy Pillars, Players and Paradoxes.* Nordicom.

applies to online gameplay. It takes the same approach to classification, combined with an online reporting tool and an independent administration, advice and dispute settlement process.[201]

The CEO Coalition for a Better Internet for Kids, established by European Commission Vice-President Neelie Kroes, includes the 'wider use of content classification' as one of its goals.[202] Participating companies have committed to supporting a comprehensive network of content classification to take into account professionally produced content available through apps stores, as well as user-generated content. Through this process, apps stores (e.g. Google Play, the App Store for Apple devices) have implemented processes for classification and certification of apps, with a mechanism for consumers to provide feedback, report an issue or file a complaint about classification. Members of the ICT Coalition[203] and signatories to the European Framework for Safer Mobile Use[204] have made similar commitments for commercially produced content.

Applying classification approaches to user-generated content (UGC) is more of a challenge. UGC falls outside the strict editorial responsibility of platform providers and, under the applicable liability regime for intermediaries, is primarily subject to notice and take-down procedures as well as the terms of service applied by the provider. Content-sharing hosts can also age-restrict content, provide age warnings or limit access to over-18s. Website operators also typically provide mechanisms to report content that violates guidelines as well as a flagging system to facilitate the self-regulation of community content. A further initiative, supported by the CEO Coalition, has been to extend labelling systems to UGC. A project titled 'You Rate It', led by classification bodies in the Netherlands and the UK, NICAM and BBFC respectively, and with participation by the Irish Film Classification Office, has developed a prototype self-rating tool that providers can use for rating.[205] The initiative is still, however, at an early stage of development and will require wider user adoption to be effective.

4.3.3 Filtering and parental controls

Parental control tools or filters are technical solutions to restrict or manage what children may be able to access on the internet. Closely linked to the development of content classification and rating systems, parental controls have long been advocated as a way of assisting parents/guardians to restrict children's access to content that may not be appropriate to their age. Some filters also allow parents to manage the amount of time children spend online or to control the kinds of applications or communications functions used. Filters can be applied at the individual device level by installing or using built-in software on a PC or other connected device. They may also in some instances be applied at the modem or router level, so that filtering is available for devices on a single household internet connection or local area network.

The application of parental controls or filtering in this context needs to carefully distinguished from network level filtering or blocking, typically the solution designed to block access to a blacklist of banned or illegal internet content. Here, we refer only to parental controls that are applied on individual devices or applications, and at the level of the individual household connection.

---

201 See http://www.pegionline.eu/

202 CEO Coalition, Statement of Purpose (2012). Retrieved from http://ec.europa.eu/digital-agenda/en/self-regulation-better-internet-kids

203 http://www.ictcoalition.eu/

204 http://www.gsma.com/gsmaeurope/safer-mobile-use/european-framework/

205 http://www.yourateit.eu/

With wider use of portable connected devices such as tablets and smartphones, and diversification of ways of accessing content online, the application of parental controls has become more complex. Parental control features are integrated in operating systems, such as Android and iOS, but require configuration. Popular applications such as YouTube and Google Search also have built-in safe-mode or parental-lock features. In addition, mobile network operators offer parents control options to monitor their child's mobile-phone usage and the services they access.[206] Some operators provide a filtered service, restricting access to adult content, by default on their pre-pay services.[207]

Take-up of parental controls in Ireland is relatively high. Close to two-thirds or 61% of Irish parents report using parental controls or other means of blocking or filtering some types of websites.[208] This is almost double the European average, placing Ireland in a group of countries that have tended to favour restrictive mediation of young people's internet use.[209] Parents use filters to restrict access to potentially unsuitable content, to limit the amount of time their children spend online, and to monitor their use as well as who their children may be communicating with. Reasons for not using parental controls vary: some believe they are not necessary while others find them too complicated or awkward to set up and manage.[210] There are also contrasting views on the appropriateness and effectiveness of parental controls; some view their use as an intrusion in the child-parent relationship and an infringement on children's privacy.[211] There is also a concern that filters may lull parents into a false sense of security, and that, once they are installed, parents may take no further role in mediating their children's internet use.[212]

