

DÁIL ÉIREANN

AN COMHCHOISTE UM CHUMARSÁID, GNÍOMHÚ AR SON NA HAERÁIDE AGUS COMHSHAOL

JOINT COMMITTEE ON COMMUNICATIONS, CLIMATE ACTION AND ENVI- RONMENT

Dé Máirt, 6 Samhain 2018

Tuesday, 6 November 2018

The Joint Committee met at 11 a.m.

MEMBERS PRESENT:

Deputy Timmy Dooley,	Senator Tim Lombard.
Deputy James Lawless,	
Deputy Eamon Ryan,	
Deputy Brian Stanley,	

DEPUTY HILDEGARDE NAUGHTON IN THE CHAIR.

The joint committee met in private session until 11.25 a.m.

Scrutiny of EU Legislative Proposals

Chairman: There are two Schedule B EU legislative proposals before the joint committee. EU COM (2018) 630 is a proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. It is agreed that there are no subsidiarity concerns with this proposal. Therefore, it does not require further scrutiny.

EU COM (2018) 657 is a proposal for a Council directive on the position to be taken on behalf of the European Union at the second meeting of the Conference of the Parties to the Minamata Convention on Mercury with regard to the adoption of guidelines on the environmentally sound interim storage of mercury, other than waste mercury, referred to in paragraphs 2 and 3 of Article 10 of the convention. Is it agreed that the proposal does not require further scrutiny? Agreed.

I propose to suspend the sitting briefly to allow witnesses to take their seats in advance of the next part of the meeting, which involves detailed scrutiny of the Digital Safety Commissioner Bill 2017.

Sitting suspended at 11.26 a.m. and resumed at 11.29 a.m.

Digital Safety Commissioner Bill 2017: Discussion (Resumed)

Chairman: We are resuming our detailed scrutiny of the Digital Safety Commissioner Bill 2017, which is a Private Members' Bill.

I draw the attention of witnesses to the fact that by virtue of section 17(2)(l) of the Defamation Act 2009, they are protected by absolute privilege in respect of their evidence to the joint committee. However, if they are directed by the Chairman to cease giving evidence on a particular matter and they continue to do so, they are entitled thereafter only to a qualified privilege in respect of their evidence. Witnesses are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person, persons or entity by name or in such a way as to make him, her or it identifiable. Any submission or opening statement made to the committee will be published on its website after the meeting. Members are reminded of the long-standing parliamentary practice to the effect that they should not comment on, criticise or make charges against a person outside the Houses or an official either by name or in such a way as to make him or her identifiable. I remind members and witnesses to turn off their mobile phones as they interfere with the sound system.

I welcome our guests and advise them that in view of the large number of stakeholders present, opening statements will be restricted to five minutes. I will indicate when witnesses have one minute remaining. Members will be restricted to three minutes each for questions.

We will begin with Deputy Ó Laoghaire, the sponsor of the Bill. I ask him to give a brief overview of what it involves.

Deputy Donnchadh Ó Laoghaire: I welcome the opportunity to again address the committee on the Digital Safety Commissioner Bill. There is no doubt that online safety has become one of the most significant challenges facing Irish society and, arguably, one of the most significant child protection issues of our time. We face major challenges. Many people, particularly parents, are concerned about what is happening in that regard. It is hard to blame them for that when one reads reports of predatory behaviour, harmful material and online bullying. This is an issue which legislators cannot ignore and must face up to. A policy and educational response - along with strong regulation and a statutory office with real powers and teeth - is required. It is generally accepted in most policy areas that self-regulation is no regulation. The Internet and online safety are not particularly different in that regard. Some providers have good regulatory mechanisms but others have none. Legislation is needed to ensure that all providers step up to the mark and provide appropriate safeguards. Among the primary proposed functions of the commissioner are to promote digital safety for all and to support and encourage the implementation of measures to improve digital safety, including oversight, regulation and a timely and efficient procedure for the removal of harmful digital communications.

I welcome the representatives from the various organisations, the Department and industry. I note the commentary by organisations and industry on the Bill. I welcome the fact that, at a previous meeting, Ms Sweeney and her colleague from Facebook, Ms Siobhán Cummiskey, stated that they are not opposed to the idea of a digital safety commissioner and that they see great benefit in a single office having the ability to oversee and co-ordinate efforts to promote digital safety. That view is widely shared, but we need to work collaboratively and constructively on the detail of what is involved. I approach these engagements with an open mind in the context of amendments. I am not precious in that regard. I will work with the committee, departmental officials or representatives of industry or civil society organisations to improve the Bill in any way possible.

A key point raised at the committee's most recent meeting - and which may be raised again today - relates to the need for a definition of "harmful communications". It may be appropriate for the definition to be provided by the office of the digital safety commissioner. It should not be left to providers to define it. On balance, as there is a legal requirement to be in compliance with sections 4 and 5, it would be appropriate to provide a definition. I am developing a draft definition, which will be needed. We should look to the recommendations of the Law Reform Commission which provide a description of a category of existing and proposed offences. I do not propose to introduce amendments to make such offences criminal offences under the Bill. However, those are the types of behaviours we must seek to address.

I will be making a submission to the committee and the Minister to inform the drafting of the scrutiny report. I suggest that other interested bodies should also consider doing so in order to allow the committee to evaluate all viewpoints in advance of drafting its report and the Committee Stage debate on the Bill.

The issue of freedom of expression has also been raised. I acknowledged this in my comments on the previous occasion. It is correct that we must proceed very carefully. Freedom of expression is a value we all treasure and is essential to a functioning democracy. I do not believe, however, that this is a reason to prevent us proceeding. It is not an absolute right, especially where harmful communications are damaging, hurtful or, in some circumstances, illegal. There is a consensus. We cannot simply allow self-regulation to be the only approach. We need to show vision and be ambitious and imaginative. In view of the fact that this has been done in other common law jurisdictions, there is no reason for not doing the same here. We need to

do it.

Chairman: I thank Deputy Ó Laoghaire. Our next witnesses are from the Department of Communications, Climate Action and Environment. I welcome Ms Patricia Cronin, assistant secretary, and Ms Triona Quill, principal officer. I invite Ms Cronin to make her opening statement.

