

Opening Statement by Professor Mary Aiken to the Oireachtas Joint Committee on Tourism, Culture, Arts, Sport and Media, Wednesday, 2nd February 2022 from 13:30 – 14:55 virtually through Microsoft Teams.

First of all, I would like to thank the Joint Committee on Tourism, Culture, Arts, Sport and Media for the invitation to discuss online disinformation¹ and media literacy² (definitions in footnotes). Whereas a number of online harms have been specified and defined in the Irish Online Safety and Media Regulation Bill 2022, online disinformation is currently not referenced in the proposed legislation.

In May 2020 the Draft UK Online Safety Bill provided for the establishment of an Advisory committee on disinformation and misinformation.³ Subsequently, the House of Lords and House of Commons Joint Committee on the Draft Online Safety Bill (December 2021) features an extensive consideration of online disinformation covering topics ranging from vaccine hesitancy to integrity of elections. The joint report outlines that the UK Government aims to tackle the problem of disinformation through strengthened media literacy, and includes a requirement for Ofcom the UK's communications regulator to establish an advisory committee, however, the report also notes that "the viral spread of misinformation and disinformation poses a serious threat to societies around the world" and that media literacy is not a standalone solution.⁴ I agree, particularly regarding the establishment of an advisory committee.

The reason I reference the UK Online Safety Bill is that as a cyber behavioural scientist I have worked closely with the UK Government for a number of years, specifically the Department for Digital, Culture, Media & Sport (DCMS) in the area of online harms. I have also contributed to symposiums and reports regarding the EU Audiovisual Media Services Directive (AVMSD).⁵

For the purposes of informing Irish legislative or indeed any other initiatives to counter online harms, such as online disinformation, I would like to highlight the following points to the committee;

1. Requirement to scope the problem space

Rather than consideration of online harms on an ad hoc basis, I would recommend a research initiative to create an Irish taxonomy of online harms, this would create context for the consideration of any specific harm such as online disinformation. I refer the committee to our report "Research on the Protection on Minors" which was commissioned by Ofcom, the UK regulator for online harms. I was co-lead on this research and report, see below our classification of risk of online harm which was

¹ European Commission: Tackling Online Disinformation the EU describes disinformation as follows; 'verifiably false or misleading information created, presented and disseminated for economic gain or to intentionally deceive the public'. The spread of both disinformation and misinformation particularly mediated by technology, may have a range of consequences, such as threatening our democracies, polarising debates, and putting the health, security and environment of EU citizens at risk <https://digital-strategy.ec.europa.eu/en/policies/online-disinformation#:~:text=Disinformation%20is%20verifiably%20false%20or,believes%20it%20to%20be%20true>.

² Council of Europe: Media and Information Literacy - according to the Council of Europe "Media and information literacy provides the backbone to understanding media and the role of media in our society," it also provides some of the essential skills necessary for critical thinking, analysis, self-expression and creativity – all necessary skills in a democratic society <https://www.coe.int/en/web/digital-citizenship-education/media-and-information-literacy>

³ (Chapter 7 -UK Committee Research and Reports) <https://www.gov.uk/government/publications/draft-online-safety-bill>

⁴ Report of Session 2021–22 <https://committees.parliament.uk/publications/8206/documents/84092/default/>

⁵ Aiken, M. P. (2019, June). (Contributor to European Regulators Group for Audiovisual Media Services Academy 2018 Workshop) *Protecting Children in Audiovisual Media Services - The effectiveness of age verification and media literacy*. Retrieved from http://erga-online.eu/wp-content/uploads/2019/05/ERGA-Academy-2018-Workshop-PoM-Effectiveness-of-age-verification-and-media-literacy_03-10-2018.pdf

commissioned to inform UK VSP regulation (VSP stands for video sharing platforms i.e. Tik Tok, YouTube, Instagram and so forth).⁶ Online disinformation falls under a classification of 'Manipulation'

Classification of risk of online harm (Research on the Protection on Minors Report p. 57-58)

<i>Sexual</i>	<ul style="list-style-type: none"> • Pornography • Sexting • Naked selfies/nudes • Grooming • Child sexual abuse • Child sexual exploitation / coercion • Child sexual abuse materials • Livestreaming of child sexual activity/abuse • Meeting online strangers in real life
<i>Aggression</i>	<ul style="list-style-type: none"> • Hate speech • Violence/Incitement to violence • Extreme content • Cyberbullying • Online harassment • Cyberstalking
<i>Manipulation</i>	<ul style="list-style-type: none"> • Image/video filtering, editing and photoshopping • Fake profiles • Fake news • Mis/disinformation • Deep fakes • Radicalisation • Profiling • AI and algorithmic manipulation • Persuasive design, nudging and targeting
<i>Self-injurious</i>	<ul style="list-style-type: none"> • Exposure to self-harm • Exposure to eating disorders • Exposure to suicide content • Exposure to alcohol and tobacco
<i>Mental health/ wellbeing</i>	<ul style="list-style-type: none"> • Psychological distress • Depression • Anxiety • Loneliness • Isolation • Social withdrawal • Low self-esteem/inadequacy • Fear of Missing Out (FOMO) • Addictive type behaviours • Problematic Internet Use • Gaming disorder