4.3.4 UK filtering by ISPs

The introduction of a national initiative on parental controls in the United Kingdom has brought the debate on filtering centre stage. Britain's four largest ISPs – Sky, BT, TalkTalk and Virgin – agreed to offer new customers the option of having filters installed at the point of sign up. The exact nature of the mechanism depends on the provider; it may be either a network-based filter or software downloaded to individual computers.[213] The intention is to create a one-click solution for all connected devices in a household. The parental control products themselves are not new; what is different is that each customer will be asked if they wish to have filters installed or not. Over the course of 2014, this will be extended to all existing subscribers – every subscriber will be given an 'unavoidable' choice as to whether to activate filters or not on their ISP connection.

The objective of the UK initiative is to restrict access by minors to age-inappropriate material. In a speech to the National Society for the Prevention of Cruelty to Children (NSPCC) in 2013, Prime Minister David Cameron argued that online pornography is 'corroding childhood' and distorting young people's view of sex and relationships.[214] The Special Advisor to the Prime Minister, Claire Perry MP, has outlined the aspiration that

206 ICIA (2006). Irish mobile operators Code of Practice for the responsible and secure use of mobile services. Retrieved from http://www.ibec.ie/IBEC/BA.nsf/vPages/Business_Sectors~Telecommunications_and_Internet_Federation~icia-code-of-practice-04-05-2006?OpenDocument

207 Submission from Three Ireland.

208 UPC's Second Report on Ireland's Digital Future (2014) Retrieved from http://www.upc.ie/pdf/UPC_2014_report.pdf

209 Helsper, E. J., Kalmus, V., Hasebrink, U., Sagvari, B. & Haan, J. D. (2013). *Country Classification: Opportunities, Risks, Harm and Parental Mediation.* London, LSE: EU Kids Online.

210 FOSI (2011). Who Needs Parental Controls? A Survey of Awareness, Attitudes, and Use of Online Parental Controls. Washington, DC: Family Online Safety Institute.

211 Staksrud, E. & Kirksæther. *Op. cit.*

212 Byron, T. (2008). Safer Children in a Digital World: The report of the Byron Review. London: DCSF, p.81.

213 http://www.Internetmatters.org/

214 Prime Minister's Office. (2013, July 22). The Internet and pornography: Prime Minister calls for action. Retrieved from https://www.gov.uk/government/speeches/the-Internet-and-pornography-prime-minister-calls-for-action

most UK households with children will opt to have filters turned on.[215] Combined with a proposed code of conduct or a trust mark scheme for family-friendly Wi-Fi in public spaces, the objective is to ensure availability of filtering in all the places that young people are likely to go online.

The UK's approach to ISP-led parental controls and filtering has been criticised as too intrusive on the part of the state with the potential to generate a form of creeping censorship.[216] The approach has also been criticised as being ineffective due to over-blocking of many legitimate, health-related websites whilst allowing other intended targets of filtering through unimpeded.[217] To date, no other European member state has adopted a similar approach though the European Commission strategy maintains support for wider availability and use of parental controls in helping to keep children safe online;[218] Council Conclusions have also echoed this approach.[219]

In the public consultation, respondents were asked if they believed additional measures were required to deal with the accessing by children and young people of content that may be age-inappropriate or harmful for their development. Responses included a range of possible measures including better labelling and classification of content, access controls and age verification techniques and more education for parents. Specifically, with reference to the UK measures for ISP-led filtering – though not a representative sample – a majority, 51% of respondents, stated they were against such an initiative; 28% were in favour of similar measures being made available in Ireland while 21% did not express an opinion. A far higher number of responses in support of an ISP-led filtering initiative were represented among the submissions to the National Parents Council – Primary.

