

**Opening Statement by Dr Mary Aiken, Hon. Professor Department of Law and
Criminology, University of East London
to the Oireachtas Committee on Justice and Equality.**

Wednesday, 16th October 2019

I am grateful for the committee's invitation to speak on the topic of online harassment, harmful communications and related offences. My understanding is that the committee wishes to examine the nature and extent of the following problems; cyberbullying, harassment, stalking, 'revenge porn' and other forms of harmful communications; along with international best practice for addressing these problems; whether self-regulation of harmful communications by social media companies is the best approach; or whether new laws are necessary to cover such activities, and what forms such laws should take. Notwithstanding the remit of this committee, the challenge is that in Cyberspace everything is connected. Therefore, laws that attempt to address cyberbullying will arguably be ineffective in the absence of addressing a more comprehensive range of 'Online Harms.' The UK Online Harms White paper¹ offers a thorough treatment of these issues, noting that;

"Illegal and unacceptable content and activity is widespread online, and UK users are concerned about what they see and experience on the internet. The prevalence of the most serious illegal content and activity, which threatens our national security or the physical safety of children, is unacceptable. Online platforms can be a tool for abuse and bullying, and they can be used to undermine our democratic values and debate. The impact of harmful content and activity can be particularly damaging for children, and there are growing concerns about the potential impact on their mental health and wellbeing.... the internet can be used to harass, bully or intimidate, especially people in vulnerable groups or in public life. Young adults or children may be exposed to harmful content that relates, for example, to self-harm or suicide. These experiences can have serious psychological and emotional impact. There are also emerging challenges about designed addiction to some digital services and excessive screen time."

Notably, the UK approach does not focus exclusively on fragmented aspects of harm, rather they are considering a broad range of harms simultaneously; online anonymous abuse, child sexual exploitation and abuse, harassment and intimidation directed at those in public life, cyberbullying, violence online, designed addiction, underage sharing of sexual imagery, self-harm and suicide. The point being connectivity, there is a relationship between cyberbullying, self-esteem, and self-harm², there is also a relationship between 'sexting'³ images, harassment, online coercion and extortion⁴.

Many countries are in the process of developing new regulatory approaches to tackle online harms. However, none has as yet established a regulatory framework that tackles the connected

¹ UK Online Harms White paper: <https://www.gov.uk/government/consultations/online-harms-white-paper>

² Hinduja, S., & Patchin, J.W. (2010). Bullying, cyberbullying, and suicide. Archives of suicide research : official journal of the International Academy for Suicide Research, 14 3, 206-21 .

³ Self-produced content is part of the wider phenomenon of user-generated content. Self-produced images are also referred to as 'sexting', that is, 'the sending of sexually explicit texts and pictures by cellphone' (Oxford English Dictionary)

⁴ Europol: Online sexual coercion and extortion of children: <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation/online-sexual-coercion-and-extortion-of-children>

range of online harms - the UK will be the first country to do this. I have advised the UK Department for Digital, Culture, Media and Sport on the role of technology in online harm, significant progress has been made. Unfortunately, Ireland an important hub for technology companies should be demonstrating cyber leadership, but has made little or no progress to date despite numerous investigations and reports (Ref: Appendix A)

Technology is new, fascinating; it has a pervasive, profound impact on humans⁵ and a highly seductive momentum. It has revolutionised access to knowledge, education and social reform. Nevertheless, unfettered it has also exploited the vulnerabilities of our children. The influence of the internet and social media is not an abstract concept. Its impact is not virtual; it impacts real lives in the real world.⁶

Monetising harm by designing intelligent algorithms to promote extreme content, and harvest dollars from a child in the 'attention economy'⁷ is not about celebrating access; it is about exploitation. In the bricks and mortar world, we have recognised for centuries that defending freedom for adults to speak and express opinions does not mean giving adults a licence to exploit and harm children.

I passed an Eason's store on the way here. I didn't see any glossy magazines on the lower shelves promoting self-harm, DIY suicide or anorexia, freely available to children beside comics. It is a repugnant idea of course. But this is the reality of the Internet.

We have been here before. We have seen the damage that is done when commercial interests are allowed to exploit vulnerability and addiction to operate without restraint. We have seen it with Big Tobacco, we have seen it more recently with the Opioid crisis.

