Opening Statement by
Professor Barry O'Sullivan MRIA and Adj. Assoc. Professor Mary Aiken
to the Oireachtas Joint Committee on Children and Youth Affairs
Tuesday, 13th February 2018, 1:30pm

We are grateful for the committee's invitation to speak on the implications of *Cyber Security for Children and Young Adults*. The protection of children online is an extremely important issue. One might argue, and we do, that the challenges, threats, and dangers, presented by the Internet, social media, and wider cyberspace, to our children and young teenagers, necessitate that the issues are given our utmost careful attention. It is important that this problem space is not considered in separate Government silos of, for example, education, health, justice, or communications, since in terms of the child or young person's experience of technology, each has an important contribution to make.

A key concept underpinning the security of our children and young teenagers online is age appropriate interaction with technology, and more specifically age appropriate interaction with the Internet. The Digital Childhood Report (2017)[1] highlights that the Internet was conceived as an environment for adult users and no design concessions were made for children. The utopian vision of the Internet was that all users would be equal. If all users are equal then a child user is treated the same as an adult user, and this is why, arguably, the Internet, by default, is not fit for children.

The Children's Online Privacy Protection Act (COPPA)[2] has been one of the sole mechanisms to define restrictions on the collection and processing of personal data from children under the age of 13 years unless verifiable consent has been granted by a parent or guardian. It is because of COPPA that many social media platforms require that their users are at least 13 years old. However, it has not been vigorously enforced in a regulatory context. Studies consistently provide evidence of underage usage of mainstream social media platforms.[3] We believe that robust ***age verification online*** is one of the most critical requirements to deliver on **child and youth security in cyber contexts**.

The forthcoming European General Data Protection Regulation (GDPR),[4] which comes into effect on May 25th, 2018, will formalise age protective measures online. The EU has set the **digital age of consent** at 16 years, but permits each state to decide a national age of consent that can be as low as 13 years. Notably Ireland has opted for 13, the lowest age of digital consent allowed under the GDPR. The Data Protection Bill 2018,[5] which enshrines an Irish digital age of consent of 13, was submitted to the Senate on the 8th February 2018 and is currently under consideration.

---

[1] http://5rightsframework.com/static/Digital_Childhood_report_-_EMBARGOED.pdf

[2] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[3] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[5] http://www.justice.ie/en/JELR/Pages/SP18000046

On launching the bill, the Minister for Justice and Equality said: *"The Government considers that a 'digital age of consent' of 13 years represents an appropriate balancing of children's rights, namely a child's right to participation in the online environment and a child's right to safety and protection, rights that are enshrined in the UN Convention on the Rights of the Child. Provision is made for that in section 29."*

However, 'section 29,' or rather *Article 29*, does not say this. This is a claim that has been used by a number of respondents to the Department of Justice and Equality's consultation on the digital age of consent in 2016.[6] The UN Convention on the Rights of the Child[7] was ratified in 1989, and came into effect in 1990, thereby pre-dating the Internet, online services, and social media. The assertion that "*a child's right to participation in the online environment...rights that are enshrined in the UN Convention on the Rights of the Child"* is not accurate.

If one wishes to bring this convention into play, attention should be given to Article 17 which says *"States Parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health."* Article 19 states: *"States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child."* More importantly, Article 27 states: "*States Parties recognize the right of every child to a standard of living adequate for the child's physical, mental, spiritual, moral and social development"* and *"The parent(s) or others responsible for the child have the primary responsibility to secure, within their abilities and financial capacities, the conditions of living necessary for the child's development."*

Notably Article 1 adopts an age protective stance regarding the definition of a child: *"For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier."*

We will outline in the remainder of our submission some of the many reasons why Ireland, by setting the digital age of consent to 13 years, is not honouring the spirit of the UN Convention on the Rights of the Child in terms of the risks to a child's security, well-being, and physical, and mental health. The digital age of consent is intended to provide robust protection for children from those who might seek to target and commercially exploit them. In our opinion the digital age of consent will also have protective merit in terms of the psychological and social well-being of the child, which in turn will help to deliver on child safety and security.