4.3.5 Other regulatory responses

A regulatory response to age-inappropriate content is provided by the example of Germany's youth protection system for the media, comprising a strict set of rules governing audiovisual, broadcast, gaming and online content. As a federal republic, Germany's Kommission für Jugendmedienschutz (KJM) (Commission for Youth Media Protection) acts as a central authority for Germany's sixteen Länder to set standards for the rating of content and monitoring of compliance under Germany's Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting.[220]

KJM exhibits a number of characteristics that are unique to the German system. In the federal system, individual state media authorities are responsible for monitoring and regulating within their area of jurisdiction. KJM, in this instance, acts as a central regulatory authority to ensure consistency across different states and therefore acts on behalf of the relevant media authority within each state or German Land. KJM also operates within a system of 'regulated self-regulation'[221] in which broadcasters and on-demand service providers are permitted to operate without state interference as long as they act in accordance with approved and certified self-regulatory bodies acting for distinct

---

215 Claire Perry MP, Regulation and policy for a safer internet. Westminster eForum Keynote Seminar: Childhood and the Internet – safety, education and regulation. January 29, 2014.

216 Penny, L. (January 3rd, 2014). David Cameron's internet porn filter is the start of censorship creep. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2014/jan/03/david-cameron-internet-porn-filter-censorship-creep

217 BBC News. (2014, January 31). UK to act on wrongly-blocked sites. *BBC News*. Retrieved from http://www.bbc.com/news/technology-25962555

218 European Commission. (2012). *Communication on The European Strategy for a Better Internet for Children COM(2012) 196*. Brussels: European Commission. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDF

219 (2012). *Council conclusions on the European strategy for a Better Internet for Children*. Brussels: Council of the European Union. Retrieved from http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/educ/133824.pdf

220 https://www.blm.de/de/pub/die_blm/organe/kjm.cfm

221 Schulz, W., & Held, T. (2001). *Regulated Self–Regulation as a Form of Modern Government*. Hamburg: Hans Bredow Institute for Media Research at the University of Hamburg.

parts of the media industry. The KJM, in this instance, is responsible for certifying those bodies – the Voluntary Self-Regulation of Television (Freiwillige Selbstkontrolle Fernsehen, FSF) and the Voluntary Self-Regulation of Multimedia Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, FSM).

While voluntary self-regulatory bodies such as FSF and FSM are responsible for developing codes of conduct and ensuring their members comply with protection of minors guidelines, the KJM acts in the public interest and is the public face for matters impacting on children in broadcast and on-demand services. Its central office handles complaints and requests from media users and monitors broadcasts and telemedia services. It also contributes to policy on problematic aspects of content for young people through expert assessments, contributions to judicial processes, media relations on areas of children and media and evaluates technical measures for the protection of minors in telemedia and broadcasting services. Its reach also extends to the internet through its auxiliary agency jugendschutz.net, set up in 1997 by the state media authorities to deal with problematic online content and has the function of both monitoring the internet and responding to complaints.

The German Youth Protection system is embedded within a distinct cultural and historical milieu and is less directly applicable to the Irish context. Its implementation under Irish law would also be difficult. Nevertheless, its approach to dealing with issues of age-inappropriate or potentially harmful content is one that should be the kept under review.

4.4 Recommendations

Developing recommendations in the area of age inappropriate or potentially harmful content proved to be one of the most difficult tasks faced by the group.

On the one hand, access by children to content that is by any standards offensive, age-inappropriate or potentially harmful gives rise to concerns for their welfare and development. As evidenced in many submissions to the group, this is something that clearly is a cause of anxiety for many parents and guardians. An instinctive response is to think of ways of applying regulatory models derived from the traditional media environment. Just as age-based ratings and standards apply to film and television content, it might be argued, similar standards should apply in the online world. Yet, this is rendered extremely difficult due to the disaggregated nature of the internet and the constraints this places on any single governmental actor by setting limits to its governance remit. Government action may also not be desirable or constitutionally possible in any case in light of the overriding importance of freedom of expression and freedom of access to information.