We see common themes. Wilful and deliberate exploitation and obfuscation, decisions made behind closed doors that either deliberately ignores evidence of harm, or tries to make it someone else's problem. Denial of responsibility. Victim blaming. Moreover while adults debate, posture and play 'pass the blame parcel,' the social technology industry keeps thriving, money keeps flowing, and the online harm continues.

In deliberating the broad area of online harm, we must ask ourselves Who, What, & When?

- Who is being harmed? Who sought to exploit that harm - by designing clever code to profit from it, wilfully ignore its harmful effect or actively denying responsibility for it?
- What is the harm, what real lives are being damaged? What are the consequences of doing nothing?
- When did internet stakeholders become aware of the damage being caused to children? When did we all do something about it?

⁵ Yan, Z. (2012) Encyclopedia of cyber behaviour. IGI Global. <http://www.amazon.com/Encyclopedia-Cyber-Behaviour-Zheng-Yan/dp/1466603151>.

⁶ Life In Cyberspace (Aiken, 2018) <https://www.eib.org/en/essays/life-in-cyberspace>

⁷ Blind Spot: The Attention Economy and the Law (Wu, 2017)

https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=3030&context=faculty_scholarship

In 2014, I raised some of these issues in the report of the Internet Content Governance Advisory Group.⁸ I also advised the Law Reform Commission, whose report “Harmful communications and digital safety⁹” was published some three years ago. In the intervening five years thousands more children have been unnecessarily exposed to repugnant, harmful, toxic and life-damaging material.

This must stop, it demeans all of us.

The Internet was designed on the premise that all users are equal – this is not the case, some are more vulnerable than others, and children are particularly vulnerable.¹⁰ Our challenge as a society is to “help shape an Internet that is open and vibrant but also protects its users from harm.”¹¹

The Irish Constitution (Article 40.3)¹² requires the state, and organs of the state, to protect and vindicate as best it can from unjust attack. Article 42A affords additional rights “the State recognises and affirms the natural and imprescriptible rights of all children and shall, as far as practicable, by its laws protect and vindicate those rights” Exposing Irish children to a range of online harms is a fundamental breach of their constitutional rights.

Our challenge as policymakers is not to engage in determined myopia and deliberate fragmentation strategies, or to allow commercial stakeholders to perpetuate skilful deflection and obfuscation strategies, but to urgently develop a new system of accountability, legislative and statutory instruments and oversight, that will replace the current failed model of self-regulation. A new Irish regulatory framework regarding online harm is urgently required, one that will make clear the technology industry’s responsibility to protect Irish users, particularly our children, online.

Biography

Cyberpsychologist Dr Mary Aiken is an Honorary Professor in the Department of Law and Criminology at the University of East London, Academic Advisor to Europol's European Cyber Crime Centre (EC3), member of Medico-Legal Society of Ireland, International Affiliate Member of the American Psychological Association (APA), Fellow of the Society for Chartered IT Professionals International Global Fellow at the Washington DC Wilson Center and a member of the INTERPOL Specialists Group for Crimes against Children.

Dr Aiken has served as an Adjunct Associate Professor at University College Dublin, Geary Institute for Public Policy, and as a lecturer in Criminology and Research Fellow at the School of Law, Middlesex University. She is the former Director of the Royal College of Surgeons Cyberpsychology Research Centre. In 2014 Dr Aiken was inaugurated into SameShield an

⁸ O’Neill, B., Aiken, M.P., Caffrey, M., Carthy, J., Lupton, R., Lynch, A. & O’Sullivan, K. (2014). Report of the Internet Content Governance Advisory Group. Department of Communications, Energy and Natural Resources, Ireland. <https://www.dccae.gov.ie/en-ie/communications/publications/Pages/Internet-Content-Governance-Advisory-Group-Report.aspx>

⁹ Law Reform Commission report ‘Harmful communications and digital safety’ (2016) <https://publications.lawreform.ie/Portal/External/en-GB/RecordView/Index/37669>

¹⁰ Aiken, M. P. (2016). *The Cyber Effect*. New York. Random House, Spiegel & Grau.