Ms Patricia Cronin: I thank the Chairman and members for inviting us to participate in the detailed scrutiny of Deputy Ó Laoghaire's Bill. As members are aware, the Minister, Deputy Bruton, expressed his preliminary views on the Bill at the committee's meeting on 25 October. He outlined his view that if the Oireachtas is to pass a law in this area, it must ensure that it is robust, effective, and proportionate and that it properly meets the public policy need to protect children online. The Minister has asked the Department to consider the Private Members' Bill in detail. He also asked the Attorney General for urgent advice on a range of legal issues which the draft legislation presents.

As members are aware, the action plan for online safety, which was published by the Taoiseach on 11 July, contains 25 actions to be implemented or substantially progressed by the six Departments involved by the end of 2019. Since the publication of the plan, an interdepartmental sponsors' group, chaired by the Department of Education and Skills, with membership from the other five Departments, has been established. That group will report to the relevant Cabinet committee on progress in implementing these commitments.

The National Advisory Council for Online Safety has also been established. Its secretariat is provided by my Department. The first meeting of the council was held on 4 October and the next meeting will be held in the coming weeks. The Minister of State, Deputy Canney, has succeeded the Deputy Kyne, who is now Minister of State at the Department of the Taoiseach, as chairman of the council. The committee may also be interested to note that the council has established two sub-groups, the first to consider the role of the council in relation to guidance material, and the second to consider the council's role in relation to research. A wide range of organisations have accepted the Government's invitation to be members of the council, including the four other organisations represented at this meeting, as well as other bodies representing parents and older people, academic experts, and State bodies including An Garda Síochána, the Data Protection Commission and the Ombudsman for Children.

It is envisaged that the council will publish a report on its work to date to coincide with Safer Internet Day in February. This will, in subsequent years, will become the council's annual report. The overall focus of the action plan for online safety is to identify and deliver the activities that can be delivered over a period of 12 to 18 months and that will have the greatest impact on online safety for all our citizens, especially children. Action 18 of the plan commits the Government, and specifically my Department, as well as the Departments of Justice and Equality and Business Enterprise and Innovation, to work with this committee to explore the issues arising in respect of this Private Members' Bill.

There are a number of issues which the committee may wish to consider in the context of its scrutiny, a number of which were referenced by the Minister on 25 October, some of which I will now outline. There is an absence of a definition of harmful digital communications. It will be important to define what illegal offences will come within scope; whether the definition would also include harmful but not illegal communications, and, if so, of what nature. Another issue is the definition of a digital service undertaking which appears to encompass a very wide range of undertakings, some of which may pose little or no risk in respect of harmful com-

munications. In the context of illegal content, would the Data Protection Commissioner have the power to seek the take-down of such material without consulting An Garda Síochána? In the case of harmful but legal content, are there enforcement issues arising given that under the e-commerce directive 2000, notice and take down requirements relate only to the take-down of illegal content? Is the enforcement mechanism envisaged for the take-down of harmful content by an undertaking located outside the State appropriate given that the speed of take-down would likely be the key outcome sought in such cases?

It may be helpful for the committee to be aware of some additional developments in the regulation of online content at European level. It is expected that the final text of the revised audiovisual media services directive will be published shortly, with a requirement that it be implemented by member states within 21 months. The original audiovisual media services directive, which was agreed in 2010, established the framework for regulating traditional television and on-demand services such as RTÉ Player and Netflix. While there are many aspects of the revision which will be of interest to the committee, of particular relevance to today's discussion are the new provisions that will apply to video-sharing platform services. Aspects of services such as YouTube are likely to fall within the scope of these provisions. The revised directive will require member states to introduce, by means of co-regulation, a system to ensure that these services have measures in place in order that minors will be protected from audiovisual content, including advertising, which may impair their physical, mental or moral development and that the general public will be protected from audiovisual content, including advertising, containing incitement to violence or hatred and from such content, including advertising, the dissemination of which is a criminal offence under Union law. The latter covers terrorism-related offences, child sexual abuse material offences and offences of racism and xenophobia.

Ireland will be required to appoint a national regulatory authority which will monitor and ensure that video-sharing platforms have appropriate measures in place to meet the goals I have outlined. Among the measures which may be appropriate are age-verification and parental controls. This presents an alternative approach to the regulation of harmful online content, albeit only for video-sharing platforms. The Department intends to commence a public consultation on Ireland's approach to the implementation of the revised directive before the end of this year.

Chairman: There are two witnesses from the Irish Society for the Prevention of Cruelty to Children, ISPCC, Mr. John Church, chief executive officer, CEO, and Ms Fiona Jennings, policy co-ordinator. I invite Mr. Church to make his opening statement.

Mr. John Church: I thank the committee for inviting us to attend and I thank Deputy Ó Laoghaire for bringing the Bill forward. We welcome the drafting of legislation to establish an office of digital safety commissioner and look forward to its progress.

Online safety is the child protection issue of our day. I would like to share a typical example of a Childline case with the committee. A 15 year old female contacted Childline's web chat service. She stated that she sent nude pictures of herself to her boyfriend and that when they broke up, he sent them to his friends. Now her friends and people in school are talking about her and calling her vile names. She feels really embarrassed, stupid and ashamed. She feels very hurt and betrayed by her ex-boyfriend. She did not think that he would do such a thing. She is terrified that her parents will find out and is scared about how they might react, especially her dad because he is so strict. She is so upset that she wants to kill herself. This example illustrates the fear and isolation children feel when something they do online goes horribly wrong and they perceive that the situation is out of their control to manage.

The ISPCC has been pleased to see the Houses of the Oireachtas take seriously the issue of online safety, with a significant increase in activity in Departments in the past year. We would like to take this opportunity too, to acknowledge the work of the Office for Internet Safety and Webwise and the work they do with limited resources. These structures need to be better resourced to make them more effective and for every parent, child and teacher in the country to become aware of them and embrace their resources and expertise.

The ISPCC broadly welcomed the publication of the Government's first action plan for online safety last July, particularly its provisions in respect of enhanced education measures and proposed law reform. However, the ISPCC expressed its disappointment at the time that the action plan fell short of a commitment to statutory regulation. Not long after the launch of the action plan, and indeed in recent times, the public has been presented with stark examples of self-regulation failing. It is our experience that these failures can impact negatively on children and that there are positive actions that Ireland can take to better protect children online. Notwithstanding the commitment to self-regulation in the action plan, and perhaps to reflect the fast-changing nature of this space, we were delighted to hear the comments of the Minister for Communications, Climate Action and Environment, Deputy Bruton, at the committee's detailed scrutiny stage where he stated it was time to move beyond self-regulation and highlighted the need for a regulatory body in the online space.