One option, therefore, is adoption of industry-wide support for ISP-led parental controls, similar to the UK measures. While the group did not have a consensus on this topic, the majority view was that such an approach is neither warranted nor appropriate in the Irish context. In the view of the group, the scheme proposed in the UK is still at an early stage of implementation and awaits full assessment of its effectiveness. Also, the fact that there is already high usage of parental control filters in the Irish market suggests that there are already solutions available to parents and that those who wish to use them already do so. One area where the group felt there was a gap in the market is in relation to modem or router-based filtering products. Responding to parental requests for more accessible, one-click solutions, this is an area where internet service providers could offer greater support for filtering solutions that are effective for all devices linked to a single internet connection. However, in the view of most members of the group, the adoption of parental controls was a matter for individual subscribers and households to determine according

to their own needs. There also remains an important role for education and awareness-raising about the role that parental controls play in a digital parenting context, including examination of limitations to their use.

The other overriding consideration for the group in relation to governance and age-appropriateness of content concerned issues related to the rights of internet users and defending freedom of expression online. Commitment to the values of a free and open internet are of such fundamental importance that any intervention by the State or public agencies, beyond the scope of clear illegality, must be carefully weighed. Striking the balance between the needs to protect vulnerable users, such as children and young people, and to support in the public interest an open and self-regulating global internet community therefore requires careful mediation and the cooperation of all involved. Ultimately, the conclusion of the group was that the interests of citizens, including children and young people, are best served by supporting multi-stakeholder collaboration and dialogue through initiatives such as the National Council for Child Internet Safety.

That said, the group was also of the view that some progress could be made in developing the regulatory capacity of the State to deal with content standards and oversight of the self-regulatory processes that operate across the expanding communications environment. In anticipation of a future reconfiguration of regulation at the European level to take account of increasing convergence in the provision of audiovisual media services, we recommend that the system chosen for the implementation of the AVMSD be amended, with ODAS, the on-demand audiovisual services entity, continuing to exist but transferred from the Irish Business and Employers Confederation (IBEC), where it is convened as a self-regulatory body, to the Broadcasting Authority of Ireland with Statutory recognition being given to this new arrangement. This is not to imply that ODAS, or the BAI, functions as an internet regulator. Given that the remit of ODAS extends only to on-demand audiovisual provision within Ireland, it has no impact on internet content originating beyond the jurisdiction of the state. However, developing capacity within a national regulatory authority in areas such as oversight of commercial communications, content classification and in monitoring developments in protection – in conjunction with equivalent agencies in other member states – would be advantageous and would lend greater coherence to national policy in this area.

4.4.1 Awareness, availability and use of parental controls and filters

Given the diversity of ways of going online and the pervasive nature of internet content, parental controls are now a vital part of negotiating the online world. Internet service providers (ISPs) and mobile network operators (MNOs) can play a crucial role in providing access to filtering solutions and providing education and support about their use. Therefore, we recommend that ISPs and MNOs should be encouraged to include this service as a core part of their consumer offering.

Filtering in public Wi-Fi access points or hotspots is another area for consideration. While ultimately a decision for the provider concerned, taking into account the likelihood of children using Wi-Fi in that location for internet access, we recommend the development of a 'family-friendly' logo to designate the use of filtering of adult or other age-inappropriate content for public Wi-Fi access points. Terms of use should be prominently displayed at the point of access, stating clearly whether a service is a filtered one or not.

Campaigns to make parents aware of the parental controls available should be also developed as a collaborative initiative of National Parent Councils, youth representative organisations, children's charities and industry. This is not to advocate parental controls as the sole solution for internet safety; education is required to emphasise that they are not complete solutions but have a role to play in an overall digital parenting context.

Awareness-raising is also needed to provide authoritative guidance and support targeted at specific groups of users likely to access potentially harmful content, e.g. teenage girls who may access pro-anorexia content, younger adolescents who may come across sexual or pornographic content, vulnerable children or those with psychological difficulties, etc. More promotion is also needed for the range of current labelling systems, such as PEGI (Pan-European Games Information) and PEGI-Online for gaming content, as well as other emerging rating systems for online content.