[6] http://www.justice.ie/en/JELR/Pages/Consultation_on_Data_protection_safeguards_for_children_Digital_Age_of_Consent
[7] https://www.dcya.gov.ie/documents/unrightsofchild/UN_Convention_on_the_rights_of_the_child.pdf

The OFCOM (2017) *Children and Parents: Media Use and Attitudes Report*[8] highlights that more younger children are going online; half (53%) of 3-4s are now online, as are 79% of 5-7s and 94% of 8-11s. Ninety-nine percent of 12-15 year olds are also online. Age appropriate use of devices that connect to the Internet is also critical. Children are increasingly using such devices at a younger age:

- 1% of 3-4 year olds have their own smartphone and 21% have their own tablet, 53% go online for over 8 hours a week.
- 5% of 5-7 year olds have their own smartphone and 35% have their own tablet, 79% go online for over 9 hours a week. 3% have a social media profile.
- 39% of 8-11 year olds have their own smartphone and 52% have their own tablet, 94% go online for over 13.5 hours a week. 23% have a social media profile.
- 83% of 12-15 year olds have their own smartphone and 55% have their own tablet, 99% go online for over 21 hours a week. 74% have a social media profile.

It is significant that such a large percentage of young people have a social media profile despite COPPA: this represents a major cybersecurity challenge that must be addressed.

Evidence is mounting about the harmful effects of social networking sites on the well-being of children, including sleeplessness, obesity, compulsive use, and vulnerability to advertising. Sleep deprivation increases the likelihood that teens will suffer a myriad negative consequences, including an inability to concentrate, poor grades, anxiety, depression, and suicidal ideation.[9]

The statistics are worrying: rates of anxiety and depression in young people have increased by seventy percent over the past 25 years.[10] Young people say four of the five most used social media platforms make their feelings of anxiety worse. The Royal Society for Public Health report (2017)[11] states that *"the platforms that are supposed to help young people connect with each other may actually be fuelling a mental health crisis".*[12]

Insomnia is on the rise: one in five young people say they wake up during the night to check messages on social media,[13] they are three times more likely to feel constantly tired at school. Nine in 10 teenage girls say they are unhappy with their body, and there has been a surge in teenage girls being hospitalised for eating disorders; according to the HSE the number has almost doubled over 10 years.[14] Arguably these increases are linked to the use of social media along with the availability of such sites as “pro-ana” and “pro-mia” (websites encouraging and glamorising anorexia and bulimia) that influence vulnerable, self-conscious teens. Notably the

[8] https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

[9] https://med.stanford.edu/news/all-news/2015/10/among-teens-sleep-deprivation-an-epidemic.html

[10] The Mental Health Foundation. 2004. Lifetime impacts: Childhood and adolescent mental health – understanding the lifetime impacts. [Accessed Apr 17] Available from: https://www.mentalhealth.org.uk/sites/default/files/lifetime_impacts.pdf

[11] https://www.rsph.org.uk/uploads/assets/uploaded/62be270a-a55f-4719-ad668c2ec7a74c2a.pdf

[12] Collishaw, S. Maughan, B. Goodman, R. Pickles, A. Time trends in adolescent mental health. [Accessed Apr 17] Available from: https://www.ncbi.nlm.nih.gov/pubmed/15482496

[13] http://www.telegraph.co.uk/news/health/news/11865757/One-in-five-teens-wake-up-at-night-to-use-social-media.html