In 2016, the ISPCC carried out an internal case review of its Childline service and front-line services on the prevalence of online safety issues in our work. The findings of this review, in conjunction with cases in the external environment, led to online safety being an integral part of our policy work, in turn giving us a clear mandate to advocate for change in this area. In February 2017, the ISPCC made a presentation to the Joint Committee on Children and Youth Affairs and shared its experiences regarding online safety issues. These issues included access and exposure to inappropriate content, online grooming and cyberbullying. Harmful communications among children can be compounded by the fact that they are children and perhaps do not realise the reach their actions can have online. We are in no doubt that online safety is a major issue for children and young people in Ireland.

In 2005 we launched the first text-based support service for children in Ireland. We have seen a shift to our online and text service over the last decade, and we are in the final stages of development of a new online service. The ISPCC has seen the use of its Childline online services jump from just under 4,000 conversations in 2007 to just under 30,000 conversations in 2017. We know that children want us to be online, and to be more accessible to them in the spaces they inhabit. Through listening to and engaging with more than 1,000 children a day on our Childline service we have been able to spot trends over the years and raise these issues in the media and with policy-makers and legislators. Over the past two decades in particular we have seen how children's technological lives are becoming increasingly embedded in their lives as a whole. The online-offline distinction for children is an unfamiliar concept. Utilising technology and being online are no longer an add-on; it is how and where they live their lives.

Children make up one third of all Internet users globally. One in two users in the developed world is a child. Their participation and protection rights in the digital environment are widely supported across EU laws and policies. Irish policy sets out ambitions for all Irish citizens to be connected and online. ICT is broadly available and its use encouraged in many schools. The Government's action plan for online safety recognises that children's specific vulnerability warrants greater protection. The Net Children Go Mobile report of 2015 found that one in five children in Ireland reported being bothered by something they saw on the Internet in the past.

The Internet was not created with children as users in mind, but they use it. We know this, and we all have a role to play in keeping them safe online. Therefore, it is imperative we recognise the need for a regulatory body, with a digital safety commissioner or equivalent, to champion children's online safety and seek remedies for them when they are unable to do so themselves.

The issue of defining harmful communications has been raised at the various stages of debate on this Bill thus far. It is important that a definition is created to reflect the examples of harmful communications referred to in the Law Reform Commission's report and elsewhere, and not be overly broad so as to render the definition unworkable and, in effect, useless.

While some of the suggested work of a digital safety commissioner is being carried out across other Departments and structures, we feel there is merit in co-ordinating this work in order to maximise its efforts and impacts for all concerned, under an office of the digital safety commissioner, or equivalent.

Children have a right to be protected, and this protection extends to being online. Being online is the public space where children frequent the most. They converse with their friends there, keep in touch with family there and shop there. It is their go-to place for information, and, like any public space, it should afford them similar safety protections.

Ms Alex Cooney: CyberSafeIreland is the children's charity for online safety in Ireland. We set up in 2015 and since then we have spoken to 14,000 children and to thousands of parents and teachers about staying safe online. We also gather data on an ongoing basis which enables us to monitor trends and usage and to highlight risks. We recently launched our annual report and published the data that we had gathered over the last academic year, based on responses from more than 5,000 children aged between eight and 13. Some 68% of these children owned a smartphone and 70% were signed up to social media and messaging apps, despite age restrictions of at least 13 on all such services. In short, the use of online services was pervasive among this cohort of children. Our report further highlighted that many primary school teachers are seeing the consequence of children's online use in the classroom with 62% of teachers having dealt with online safety incidents over the last academic year. More than a third of teachers had dealt with between two and five incidents last year. Some of these incidences involved the uploading and sharing of harmful and upsetting material, including intimate images.

I am providing this data as a context to our position on the digital safety commissioner. We believe that a digital safety commissioner will offer a level of co-ordination and oversight that we currently do not have in Ireland. It will furthermore introduce a level of accountability by helping to ensure that social media companies are timely and responsive in their removal of any harmful material and consistent in their application of safeguards by providing monitoring, oversight and reporting on their performance in this regard. As a charity that is often approached for help by parents, teachers and those working with vulnerable children, we are more aware than many of the reality of when things go wrong online, when harmful or upsetting content is either not removed or not removed quickly enough. We also know that self-regulation means that online service providers get to be judge and jury in cases of troublesome and sometimes controversial content. This is where a digital safety commissioner could play an important role in the review of materials and decision-making in respect of take-down procedures.

The Bill also proposes the introduction of a code of practice, which would mean that there would be greater consistency across platforms. The office would also have an education and research remit and would offer an important level of co-ordination in these areas. It is important to recognise that many of the leading social media platforms, including Facebook and Google,

have worked consistently to improve safeguards on their platforms and have also provided some useful educational resources. It is incredibly important that they continue to prioritise safeguarding practice and design into the future. However, we need to go one step further by ensuring that all platforms are held to the same high standards and that there is a regulatory body that can provide oversight and step into the breach when needed.

In any discussion about a proposed digital safety commissioner, it is helpful to consider the precedents. The Australian Office of the eSafety Commissioner was set up in 2016 as a result of the Enhancing Online Safety Act 2015. While this office is still new - and it is too early to fully assess its effectiveness - commentators such as Matthew Rimmer, professor of intellectual property and innovation law at Queensland University of Technology, think that it offers value and addresses “genuine child safety issues in the digital environment which haven’t been well dealt with by governments or IT companies or the community”. The Australian Parliament’s legal and constitutional affairs references committee also acknowledged the importance of this office in its review of laws relating to cyberbullying earlier this year. It urged the Government to ensure that it was given appropriate levels of resources to carry out its mandate effectively.

While the UK does not have the equivalent of a digital safety commissioner, it is in the process of developing a new Internet safety strategy which will be introduced before the end of the year and which outlines some similar plans in terms of regulation. The UK Government published the results of its public consultation on its Green Paper in May and one of the findings from the consultation was that users, including children, felt powerless to address safety issues online and there was insufficient oversight of technology companies, as well as a lack of transparency on their part. The culture secretary, Matt Hancock, outlined plans to introduce a social media code of practice and transparency reporting as part of its digital charter and this may well become a legislative requirement in due course.