⁶ Davidson, Aiken, Gekoski, Phillips & Farr (2021) Video Sharing Platform Research on the Protection of Minors Literature Review and Taxonomy (Publisher Ofcom) Retrieved from https://www.ofcom.org.uk/data/assets/pdf_file/0023/216491/uel-report-protection-of-minors.pdf

<i>Cognitive</i>	<ul style="list-style-type: none"> • <i>Attention</i> • <i>Memory</i> • <i>Executive function</i> • <i>Brain structure/functioning</i>
<i>Moral</i>	<ul style="list-style-type: none"> • <i>Judgement</i> • <i>Decision-making</i> • <i>Character traits</i> • <i>Values</i>
<i>Physical</i>	<ul style="list-style-type: none"> • <i>Sleep deprivation</i> • <i>Obesity</i> • <i>Tech ergonomic risk</i>
⁵⁷ <i>Cyber deviance</i>	<ul style="list-style-type: none"> • <i>Identity theft</i> • <i>Hacking</i> • <i>Cyberscams/Cyberfraud</i> • <i>Malware/Spyware</i>

2. Develop the Irish Safety Tech Sector

I have worked closely with DCMS regarding the establishment and development of the UK Safety Tech sector. "Safety Tech providers develop technology or solutions to facilitate safer online experiences, and protect users from harmful content, contact or conduct." (p.19).

I was one of the expert advisors to the UK Gov Safety Tech report "Safer technology, safer users."⁷ We developed an evidenced based taxonomy of technical solutions to online harms from child exploitation and abuse, to mis and disinformation, operating at multiple levels for example; System, Platform, End point and so forth (see table below p.21 in report).

Safety Tech is gaining traction world-wide, I have recently presented at both UN and G7 dedicated Safety Tech events, last month we published the first research report on the emerging billion dollar US Safety Tech market.⁸

⁷ Donaldson, S., Davidson, J., & Aiken, M. P. (2020) Safer technology, safer users: The UK as a world-leader in Safety Tech. Online Safety Technology Sectoral Analysis. Report prepared for the Department for Digital, Culture, Media & Sport UK.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/887349/Safer_technology_safer_users-_The_UK_as_a_world-leader_in_Safety_Tech.pdf

⁸ <https://www.prnewswire.com/news-releases/paladin-capital-issues-first-ever-report-on-emerging-billion-dollar-us-safety-tech-market-301459019.html>

SAFETY TECH TAXONOMY AT A GLANCE



01 AT SYSTEM LEVEL

Automated identification and removal of illegal content

- Use of technology to identify and remove known illegal child sexual exploitation and abuse (CSEA) and terrorist content especially imagery and video), frequently through use of hashlists.



02 AT PLATFORM LEVEL

Supporting human moderators

- Identifying and flagging to human moderators for action:
 - Potentially illegal content or conduct, such as grooming, hate crime, harassment or suicide ideation
 - Harmful content or conduct which breaches site T&Cs, such as cyberbullying, extremism or advocacy of self-harm
- Reducing moderators' own exposure to harmful content.

Enabling age-appropriate online experiences

- Use of age-assurance and age-verification services to limit childrens' exposure to harmful content.



03 AT DEVICE OR ENDPOINT LEVEL

User-initiated protection

- User, parental or device-based products that can be installed on devices to help protect the user from harm.

Network filtering

- Products or services that actively filter content, through black-listing or blocking content perceived to be harmful. This can include solutions provided to schools, businesses or homes to filter content for users.