[14] https://www.irishtimes.com/news/health/surge-in-teenage-girls-being-hospitalised-for-eating-disorders-1.3108388

negative impact of these sites along with the availability of harmful and age-inappropriate online content, such as violent, aggressive or gory content involving cruelty, abuse of animals and killings, adult pornography, extremism, and radicalisation, was highlighted in the Irish 'Internet Content Governance Report' (2014).[15] Ireland has one of the highest rates of "sexting" among young people in Europe.[16] The exchange of explicit images present a significant security risk rendering young people vulnerable to cyberbullying and to sextortion. In 2017 Europol reported that "sextortion" and "webcam blackmailing" has "skyrocketed" in the past few years, it was noted that victims as young as 7 years old are being targeted online.[17]

Instant messaging apps are problematic in terms of cyberbullying since they can act as rapid vehicles for circulating bullying messages and spreading images. The National Anti-Bullying Research and Resource Centre at Dublin City University found that new apps and social media platforms are targeting children as young as nine years of age,[18] children can be very reluctant to tell their parents about the bullying because they're worried that their Internet access will be taken away. Victims of bullying are more likely to experience low academic performance, depression, anxiety, self-harm, feelings of loneliness and changes in sleeping and eating patterns which is extremely worrying regarding the overall health and well-being of our children and young people.

Teachers are frontline witnesses to these problems. UK Teachers have reported a significant increase in children as young as four years suffering panic attacks, eating disorders, anxiety and depression. Schools are struggling to access support to deal with the surge in the number of children and young people suffering from mental health issues. The National Association of Schoolmasters Union of Women Teachers (NASUWT) general secretary Chris Keates has warned of growing concern among teachers about a gap in the availability of experts and counselling to help children with mental health needs.[19] A recent survey by the Irish Primary Principals Network (IPPN) reported that a quarter of its members reported a spike in anxiety levels in their schools.[20] The 'Growing Up in Ireland' study (2016) found that: 10% of 17-18 year olds reported that they had been diagnosed with depression, anxiety or both by a medical professional; 17% of 17-18 year olds admitted to engaging in self-harm behaviour. Self-harming was twice as common among females (23%) as it was among males (12%).[21]

Setting an appropriate **digital age of consent** is a complex issue. The decision must be informed by the impact that technology has on the cyber-cognitive and sociological development of children so that we avoid placing them in positions where they neither have the digital skills,

[15] https://www.dccae.gov.ie/en-ie/communications/publications/pages/Internet-content-governance-advisory-group-report.aspx
[16] https://www.irishexaminer.com/breakingnews/ireland/irish-teens-have-one-of-the-highest-sexting-rates-in-europe-739123.html
[17] https://www.europol.europa.eu/newsroom/news/police-across-europe-issue-warning-about-online-coercion-and-extortion-of-children
[18] http://www.thejournal.ie/online-games-children-cyberbullied-3224737-Feb2017/
[19] https://www.nasuwt.org.uk/article-listing/pupil-mental-health-support-announcement.html
[20] https://www.irishpsychiatry.ie/blog/school-stress-the-emerging-issue-of-anxious-schoolchildren/
[21] http://www.esri.ie/growing-up-in-ireland/growing-up-in-ireland-official-publications-from-the-child-cohort/

nor the understanding of the consequences of sharing their data or aspects of their personal lives. Children need guidance from their parents in this regard.

When it comes to technology and children, the digital age of consent is both a security and a child protection issue. An arbitrary statement that every child at 13 is capable of consenting to the terms and conditions of online service providers is problematic given the potential risks that they face. For example companies can collect, record and share a child's home and school address, their location, their date of birth, their photos, phone number, their likes and dislikes, who they know, and the content of their conversations, including direct messages sent privately. Not only does this present a security risk to the individual child but, by association, it also presents risk to the family.

Notwithstanding a young person's right to freedom of speech and to access information, the requirement for **verifiable parental or guardian consent** for those under the digital age of consent seems entirely appropriate and responsible. The point is that parents and guardians know their child best, and they are the primary custodians of their security and welfare. They are best placed to properly evaluate when it is appropriate to grant consent on behalf of their child. It is only they who can appropriately assess an individual child's level of maturity, understanding, and judgement in an online context.