Given Ireland’s membership of the European Union, it is important to consider what is happening at a European level in order to put these proposals into the appropriate context. In July, the Council of Europe made some recommendations to its member states regarding children’s rights in the digital environment. The recommendations acknowledge the importance of children being able to access the online world and include a wide range of measures and proposals around children’s rights but also measures to protect them, including ensuring in-built safety by design, privacy by design and privacy by default as guiding principles for products and services, particularly those used by children. The recommendations also recognise that children, and those who care for them, need guidance and education. The document states that digital literacy education should be included in the basic education curriculum from the earliest years, taking into account children’s evolving capacities. While the recommendations are wide-ranging in nature and there is not the space to touch on all points here, I would like to highlight one other piece relating to them, namely, the need to identify and establish competent bodies with the responsibility and authority to implement actions in a timely and efficient manner, and that such bodies should be adequately resourced both in terms of funding and staffing.

The proposal for an office for a digital safety commissioner seems to offer several opportunities to meet the standards set out in the Council of Europe recommendations, although it could go further than the current proposals and include reference to the ethical and safe design of any new apps and games, as recommended by the Council of Europe. We would also like an explicit reference to the need to embed digital literacy into the curriculum to be reflected in the Bill. We must equip young people with the skills and know-how to navigate the online world in a safe and responsible manner. Education is an important part of any prevention strategy and

the need for digital literacy to be taught in schools is recognised in both the UK strategy and European Council recommendations. The Bill includes many significant measures and, with some additions, it could provide a strong basis for our national strategy for dealing with online safety well into the future.

Chairman: Ms Niamh Sweeney is head of public policy at Facebook Ireland.

Ms Niamh Sweeney: I thank the committee for asking me to be here today. I will give a brief overview because I have been before the committee on a few previous occasions when I provided more lengthy explanations of our approach to safety.

Every day, more than 1.4 billion people around the world use Facebook. They post everything from photos and status updates to live videos in many different languages. Deciding what stays up and what comes down involves hard judgment calls on complex issues ranging from bullying and hate speech to harassment. It is why we developed our community standards with

input from outside experts, including academics, non-governmental organisations, NGOs and governments around the world. Our community standards have been publicly available for many years and in April of this year, we published the more detailed internal guidelines used by our review teams to enforce them for the first time. We decided to publish these internal guidelines for two reasons. First, the guidelines aim to help people understand where we draw the line on nuanced issues. Second, providing this detail makes it easier for everyone, including experts in different fields, to give us feedback in order that we can improve the guidelines, and the decisions we make, over time.

We also have a safety advisory board, which comprises leading Internet safety organisations on child abuse, domestic violence and Internet safety for children and women. Facebook consults these organisations on issues related to online safety and keeping our community safe.

For the content review process, we use a combination of artificial intelligence and reports from people to identify posts, pictures or other content that may violate our community standards. These reports are reviewed by our community operations team, who work 24/7 in over 50 languages all around the world.

This year, we have doubled the number of people working on our safety and security teams to 20,000. This includes more than 7,500 content reviewers specifically. We are also investing heavily in new technology

to help deal with problematic content on Facebook more effectively. For example, we use technology to assist in sending reports to reviewers with the right expertise to cut out duplicate reports and to help detect and remove known terrorist propaganda and child sexual abuse images before they have been reported. Last month, we also announced that

we have been increasingly using artificial intelligence and machine learning to detect child nudity and previously unknown examples of child sexual exploitation imagery. Content review on this scale has never been done, as there has never been a platform where so many people communicate in so many languages across so many countries and cultures, but we very much recognise the responsibility we have to get this right.

I am here today in the context of the committee's detailed scrutiny of the Bill. Members will recall that I gave an outline of our thoughts on this topic at the 1 August hearing I attended but I am happy to be here again today as the committee considers the Bill in detail. We understand

the motivation behind the establishment of a digital safety commissioner, particularly the appeal of having an independent, statutory body that is authorised to adjudicate in cases where there is disagreement between a platform and an affected user about what constitutes a harmful communication, or to provide a path to appeal for an affected user where we have, in error, failed to uphold our own policies. We also acknowledge the Bill's efforts to ensure its scope is not overly broad, in that an appeal to the digital safety commissioner can only be made by individuals where the specified communication concerns him or her.

We very much see the benefit in having a single office with the ability to oversee and coordinate efforts on the promotion of digital safety throughout communities, much of which has been captured in the Government's Action Plan for Online Safety. It is only through this multi-pronged approach, of which education is critical, that we can begin to see positive changes in how people engage and protect themselves online.

In its 2016 report the Law Reform Commission, LRC, in addressing the nature of harmful communications, stated the following:

While there is no single agreed definition of bullying or of cyberbullying, the well-accepted definitions include the most serious form of harmful communications, such as ... so-called "revenge porn"; intimidating and threatening messages, whether directed at private persons or public figures; harassment; stalking; and non-consensual taking and communication of intimate images ...

We agree with the LRC with respect to all of these types of communication, a very stark example of which was given by Mr. John Church in his opening statement. The sharing of non-consensual intimate images, harassment, stalking and threatening messages are all egregious forms of harmful communication and are banned both by our community standards and, in some cases, the law. We fully support the commission's proposals to create new criminal offences to tackle non-consensual sharing of intimate images and online harassment where those offences are clearly defined and practicable for a digital environment. We have also taken steps to step up how we tackle non-consensual sharing of intimate images that are shared on our own platform, more information on which can be found online and with respect to which I have shared the link with the committee in our opening statement.

However, as Deputy Ó Laoghaire outlined in his remarks today and previously, the proposed Bill is currently unclear as to what precisely constitutes a harmful communication.

There is no definition included in the draft Bill but it does appear from the draft that this concept is intended to be broader than content that is clearly criminal in nature, much of which has been touched on. The exact parameters are left undefined, which could lead to uncertainty and unpredictability. I acknowledge Deputy Ó Laoghaire's remarks about the need to include a definition. We welcome the opportunity to work with him on that if that is possible. Previously, on 25 October, he mentioned that he felt that there was a need for legal certainty and we very much welcome that.

As the LTC stated in 2016, the Internet:

enables individuals to contribute to, and shape debates on important political and social issues and within states with a repressive regime the Internet can be a particularly valuable means of allowing people to have their voices heard. Freedom of expression is therefore the lifeblood of the Internet and needs to be protected.

The report continues:

...balancing the right to freedom of expression and the right to privacy is a challenging task, particularly in the digital and online context. Proposing heavy-handed law-based measures intended to provide a remedy for victims of harmful digital communications has the potential to interfere with freedom of expression unjustifiably, and impact on the open and democratic nature of information sharing online which is the internet's greatest strength.