4.4.2 Developing regulatory capacity in for on-demand content through ODAS

As discussed, responsibility for ODAS, the On-Demand Audiovisual Media Services group, should be assigned to the BAI. The functions of ODAS will not fundamentally change. However, it should monitor the application of codes of conduct for commercial communication and marketing on social media and online platforms. The BAI and DCENR should also monitor the impact of measures to regulate restricted on-demand content in other jurisdictions, including the application of age-verification systems.

Chapter 5: Conclusion

5.1 Developing safer and better internet strategies

The task of the Internet Content Governance Advisory Group was to assess the range of existing provision for safer and better internet strategies, taking into account the regulatory, legislative and policy responses that have been developed in response to pervasive use of the internet by all citizens, but especially by children and young people. The internet has become a central platform for media consumption, creation and dissemination of content, and is used by citizens on a daily basis. Social media, in particular, has brought the capacity to connect and to share content to everyone, creating profound opportunities but also disruptive changes to communication and information dissemination.

A focus for the group has been on the twin areas of *content* and *conduct*-related risks and harms brought about by the increasing use and prominence of online communications and social media in particular. Recent attention in Ireland and internationally to problems of cyberbullying and harassment as well as the accessing of content that may be unsuitable for minors has given rise to much media debate and policy attention. Our approach in reviewing responses by the State to such problems has been cautious, mindful that these problems are not new and that a range of measures already exist in this area to tackle some of the most urgent problems. We were concerned to ensure that any proposals made by the group did not impact negatively on the effectiveness of existing provision. At the same time, we were conscious that the low level of awareness of some existing arrangements is a serious impediment. In part, this has to do with the speed and pace at which the internet has evolved and become an issue for all citizens, and particularly so for parents and guardians who must take on internet safety as part of parental responsibility.

It was also apparent that there is fragmentation among the diverse actors and agencies responsible for internet safety. It is clear that, at different points over the last decade, consideration of the internet was added to the responsibilities of government departments, regulatory agencies and other bodies as demanded by the situation at the time. Some legislation predates the internet by many decades; in other instances, more recent legislation has had to take account of emerging developments in the communications arena that have not fully taken shape. The challenges in establishing a single or coordinating framework for managing internet-related aspects of content are therefore considerable.

Ireland was an early mover in responding to the challenges of regulation in the interests of better internet safety and protection. The Working Group on Illegal and Harmful Uses of the Internet in 1998 set out a blueprint for industry cooperation and self-regulation that has, by and large, stood the test of time. However, this was developed some six years before Facebook was established and long before internet use became a mass phenomenon for Irish citizens. Now, with near-universal use of the internet in every dimension of daily life, and rapidly expanding new modes of going online, there is a need for increased capacity, and more coherence, in governmental responses to internet safety, engagement and development.

5.2 Summary of recommendations

Our recommendations fall under three main headings:

Institutional/Structural Recommendations

We recommend a number of structural and administrative changes affecting arrangements supporting internet safety. This involves a reconfiguration of the various components of the State's engagement and that of industry and civic society groups, in order to achieve better coordination, better use of existing resources and better public awareness of solutions in the area of internet safety.

A revised role for the Office for Internet Safety

- We recommend that that the OiS should be reconfigured to deal exclusively with issues of law enforcement and illegal online content. It may be retitled or have its role reduced to an administrative function. It should be given clear terms of reference clarifying its role in providing oversight of the system of self-regulation for illegal internet content.
- The OiS should include within its terms of reference an assessment of the industry self-regulatory code of practice.
- The OiS should include within its remit oversight of the current voluntary blocking of illegal internet content undertaken by mobile network operators.