An optimum digital age of consent for Ireland can be **informed by best practice** in other countries. Notably EU leaders in child safety and protection online countries such as Germany and the Netherlands have chosen 16 years as their digital age of consent. The UK will be enacting an amendment to its Data Protection Bill to impose a stricter code of practice for protecting children's privacy online focusing on provisions for 13-17 year olds who are above the digital age of consent but still children[22]. The proposed UK amendment has several features designed to deliver on cyber security, for example:

- Ensuring high privacy settings are switched on by default;
- Not revealing GPS locations; and
- Preventing data from being widely shared.

Additionally, the proposed amendment allows for the well-being of the young person, for example by giving children time off from endless notifications during school and sleep hours and by requiring commercially-driven content presented to children to be clearly identified.

The Irish digital age of consent must be informed by the Law Reform Commission's 2011 "Report on Children and the Law: Medical Treatment (LRC 103-2011)".[23] The report recommended that when it came to persons under 16 there should not be a presumption of capacity to consent. The 2011 report involved the application of **a "mature minor" test**, which has been applied in a number of states, sometimes in case law and sometimes in legislation, to a wide variety of legal areas involving decision-making capacity of children and young persons.

[22] https://www.theguardian.com/technology/2017/dec/08/government-uk-tough-code-practice-protect-children-privacy-online

[23] http://www.lawreform.ie/_fileupload/Reports/r103.htm

It is also worth noting that Article 42A of the Constitution[24], inserted by the children's rights referendum, also recognises the concept of a "mature minor" test. Whilst Article 42A might not directly apply to the age of consent for the purposes of the GDPR, the fact that the Constitution now includes a "mature minor" test is worth noting.

The Gardai have stated that they have no substantial difficulty with the Digital Age of Consent being set at 16. It was recently reported that Assistant Commissioner Pat Leahy has criticised Government for “not serving our children well” with unregulated access to social media websites where they could become victims of online paedophiles[25]. The number of suspected incidents of online child sexual abuse referred to the Metropolitan police in the UK has increased by 700% since 2014. Reports to the current UK ‘Independent Inquiry into Child Sexual Abuse”[26] estimate that ten percent of adults take part in “online sexualised conversations” with children and teenagers aged under 18; as many as 4% of adults have engaged with images of child sexual abuse on the Internet, and 11 to 14-year-olds are most at risk from online abuse.

Given the substantial risks to the safety, security and wellbeing of children and young people online, Ireland needs to put in place a policy framework and an associated educational programme that ensures that our children are sufficiently aware and responsible to understand and exercise their digital rights by the time they reach the digital age of consent. In the absence of a rigorous basis for any specific age at this point, a prudent approach would be to set the digital age of consent in Ireland at 16.

We would like to state unequivocally our opposition to the Irish Government’s current position to set the digital age of consent in Ireland at 13 years.

In terms of specific **recommendations**, we would like to highlight the following:

1. Experts, policymakers and stakeholders should come together and agree on a **national framework** to address Irish children's well-being, safety and security online.

2. Our Government must **hold social media companies accountable** for underage usage of their platforms. As a society we do not condone or allow underage drinking - why is underage use of social media so rampant and accepted?

3. There is a need to stop conflating **a child’s right to access information online, with the digital age of consent**, which specifically relates to the age at which a child can sign legal agreements with online service providers who gather, profile, sell, and commercialise, his/her personal data.

[24] http://www.irishstatutebook.ie/eli/2012/ca/31/enacted/en/print

[25] https://www.irishmirror.ie/news/irish-news/assistant-garda-commissioner-slams-government-11929651

[26] https://www.theguardian.com/society/2018/jan/22/4-of-uk-adults-have-seen-child-sexual-abuse-images-survey

4. The Government must formalise the role, office, and statutory powers of the Digital Safety Commissioner. One specific task that could be assigned to this office is **the development of a robust system for age verification online**. Self-verification does not work. Ireland could lead in the area of online age verification. We believe that robust age verification online is one of the most critical requirements to deliver on child and youth security in cyber contexts.