I am aware that Deputy Ó Laoghaire is alive to these issues and has referenced these in his earlier contribution.

I will shorten my contribution because the committee is under pressure and I will finish by pointing out that Facebook has put community standards in place for the reason that we want our community to feel safe and secure when they use our platform. We are committed to the removal of content that breaches those standards, and we are keen to continue to engage with this committee and others as the Bill moves into the next phase in the legislative process.

I thank the committee.

Chairman: I call our final witnesses now: Mr. Ryan Meade, public policy and government relations manager at Google Ireland and Ms Rachel Madden, public policy analyst with Google based in San Francisco.

Mr. Ryan Meade: I thank the Chairman and the committee for the invitation to participate in this session. I work with Google in Ireland as public policy and government relations manager, based in our Europe, Middle East and Africa headquarters in Dublin. I am joined by my colleague, Ms Rachel Madden, who works as a senior public policy analyst, focusing on online safety and based in our San Francisco office but hailing from Dublin. Ms Madden's remit is global and she works closely with our product team and I am delighted she is able to join us.

Google welcomes the committee's efforts to engage with stakeholders in its consideration of the Bill. We appreciate this opportunity to outline our views on a number of the issues raised in the Bill which we feel merit deeper consideration by the committee.

Before I address these issues specifically, it might be helpful to outline Google's actions and approach to safety online. Google believes deeply in technology's ability to unlock creativity and engagement. We also believe that technology companies have a responsibility to their users; that what is unacceptable offline should be unacceptable online; and that all users should be empowered to manage online risks and make safe choices. We work hard behind the scenes to ensure that our users have as positive as possible an online experience as possible. Our approach to online safety and well-being falls into three main themes: strong community guidelines; technological innovation; and working in partnership.

We are a company fundamentally committed to access to information, yet our community guidelines and content policies offer clear rules on what we do not allow on our platforms. These often go above and beyond what is in the law and we employ thousands of staff around the world who work 24 hours a day to ensure violations of our guidelines are acted upon.

On technological innovation, Google has aimed to be the industry leader in creating and developing products and tools which help protect and empower our users, and we will continue to invest the resources necessary to ensure families can make safety choices that are right for them.

We developed YouTube Kids to offer an alternative YouTube specifically designed for

young children. It provides a restricted version of YouTube for families with built in timers, no public comments, no option to upload content and the ability for parents to block or allow access to specific channels or videos. Last year, we launched Family Link, which enables parents to create a Google account for their child and then helps them set and tailor the digital ground rules that work for their children including on-screen time, device bedtimes and approving or blocking specific apps or functions like the camera. Ireland was the first country outside of the US in which we launched Family Link and it has since been rolled out in 170 countries.

My colleague, Ms Madden, will be happy to speak more about these online safety products we have developed. At Google, collaboration has been key to ensuring our products and services offer families a positive and secure experience online. That is why we work regularly with NGOs, Government and industry partners to empower parents and children with the tools and skills they need to make the most of the Internet. Companies like Google have a responsibility to ensure not only that products and services offer a great user experience but that we work with a wide range of stakeholders and industry partners to creatively and effectively raise awareness, offer support on how to navigate technology responsibility and share technological solutions to tackle some of the toughest problems we face. Google has invested considerable resources in these efforts and has thousands of employees across the companies working in this regard. More detail on each of these teams is included in the written submission to the committee which has been circulated. The submission also includes views and suggestions on the Digital Safety Commissioner Bill which are drawn from this overall approach as well as from our knowledge and experience of the practical implications associated with these issues. We are also happy to provide a more detailed written submission if that is considered appropriate.

In the time available, however, I can set out briefly some of the points we believe the committee should take into consideration. In doing so, I echo some of the things other witnesses have mentioned already. Google welcomes the recognition of the need for ongoing awareness and education on harmful digital content. We support an approach which includes national initiatives to educate Internet users on what it means to be a responsible online citizen, the resources and tools available to protect their privacy online and how to deal with and report cyberbullying, inappropriate content and online abuse. Google also welcomes the consideration of additional measures by Government to address the posting online of videos or images with embarrassing and intimate content, often referred to as “revenge porn”. This amounts to an egregious invasion of an individual’s privacy as other witnesses have already said. It is essential that any new legal framework in Ireland reflects and is consistent with the laws governing online services in the EU, in particular the e-commerce directive. In particular, we highlight the need for national legislation to reflect the notice and take-down procedure specifically envisaged in the e-commerce directive at articles 12 to 14 together with the prohibition on imposing general monitoring obligations contained in article 15.

I will not repeat the point on the need for a definition of “harmful communication” which was made by every other witness except to say that we agree that a clear definition would provide legal clarity for all parties. We welcome Deputy Ó Laoghaire’s comments in that regard. The delineation of responsibility between the digital safety commissioner and the Data Protection Commissioner merits deeper consideration as the Bill progresses, in particular in light of the Data Protection Commissioner’s responsibility for dealing with complaints by individuals related to their data protection and privacy rights under the GDPR. As a general point, we ask the committee to ensure that any legislation is future-proofed by making it as technology and platform neutral as possible. I will finish there except to ask the committee to take those points on board as it continues its deliberations on the Bill. The suggested changes would make the

legislation more effective and increase clarity in its application. I thank the committee for its time.

Chairman: The committee would welcome any further written submissions and detail. That goes for all witnesses as we progress through our discussions on the Bill. Any input in writing would be very welcome. I will start by asking a number of questions and then open questioning to members of the committee. Witnesses might want to note the questions.

I note to the departmental witnesses that one of the issues raised last week by the Minister, Deputy Bruton, was the need to be conscious of the nexus between the ministerial responsibility and the role of the digital safety commissioner. Are the witnesses in a position to elaborate on that? My understanding of what the Minister said was that he is there to put forward policy and to ensure it is delivered which would not be the role of a statutory body. I might be mistaken but perhaps the witnesses could elaborate on it. Has the Department had an opportunity to review Australia's Enhancing Online Safety Act 2015? Has there been any engagement with the Department's Australian counterpart as I understand the legislation there is working well? Common law issues arise in that jurisdiction which may be similar to issues arising here. Will the Attorney General's evidence be made available to the committee in respect of its work on this legislation?