¹¹ UK Online Harms White paper: <https://www.gov.uk/government/consultations/online-harms-white-paper>

¹² Constitution of Ireland <http://www.irishstatutebook.ie/eli/cons/en/html>

organisation that honours women’s leadership in traditionally closed professions. In 2016 she was named as one of the top 50 most inspiring women in technology in Europe. In 2017 she was inducted into the Infosecurity Europe Hall of Fame, in recognition of her contribution to the information and cybersecurity sector.

Appendix A.

Timeline of Government Action on Online Safety for Children

- 2013: The Internet Content Advisory Group established by Department of Communications, Energy and Natural Resources in December 2013 to address internet governance including sharing and accessing content online.
- 2014: The Department of Communications publishes the Report of the Internet Content Governance Advisory Group. The report highlights legal but age inappropriate harmful content online and recommends the establishment of a National Council for Child Internet Safety.
- 2014: Submissions are invited from all interested parties on the Law Reform Commission's Issues Paper on 'Cyber-crime affecting personal safety, privacy and reputation including cyber-bullying'.
- 2016: The Law Reform Commission (LRC) publish its Report on Harmful Communications and Digital Safety. The Report recommends that harmful communications online be regulated by law. A draft Harmful Communications and Digital Safety Bill is appended to the Report. The LRC recommend that the Office of a Digital Safety Commissioner of Ireland should be established on a statutory basis to promote digital and online safety and to oversee and regulate a system of “take down” orders for harmful digital communications.
- 2017: The Harmful Communications and Digital Safety Bill 2017 is introduced in the Dáil. The Bill has remained at second stage in Dáil Éireann since January 2017 and has not been progressed. This Bill does not propose the establishment of the office of a Digital Safety Commissioner.

Jan 2018

The Harassment, Harmful Communications and Related Offences Bill 2017 is introduced in Dáil Éireann by Deputy Howlin. The Bill has remained at third stage in Dáil Éireann since January 2018. The Bill, like the Harmful Communications Bill, seeks to create an offence of harassment online and enacts many of the recommendations set out in the LRC Report. However, as with the 2017 Bill, it does not establish the office of a Digital Safety Commissioner.

March 2018

The Joint Committee on Children and Youth Affairs publishes its Report on Cyber Security for Children and Young Adults. The Report of the Joint Committee

recommends that an Office of a Digital Safety Commissioner should be established and that it should have particular regard to ensuring that Children and Young People, who are some of the most vulnerable online users, are protected.

Nov 2018

In November 2018, the revised Audiovisual Media Services Directive (AVMSD) was adopted by the Council of Europe on 6 November 2018. By 19 September 2020, Ireland is required to regulate video sharing platform services (for example, Facebook and Instagram) so that minors are protected from harmful content or content which impairs their physical, mental or moral development. The Directive recommends that for the purposes of the protection of minors, the most harmful content should be subject to the strictest access control measures. If Ireland fails to implement the Directive in our national legislation, or fails to fully transpose the Directive, it will be subject to the EU Commission's infringement procedures.

Dec 2018

Senator Joan Freeman and Associate Professor Mary Aiken introduces the Children's Digital Protection Bill 2018 which seeks to regulate legal but age-inappropriate content by way of takedown enforcement procedure. Harmful content is described in section 3(2) of the Children's Digital Protection Bill 2018 as content containing encouragement and incitement to suicide and encouragement of prolonged nutritional deprivation that would have the effect of exposing a person to risk of death or endangering health.

March 2019

Minister Richard Bruton announces proposed legislation, the Online Safety Act, which will improve online safety and ensure that children can be protected online. The proposed legislation, which has yet to be published, is said to regulate serious cyberbullying, humiliation and harassment; material that promotes self-harm or suicide; and material that encourages nutritional deprivation, that can damage health or that can expose a person to the risk of death.

May 2019

Minister Charlie Flanagan secures government approval for amendments to the Harassment, Harmful Communications and Related Offences Bill 2017. The proposed Government amendment is to add in the offence of "upskirting".. This strategy appears to lack consistency given the Department of Communications proposed an omnibus Online Safety Bill two months previously.

Oct 2019

The Children's Digital Protection Bill 2018 is to take third and fourth stage in Seanad Éireann.

Sept 2020

All EU member states are required to transpose the provisions of the AVMS Directive regarding online harms.