5. We must develop robust policies and safeguards to ensuring that children are delivered **content that is age-appropriate** and that careful consideration is given to **limiting/eliminating advertising** to them online.

6. In tandem to setting an appropriate digital age of consent, consideration must be given to making the **Internet and social media safer for kids**, as well as educating children and parents on Internet safely. There is clearly a role here for the Office of the Digital Safety Commissioner.

7. The Report of the **Internet Content Governance Advisory Group** (2014)[27] should be revisited. Specifically, consideration should be given to Recommendation 12, p.9, and its possible implementation through the Office of the Digital Safety Commissioner, to provide *"...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 enquiries, aggregating available support content and serve as a directory/information resource for the general public."*

8. The Office of the Data Protection Commissioner must work in tandem with the new Office of the Digital Safety Commissioner to provide a **seamless reporting mechanism** for violations of the GDPR, digital age of consent, age verification online, and the provision of safe and age-appropriate Internet content.

[27] https://www.dccae.gov.ie/en-ie/communications/publications/pages/internet-content-governance-advisory-group-report.aspx

Biographies

Professor Barry O'Sullivan, MRIA is an award-winning academic working in the field of artificial intelligence and data analytics for more than two decades. He is the founding Director of the Insight Centre for Data Analytics at University College Cork, and a founding investigator at the Confirm Centre for Smart Manufacturing which is based at the University of Limerick. Professor O'Sullivan is well-known for his advocacy of digital rights and data ethics.

Professor O'Sullivan is current Deputy President of the European Artificial Intelligence Association (EurAI), one of the world's largest AI associations with over 4500 members in over 30 countries. He is a Fellow of EurAI, an honour that recognises 3% of the European AI community. He was President of the International Association for Constraint Programming from 2007-2012; his leadership of the association was recognised in 2014 when he was awarded the Association for Constraint Programming Distinguished Service Award. In 2013 he received a University College Cork Leadership Award. He was named Science Foundation Ireland Researcher of the Year for 2016, University College Cork Researcher of the Year in 2017, and elected a Member of the Royal Irish Academy in 2017, Ireland's highest academic accolade.

Professor O'Sullivan was actively engaged in advising European stakeholders on the implications of many aspects of the General Data Protection Regulation which comes into effect in May 2018.

Mary Aiken is an Adjunct Associate Professor at the Geary Institute for Public Policy University College Dublin and Academic Advisor to Europol's European Cyber Crime Centre (EC3). She is a lecturer in Criminology and Fellow at the School of Law, Middlesex University, a Fellow of the Society for Chartered IT Professionals and has served as Distinguished Professor of the Practice of Cyber Analytics and Sensemaking Fellow at the IBM Network Science Research Center. She is the former Director of the Cyberpsychology Research Centre at the Royal College of Surgeons in Ireland.

Mary has conducted research and training workshops with multiple global agencies including INTERPOL, Europol, the FBI, the EU and the White House. She was a member of the 2013 Irish Government Internet Content Governance Advisory Group and an expert contributor to the Irish Law Reform Commissions 2016 Report on Harmful Communications and Digital Safety. Mary is a member of the INTERPOL Specialists Group on Crimes Against Children and an advisory board member of The Hague Justice Portal.

In 2016 Mary was named as one of the top 50 most inspiring women in technology in Europe, in 2017 she was Inducted into Infosecurity Europe Hall of Fame in recognition of long-term contribution to the information security sector and her work as an advocate and educator in information security. In 2018 Mary was appointed as a Global Fellow at the Washington DC Wilson Center chartered by the US Congress as the official memorial to President Woodrow Wilson, it is the key US non-partisan policy forum for tackling global issues through independent research and open dialogue to inform actionable ideas for the policy community.