I turn to the witnesses from Facebook. Facebook has said previously that it is broadly supportive in principle of the creation of a digital safety commissioner role and we welcome that. There are some issues around the definition of "extraterritorial" and the effect of that on the legislation. What has Facebook's engagement with Australia's eSafety Commissioner been or are the witnesses in a position to expand on that today? How is the process working? It seems to be working very well. There is very little conflict. I heard an interview with the Australian digital safety commissioner in which she said that her engagement with social media platforms has been very good and quite effective, to the point that fines are not always needed. I do not think she has ever used fines. Her engagement with social media platforms has been very positive. I would welcome the views of the representatives of Facebook on the company's interaction with the Australian setup.

I thank Mr. Meade of Google for his comments. I ask him to expand on his request for the Bill to be as platform-neutral and technology-neutral as possible.

Do the witnesses from the ISPC have a breakdown of the most common complaints? Can they provide any figures for the complaints which are coming before them? Do the complaints relate to cyberbullying? It would be useful for the committee to get a breakdown.

The need to define what constitutes "harmful communication" has been a common thread throughout this discussion. I appreciate that it would be difficult for the witnesses to formulate a definition here. The committee would welcome any assistance that the witnesses who are in attendance today could provide with regard to the definition as we move forward with this legislation.

When Ms Cooney spoke on behalf of CyberSafeIreland, she referred to "the ethical and safe design of any new apps" and to "digital literacy". I would be concerned that if this legislation is too broad - if the digital safety commissioner has too broad a role and too wide a remit - it may be less effective. It might be preferable to limit our endeavours in this regard to the areas of online content focused on in this legislation. A narrow focus is needed, certainly initially. If we need to build on that remit in future years, that could be done. I would be cautious about

extending the remit in case it becomes too wide because it would not be effective in such circumstances.

I would like to get the witnesses' views on that. I have also asked for their views on what constitutes "harmful communication" and for any data or information that might be available to them in this regard and could be provided to the committee. After they have responded to my questions, I will bring in Deputies Stanley and Lawless.

Ms Patricia Cronin: I will respond to the Chairman's questions about the policy area and the Office of the Attorney General. My colleague, Ms Quill, will answer the Chairman's questions about engagement and cover off the Australian e-commissioner angle.

As the Chairman has rightly said, the role of the Minister and the Department is to look at the policy context at national and European levels. Our job is to set legislation in a broad policy context. There are many examples of areas in which external implementation bodies have been established. There is a great deal of European legislation. Reference has been made to the audiovisual media services directive, which is coming down the tracks for us. When that is finalised at the end of this month, our job will be to consult on the online safety aspects of the directive and on the co-regulation of video-sharing platforms. We will look at what the Commission has set out and we will work with the Minister to figure how that will be transposed.

I will set out the choices here. We must choose to have either secondary or primary legislation. We have to decide what the national regulatory authority will be. We have not made up our minds on that. We will have to speak to the Minister. He will make that decision. That will be an important component of this process. We will also have to decide how we will transpose the requirements of the regulation. That is broadly how we will do things in this area.

Many speakers have alluded to the fact that there are many players in the area of online safety. The Department of Justice and Equality has a role in respect of any content that relates to terrorism. It manages the transpositions in that area. The Department of Business, Enterprise and Innovation has a role in respect of e-commerce. The online world is fairly complicated. The broad policy context is certainly put in place by Government Departments.

I can tell the Chairman in response to her second question that the Minister for Communications, Climate Action and Environment, who is still relatively new in the job, asked us to write to the Office of the Attorney General to get its advice on certain aspects of the Bill. As Deputy Ó Laoghaire has recognised, some of it is quite complicated. We have sought the advice of the Office of the Attorney General on aspects of the Bill that have been mentioned, including the definition of a "digital service undertaking". We have considered how it interacts with the e-commerce directive and how matters involving entities outside the State would be enforced. We have sought advice from the Office of the Attorney General in that regard but will have to ask it whether such advice could be shared as matters such as legal privilege must be considered. We are happy to ascertain whether the advice may be shared and will revert to the committee in that regard.

Ms Triona Quill: On the Australian office for digital safety, a key aspect worth bearing in mind is the different legal frameworks within which we operate, particularly in the context of our membership of the European Union. The e-commerce directive 2000 sets out the limitations on legal liability that apply to digital service undertakings. As Ms Cronin pointed out, that is an issue on which we have sought advice from the Office of the Attorney General. It must be recognised that there are differences in the legal framework which may impact on the capacity

of an office in this jurisdiction to operate in the same way as a similar office in Australia. That is probably the key element to bear in mind when considering the system in operation there. In addition, aspects of the Australian office for digital safety focus solely on children rather than the broader focus on all citizens - while recognising the particular vulnerability of children - as proposed in the Bill. In particular, legal liability is an issue that needs further reflection and examination.

Chairman: Does Ms Sweeney wish to contribute?

Ms Niamh Sweeney: It has been some time since I spoke to my counterpart in Australia regarding how things are working there. Ms Quill is correct insofar as the last update I received stated that the commissioner there has never used her official powers, although there is much consultation and ongoing work with the platforms. When I last spoke to my colleague on this issue, I knew of early anecdotal evidence to suggest that the office was not necessarily operating in the way one might have anticipated. For example, some reports regarded hacked accounts rather than specific instances of harmful communication. In other instances, complaints were not first reported to the platforms, such as Instagram and Facebook in our case. Rather, the affected user went directly to the commissioner. Obviously, we would still work with the office on such complaints but the system there was not necessarily working as envisaged. The numbers there were quite low in its first year. I do not know the numbers for 2017, but they probably reflect how it played out in 2016. That said, there is ongoing interaction between my organisation and the commissioner there.

Chairman: The committee would welcome any update in that regard which Ms Sweeney could provide it in writing.

Ms Niamh Sweeney: I will ask that an update be sent to the committee.

Chairman: The committee will liaise with its Australian counterpart to see how the system is working there. It would also welcome the viewpoint of Facebook in that regard. I call Mr. Meade.

Mr. Ryan Meade: I wish to make clear that the final point in my submission, when I asked the committee to attempt to make the legislation as platform and technology neutral as possible, is a general one which I regularly make. I do not suggest that the Bill is running the risk of being too technology-specific. It is important to bear in mind that when framing regulation one looks at existing practices and industry players and how technology is used. However, by its nature, technology changes. If we were discussing legislation such as this three or four years ago, issues such as the use of ephemeral content available through Snapchat and other apps which involves content that disappears after a time might not have been considered. That is very much a general point. I am not suggesting that any specific provision of the Bill will limit its usefulness in the future. However, when considering regulation in this area, ideally one would have a framework that will stand the test of time. I ask the committee to bear that in mind.