04 IN THE INFORMATION ENVIRONMENT

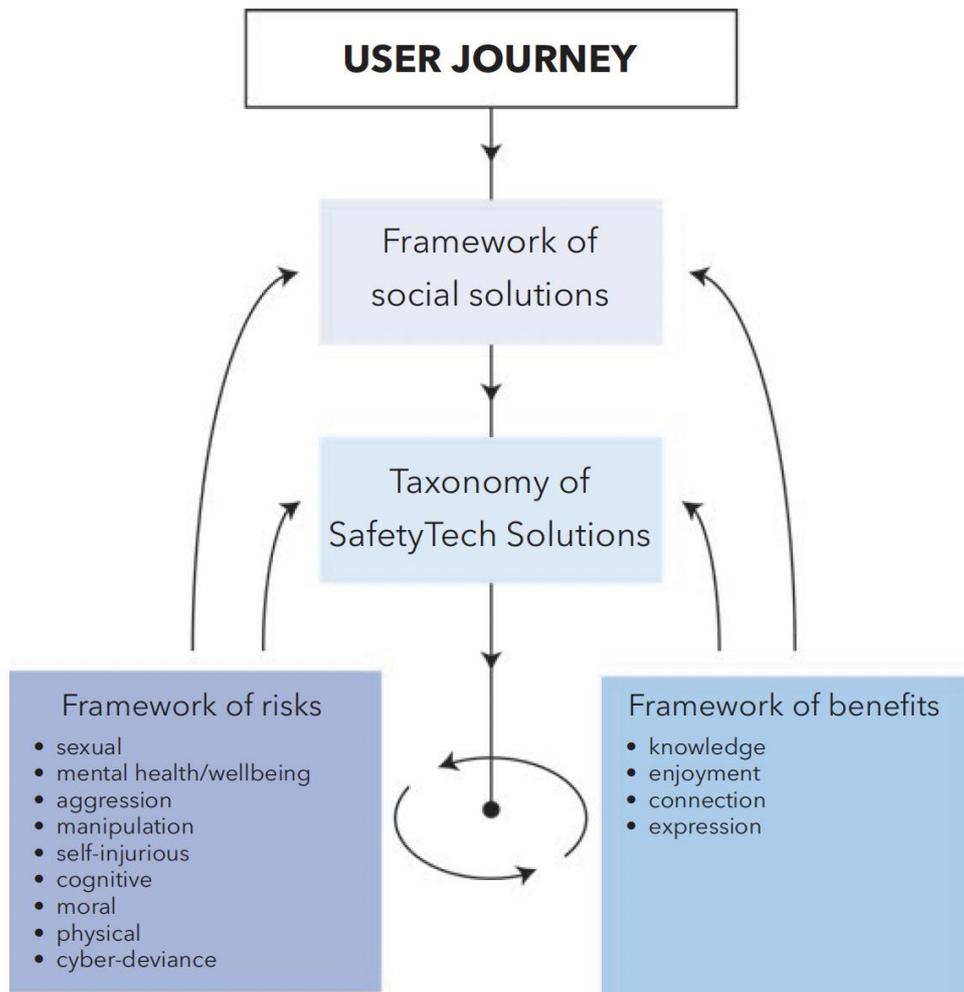
Identifying and mitigating disinformation

- Flagging of content with false, misleading and/or harmful narratives, through the provision of fact-checking and disruption of disinformation (e.g. flagging trusted sources).

3. Conceptualise a workable framework of solutions

There is a requirement to conceptualise a framework of solutions whereby in the case of online disinformation the users exposure to online harms is mitigated by the following; social solutions i.e. media literacy; Safety Tech solutions i.e. automatically detect and disrupt false, misleading or harmful narratives; and importantly do so while balancing both the benefits and risks of online technologies.

The User Journey: Interconnected Frameworks (Research on the Protection on Minors Report p.5)



9

⁹ Davidson, Aiken, Gekoski, Phillips & Farr (2021) Ofcom report: Video Sharing Platform Research on the Protection of Minors Literature Review and Taxonomy https://www.ofcom.org.uk/data/assets/pdf_file/0023/216491/uel-report-protection-of-minors.pdf

In summary, any consideration of online harms in an Irish context must be informed by an evidenced based approach. Recommendations are as follows

1. Requirement to scope, define and characterise the problem space
2. Commission research to explore the Irish Safety Tech sector and ecosystem
3. Develop a workable interconnected framework of solutions
4. Establish an Advisory Committee on disinformation and misinformation

Online harms have the characteristics of Big Data, in terms of volume, velocity and variety. Tackling these issues requires, an understanding of the threat landscape, clear definitions and classifications, and characterisation of the scale of the problem, along with consideration of AI and ML workable solutions.

Online safety and media regulation is extremely important, however my prediction is that regulation will not be practicable, feasible, workable or indeed successful if the recommendations I have outlined are overlooked.

Professor Mary Aiken outline biography

Dr Mary Aiken is a [Professor of Cyberpsychology](#) and Chair of the Department of Cyberpsychology at Washington D.C.'s premier STEM University, Capitol Technology University. She is Member of the INTERPOL Global Cybercrime Expert Group and Academic Advisor to Europol's European Cyber Crime Center (EC3). Mary is a Professor of Forensic Cyberpsychology in the Department of Law and Criminology at the University of East London, and an Adjunct Professor at the Geary Institute for Public Policy at University College Dublin, she is a Fellow of the Royal Society of Medicine, member of Medico-Legal Society, International Affiliate Member of the American Psychological Association (APA), Fellow of the Society for Chartered I.T. Professionals, and International Global Fellow at the Washington DC Wilson Center. Professor Aiken is an expert advisor to the UK government Department for Digital, Culture, Media & Sport (DCMS) on online safety technologies (Safety Tech). She recently co-authored a position paper on the social impact of cybercrime for Europol titled "[The Cyber Blue Line.](#)"

Professor Aiken has an M.Sc. in Cyberpsychology and a PhD in Forensic Cyberpsychology, her research interests include Safety Tech, AI, FinTech, human factors in infosec & cybersecurity, organized cybercrime, Internet psychology, human & technical drivers of cybercrime, online behavioural profiling, personal cyber security & safety, child protection online and cyber ethics. Professor Aiken is recognised as an expert at national and international level in policy debates at the intersection of technology and human behaviour. In 2014, she was inaugurated into SameShield an 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. In 2019 and 2021 she was named in the Top 50 inspiring "Women in GovTech."