The National Council for Child Internet Safety

- We recommend that the Internet Safety Advisory Committee be expanded and reconfigured as the National Council for Child Internet Safety. This council should act as the primary multi-stakeholder forum for internet safety strategy in Ireland. It should include representation from industry, relevant government departments, public bodies, civil society including youth representation and child protection interests.
- Responsibility for the secretariat function for the council should be assigned to the Department of Children and Youth Affairs. The council should be chaired at ministerial or junior ministerial level to ensure that its work receives the appropriate level of political support.
- The council should act as coordinator for the Safer Internet Ireland project, in particular its awareness-raising, education and helpline functions.
- The council should establish working groups to deal separately with issues of research, education and industry safety implementation. Working groups reporting to the council should guide its work with the most up-to-date information available, informed by international best practice.
- The council should seek to harness innovative technology, tools and educational approaches in promoting internet safety and standards of digital citizenship, advising all relevant stakeholder groups with regard to emerging risks and good practices in dealing with online abuse.
- The council should foster close co-operation between stakeholders and in particular ensure the effectiveness of industry measures, as envisaged in Objective 3.19 of the National Policy Framework for Children and Young People. In particular, the participation on the council of leading internet companies located in Ireland and representative industry associations should be encouraged.

- The council should collaborate with the implementation group for the Anti-Bullying Action Plan to coordinate stakeholder responses to all internet-related dimensions of bullying and abuse, including should commission research on the most effective ways to counteract bullying and harassment and on the impact of exposure by minors to age-inappropriate content.

The Safer Internet Ireland Centre (SIIC)

- We recommend that the Safer Internet Ireland project, currently co-financed by the European Commission, be enhanced to act as the Safer Internet Ireland Centre (SIIC). While it is envisaged that resourcing will continue to be available through the Connecting Europe Facility, it is important that government ensures that this vital public service is fully resourced.
- The SIIC should operate through a common online platform, and brand and offer a helpline, educational resource and awareness-raising function for children and young people, for teachers and educators, and for parents. It should act as a one-stop portal designed to address the likely volume of enquires, aggregating available support content and serve as a directory/information resource for the general public.
- Oversight of the SIIC should be undertaken by the National Council for Child Internet Safety, with advisory input as required from government departments such as the Departments of Communications, Energy and Natural Resources (DCENR), Education and Science (DES) and Justice and Equality (DJE).
- The SIIC should:
  - compile resources of best practices in dealing with online abuse and harassment for parents, teachers and young people;
  - plan and direct a national awareness campaign on effective measures to deal with the reporting cyberbullying and online abuse;
  - provide guidance to schools on incorporating in their anti-bullying policies best practice in relation to social media and online communication;
  - work 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;
  - promote the Hotline.ie services for reporting illegal content, including racist speech and incitement to hatred.

Legislative Measures

In assessing legislative provision for electronic communications, we are aware of the ongoing review of European regulation of audiovisual media and the need for legislation to address new converging modes of delivery of services. In addition, negotiation of a new Regulation on Data Protection will establish new procedures and structures at a European level for dealing with data processing and privacy of personal information. As such, any modification to existing broadcasting or data protection legislation would be premature.

The Law Reform Commission of legislation is also undertaking a comprehensive review of legislation relating to bullying and harassment, including cyberbullying, and accordingly, the group does not make any recommendation in relation to the Non-Fatal Offences against the Person Act, 1997. As a general principle, we support the position adopted by the Anti-Bullying Working Group that criminalising cyberbullying offences for minors is not the way to proceed.

However, we do recommend closing the gap that has been identified in the legislation in order to strengthen the capacity of law enforcement and the courts to deal with online abuse.

We, therefore, recommend the amendment of the Communications Regulation (Amendment) Act 2007 to include 'electronic communications' within the definition of measures dealing with the 'sending of messages which are grossly offensive, indecent, obscene or menacing'. Further, we advise that the Minister for Communications bring to cabinet the recommendation that the Minister for Justice, in conjunction with the Attorney General and the High Court Rules Committee, establish a review of the suitability of current non-party discovery and disclosure rules of court, to bring current court discovery and disclosure processes in line with societal and technological norms.