Mr. John Church: The Chairman asked about numbers and trends. The ISPCC has identified some trends in this area. We run Childline, a confidential listening service, which will probably answer approximately 1,200 calls today from children under the age of 18. Approximately 6,000 of the 350,000 calls received by Childline last year related to online bullying. We very often deal with the issues caused by bullying in general and our categorisation deals with behavioural issues as well as issues such as domestic abuse, sexual abuse, body image, online

abuse and other bullying. It causes us to look at our statistics and how we categorise it. If one considers the use of our online platform, last year we had just less than 30,000 conversations compared to just under 4,000 ten years ago. This is going to become an issue and I believe we will have to look at how we categorise conversations. When one looks at trends, we often use Childline figures but we also consult our child support workers in the community who do one-to-one counselling therapeutic interventions. We also have voluntary children's advisory committees set up. In those latter two areas we see a bigger rise, which is not fully reflected in our numbers.

The Chairman also asked about harmful communications and definitions. My colleague, Ms Jennings, will elaborate on that.

Ms Fiona Jennings: On defining harmful communications, and the exercise that is before the committee, we would refer to the consultation the Law Reform Commission had with the young people and the different themes, issues and behaviours that they identified as harmful. The Law Reform Commission brought that information, along with the extended consultations it had, and it looked at issues such as the taking and distribution of an intimate images without consent, the setting up of false accounts to cause or intend to cause harm, and stalking or actions that would cause alarm, distress and harm. As Mr. Church said earlier, we would encourage the committee to create a definition that is not overly broad and which is workable. In Australia, the Enhancing Online Safety Act 2015 pertains to cyberbullying but it also has quite a niche definition that covers material that is seriously threatening, seriously intimidating, seriously harassing or seriously humiliating. New Zealand has a Harmful Digital Communications Act 2015. New Zealand does not have an entity such as our Digital Protection Commissioner. It has an approved agency called Netsafe. The New Zealand legislation looks communications principles, including where a digital communication should not be threatening, intimidating or menacing, and should not be used to harass an individual. There are several other principles also and I believe they would be a good starting point when looking to create a definition of harmful communications.

Chairman: Would Ms Cooney like to respond to that same question on harmful communications?

Ms Alex Cooney: I agree with my colleague that we should look at the existing definitions in the Australian and New Zealand context that have been approved and are working in practise, and that we should look to have something similar here.

Chairman: Did Ms Cooney want to come in on something else?

Ms Alex Cooney: Reference was made to digital education and safety design. The Australian model has education as part of the remit, which is worth knowing, and that function is used. The office does awareness raising with parents, produces resources and so on. That mandate is there. The focus was just on children and cyberbullying, but in 2018 it has been extended it to all Australians. It is increasing its mandate, which is one of the observations that has been made as time has gone on. It has also been suggested that increased resources be made available to the office. I believe it has dealt with some 500 cases to date.

Chairman: I thank Ms Cooney. I am going to bring in other members. If the witnesses want to come in on any of the questions, then please just indicate to me and I will let them in.

Deputy Brian Stanley: I will deal first with the presentation by CyberSafeIreland and

the Irish Society for the Prevention of Cruelty to Children, ISPCC. There is a feeling and a view being propagated out there that the Internet has empowered everybody now that we can connect with people all over the world. According to Facebook there are 1.4 billion users on Facebook daily. I believe the Internet has had a hugely disempowering effect in some ways. CyberSafeIreland highlighted the UK survey where adults and children felt powerless to address online safety issues. If they are powerless to address their own safety they are seriously disempowered. It is useful that Ms Cooney highlighted that and the insufficient oversight today. The example given by the ISPCC of the 15 year old girl is shocking. That is a life and death issue because she feels she wants to kill herself. Facebook and Google talk about their online communities. There are no communities of 1.4 billion people. Communities are a different entity and it is a misuse of the word by Facebook and Google. In real communities we know, unfortunately, of cases like this where lives have been taken over issues such as revenge pornography and bullying of young people online. That is the context for the important Bill that Deputy Ó Laoghaire has brought forward.

Google highlighted the importance of education and said that it alone could solve the problem of online bullying. That is what it seems to indicate in its presentation. Education of itself will not stop somebody who wants to misuse the Internet. That is a huge challenge for Google and Facebook and for us as legislators to deal with. Will the witnesses from Google address that issue in more depth because stating that education alone could deal with this does not do justice to or deal properly with this? We will need strict criteria and legislation and means of enforcing that.

Facebook says it has 1.4 billion users every day. On the last occasion it was here, in August if I remember correctly, it stated that it has 20,000 people moderating what is online. I was surprised by that number but it shows the extent of the problem, the challenge and difficulty of trying to moderate what appears on the platform. Does this show the witnesses that this problem is nearly impossible to deal with? That is probably one of the biggest challenges facing the company, us as legislators and governments around the world. Does that highlight the need for direct State intervention?

In its presentation Facebook highlighted the need for freedom of expression. As somebody who campaigned against section 31 of the Broadcasting Act 1960 throughout the 1980s and 1990s which was repealed by Uachtarán na hÉireann, Michael D. Higgins, one of the best things he ever did, I do not think we want to limit freedom of expression too much. A line, however, has to be drawn around safety and what should be allowed. Do the witnesses from Facebook and Google believe that it should be left to private companies and corporate entities to define what should be tolerated in terms of freedom of expression or is it for government bodies to do that?

The Law Reform Commission's definition of offences refers to pornography, intimidating and threatening messages whether directed at public figures or private individuals, harassment, stalking or non-consensual taking and communication of intimate images. What role should Facebook and Google have in addressing the issue of fake news and the spread of misinformation about individuals? Politicians have been targeted with this type of misinformation in the past, and, in some cases, it has had detrimental effects. Such misinformation included false accusations against public figures. Should that be included in the definition of "harmful material"?

The Department mentioned that certain minimum standards would be set. As a member state of the European Union should we be entitled to add to that and threaten more stringent

regulations? Does the Department feel that Deputy Ó Laoghaire's Bill is in any way counter to EU law, and if so in what way?

My final question is for Facebook or the Department. Who should fund the office of the digital safety commissioner?