Administrative/Policy Questions

Internet content governance

Responsibility for legislation and policy in relation to internet governance lies principally with the Department of Communications, Energy and Natural Resources and in the following we recommend consolidating this role with formal assignment of responsibility, alongside the formation of a cross-departmental group and the development of a high level policy framework to address emerging issues in the audiovisual field.

- We recommend that DCENR be formally charged with coordinating internet content policy at government level in addition to its extant roles in dealing with these issues at an international level.
- We also recommend the formation of a standing Inter-Departmental Committee to cover all aspects of internet governance.
- The Department should take the lead in developing a high level media policy framework, dealing with the effects of technological change on media in general, and specifically on audiovisual and online media, including an on-going review of best/new practices in European and international jurisdictions that may help address the issue of availability of age-inappropriate content regarding minors.

On-Demand Audiovisual Media Services

We believe that transferring responsibility for oversight of the operation of the code of practice for on-demand service providers in Ireland to the BAI will strengthen the capacity of the state to engage with issues of online content. While this does not entail formal regulation of internet content providers, it marks a shift from a purely self-regulatory approach to one that is more appropriately co-regulatory.

- Responsibility for the implementation of the provisions of the Audiovisual Media Services Directive, presently vested in the On-Demand Audiovisual Media Services entity (or ODAS), should be assigned to the Broadcasting Authority of Ireland.
- The Broadcasting Authority of Ireland should also monitor the impact of proposals to regulate restricted on-demand content in other jurisdictions, including the UK.

The group has considered a wide range of administrative and policy issues of a nonlegislative nature in the two areas of conduct and content related risks and harms. As such, we make the following recommendations to advance policy implementation in two key areas:

Dealing with cyberbullying and harassment

- An inter-agency working group should be established by the Department of Education and Skills in conjunction with the National Council for Curriculum and Assessment to identify appropriate mechanisms to ensure that internet safety and digital literacy skills are taught as a core element of the curriculum at both primary and post-primary levels.
- Supports for schools on the implementation of the SPHE programme as part of the Primary and Junior Cycle curricula need to be updated to promote a positive, safer, and more effective use of technology by children.
- Further support should be given to training directed at parents to make them aware of the risks of cyberbullying and how to deal with it. Training initiatives such as those developed by the National Parents' Council, should be further expanded and resourced.
- We also recommend that the Garda Síochána Schools "Respectful Online Communication" and "Connect with Respect" programmes, which deal with cyberbullying among other topics, should be extended to include an equivalent resource for parents to explain the role of policing in relation to online abuse and harassment is also recommended.

Dealing with accessing of age-inappropriate content

- Internet service providers (ISPs) and mobile network operators (MNOs) should be encouraged to include parental control products and services as part of their consumer offering. In particular, ISPs and MNOs should provide advice and support about how to configure the different filtering solutions available, including those for portable internet-enabled devices, to assist parents in managing children and young people's internet access.
- An awareness-raising campaign to encourage parents to make more use of the array of parental controls should be developed as a collaborative initiative of National Parent Councils, youth representative organisations, children's charities and industry. Awareness messages about parental controls should emphasise that they are not complete solutions but have a role to play in an overall digital parenting context.
- The application of filtering on public Wi-Fi access points or hotspots is ultimately a decision for the provider concerned, taking into account the likelihood of children using Wi-Fi in that location for internet access. Terms of use should be prominently displayed at the point of access, stating clearly whether a service is a filtered one or not. A 'family-friendly' logo to designate the use of filtering of adult or other age-inappropriate content for public Wi-Fi access points should be developed.
- Awareness-raising by relevant agencies and by industry should provide authoritative guidance and support targeted at specific groups of users likely to access potentially harmful content, e.g. teenage girls who may access pro-anorexia content, younger adolescents who may come across sexual or pornographic content, vulnerable children or those with psychological difficulties, etc.
- Awareness-raising should also include the development of specific resources targeted at parents to make them aware of the current labelling systems, such as PEGI (Pan-European Games Information) and PEGI-Online for gaming content, as well as other emerging rating systems for online content.

5.3 Future policy

The internet continues to evolve at a rapid pace, with increasing international attention given to internet governance and related areas of promoting digital inclusion, enhancing digital skills and protection of users. Internet safety has been a concern of policymakers since the earliest days of the World Wide Web. Measures to enhance the safety of users and to protect children's welfare online have focused on, first, a robust law-enforcement response to illegal content and activity online, and secondly, a range of collaboratively designed safeguards and educational initiatives intended to empower users to better protect themselves. Initial approaches to safety implementation, drawing on some of the lessons from the traditional media environment, were designed in a pre-Web 2.0 era. With the rapid take-up of social media on a global scale, new challenges arise due to the absence of formal regulation and the predominance of self-regulating approaches to the multiple forms of social interaction and online communities in which people now participate.

The test of policy now and in the future will be to sustain the principle that what is illegal in the offline world is also illegal online, just as recognising that what is harmful or injurious to young people will also be so on the internet. The objectives of the recommendations outlined in this report and in the deliberations of the Internet Content Governance Advisory Group have been to strengthen the capacity of the State to monitor, respond and collaboratively engage with all relevant stakeholders in promoting better internet use. This entails a series of incremental steps, building on what has been a solid foundation but also enhancing the coordination of policymaking and the delivery of support to all citizens, not least those most in need of education and better opportunities.

Appendix I: Organisations and Individuals who submitted to the Public Consultation

Anchor Youth Project

Ann Costello

Anti-Bullying Campaign Tools for Teachers

Aodhán Ó Ríordáin TD

Athena Media

BodyWhys

Chantal Doody

Child Watch

Ciaran Lynch, T.D. and Dr Margaret O'Keeffe

Cllr Paul O'Shea

Cllr Tom Shortt

Comhairle na nÓg County Galway

Cyber Safety Advice

Daniel Buckley

Digital Garden Limited

Digital Rights Ireland

Digital Training Institute

Éamonn Ó Gribín

Eileen Soraghan

Eircom

Facebook

Foróige

Franchise Direct

Iarla Molloy

INDIE (Irish Network for Digital Inclusion and Engagement)

Internet Service Providers Association of Ireland

Irish Heart Foundation

ISPCC

Jake Doran

Jim Phelan

John Goldbach

John Lyons TD

John Sunderland

Katie O'Sullivan

m9Security Solutions

Martha Luff

Mary McGilloway

NASC – the Irish Immigrant Support Centre

National Association of Principals and Deputy Principals (NAPD)

National Parents Council

Oisin Hurley

P. Shelton

Pat Roche

Paul Roche

Psych Services

Richard Humphreys SC

Seamus Lennon

Senator Jillian van Turnhout

Sky

Stephen Kelly

The Journal.ie

Three Ireland

Transformative Psychotherapy, LLC

TwoTen

UPC

Veronica Martin

Webwise Youth Advisory Panel

William Fagan

Youth Work Ireland

Appendix II: List of Bi-lateral Meetings with Government Departments and Other Bodies

Date	Organisation
4th March 2014	Department of Education and Skills
6th March 2014	Office for Internet Safety, Department of Justice and Equality
6th March 2014	Law Reform Commission
20th March 2014	Facebook
26th March 2014	Department of Children and Youth Affairs
26th March 2014	Google
1st April 2014	Twitter
11th April 2014	Department of Health
2nd May 2014	Three Ireland
12th May 2014	Office of the Children's Ombudsman
12th May 2014	Office for Internet Safety, Department of Justice and Equality

Appendix III: Meetings of the Internet Content Governance Advisory Group

Meeting	Date
1.	18th December 2013
2.	6th January 2014
3.	20th January 2014
4.	22nd January 2014
5.	6th February 2014
6.	20th February 2014
7.	6th March 2014
8.	3rd April 2014
9.	11th April 2014
10.	25th April 2014
11.	8th May 2014
12.	14th May 2014
13.	26th May 2014
14.	29th May 2014