Mr. Ryan Meade: I hope I did not give the impression that we believe that education alone is a silver bullet in this case; I apologise if that impression came through in any of the presentations. We are trying to emphasise, in our approach to online safety and in the collaborative work we do, that there is no silver bullet to prevent bullying or any other online safety issue. We are highlighting the importance of education. Most witnesses will probably agree that educating and empowering users is one of the key planks of any strategy for online safety. I did not want to give the impression that we believe that education alone can solve the issue of online bullying or any other online safety issue, which is why I laid out the different themes we address in our approach to online safety. Education and empowerment fall under our work in partnership with other organisations. I also highlighted our technological innovation in terms of the tools we have sought to put in the hands of users and families. We also have community guidelines, and I will ask my colleague, Ms Madden, to talk about those.

Ms Rachel Madden: We do not want anyone to feel powerless to manage his or her online safety when using our products and services. I do not believe there is one solution for these complex issues. We firmly believe that what is unacceptable offline should be unacceptable online, and we have strong policies in place on certain platforms, such as YouTube, to address bullying and harassment. We do not allow abusive videos or comments on our platform. Beneath every video and beside every comment on YouTube there is a "flagging" option which allows anyone to report content for review. Facebook has teams based around the world, working 24-7 to analyse these reports, and if content violates our policies it will be removed. We also work in partnership with other organisations. We have a trusted flagger programme, involving individual members of the YouTube community - I apologise for using that phrase because I know some people do not like it - non-profit organisations and Government agencies. These non-profit organisations are often experts in certain areas and are helpful in notifying us of content that might violate our policies on bullying or other areas. We will quickly remove that content when we are made aware of it.

Ms Niamh Sweeney: To avoid any confusion, we have 20,000 people working at Facebook on the wider safety and security of the platform, and just over 7,500 content reviewers. The remainder of the 20,000 could be working on artificial intelligence, machine learning or various technical solutions to keep the platform safe. The Deputy is right that it is a big challenge because content review has never been done on this scale. On the need for direct State intervention, we receive millions of reports every week and if the State were asked to step in and do what we, Google and others do, it would be challenging to say the least.

There was a question on freedom of expression and whether it should be for Facebook to determine what should be left up and what should be taken down. That is an important part of the conversation. As Ms Quill said, we operate within the e-commerce directive in the area of illegal content and if we are made aware of illegal content on our platform, we have to act expeditiously to remove it. In other jurisdictions it is different, such as in Germany where the NetzDG Act covers illegal hate speech. In Ireland, it is left to us to discover what is illegal and many people have an issue with being left in a quasi-judicial position in this respect. We have a short period to determine what is illegal and there is a tendency to err on the side of caution, given the exposure companies have if they do not remove the content over time. If there is legal

exposure for companies for pushing the boundaries on what constitutes freedom of expression, we could end up with the mass removal of perfectly legal content which may offend, shock or disturb but is not necessarily illegal.

On false accusations against public figures, we were part of the high-level working group on false news convened by the European Commission over the summer. This issue has travelled some distance since then and the focus now is more on electoral integrity. We have made a number of commitments as part of that and the Commissioner, Věra Jourová announced the agreed outputs in mid-October. We have undertaken to introduce additional tools with respect to electoral integrity this side of the European elections and we are working hard on this, which is in addition to the tool for viewing ads which we rolled out in April. This allows one to see any advertisement which an advertiser is running at the same time and addresses the idea of dark-outs.

If false accusations against public figures ever drift into defamatory territory, a clear process is in place. We have a dedicated reporting forum, as does Google, which is used to report defamation, which we know can be damaging. It is separate to reporting through our normal reporting channels, which are attached to every piece of content on the platform. We take this seriously.

Another question was on who should fund the office. I suspect that if it was funded by us it would attract criticism.

Deputy Brian Stanley: The BAI receives funding from the sector, as well as the State, and I do not suggest Facebook would be the sole funder. Can the witnesses address the question on whether a private company should decide what is harmful and what is not harmful?

Ms Rachel Madden: As with Facebook, we deal with this using a two-pronged approach. We abide by local laws and if anything violates a local law, we will restrict it in the relevant jurisdiction. We have also developed policies and our trusted flaggers and other experts, on whose expertise we lean heavily, inform those policies. This collaboration helps us stay one step ahead because, like the offline world, the trends of the online world morph-----

Deputy Brian Stanley: Should it be left to Google to decide what is harmful?

Ms Rachel Madden: That is a very good question. We have a huge set of standards available for anyone to see.

Deputy Brian Stanley: What, then, is the answer from Google to my question?

Ms Rachel Madden: We would welcome any collaboration in this space and we collaborate to ensure we set the correct rules. Our policies often go above and beyond the law. That is something of which we are very conscious and which we take into account when developing them.

Mr. Ryan Meade: As Ms Madden stated, there is applicable law that Google applies, which is the law set by legislators and so on, and then there are Google's own standards in terms of what we consider appropriate on our platforms. In the latter case, we try to set a standard that responds to our users and to what society wants but, similarly, we are responsive to what legislators-----

Deputy Brian Stanley: Is Google happy that the proposed digital safety commissioner

would decide what is harmful and what is not and what is acceptable and what is not? Is Google happy to go along with that?

Mr. Ryan Meade: The point we have made is that there should be a clear definition of what constitutes harmful communication. That would provide legal clarity not just for Google-----

Deputy Brian Stanley: Is Google happy for that decision to be made by the proposed digital safety commissioner?

Mr. Ryan Meade: The point we have made is that it would be more appropriately made by legislators.

Chairman: I will bring in Ms Cronin from the Department.

Ms Patricia Cronin: I will deal with the education aspect and with the Private Member's justice Bill. Ms Quill will address the European Union requirements. One of the witnesses from Google mentioned the education aspect. A collaborative approach has been taken across Government in respect of the action plan for online safety because of the nature of the latter. There are a number of actions in the education sphere that are the responsibility of the Department of Education and Skills, with timelines for when they are to be delivered. It is a broad plan comprising, as one would expect, many actions being sought by that Department.

In terms of some of the points that were raised about revenge porn, there is a Private Member's Bill, which was not opposed by Government and which is before the justice committee - although I am sure where it stands - that examines some issues such as stalking, non-consensual distribution of intimate images or the taking and distribution of intimate images without consent. That probably covers some of the areas raised by a representative from the ISPC. I will ask Ms Quill to address the European Union requirements.

Ms Triona Quill: As the Deputy mentioned, there are two levels of legal frameworks that we need to consider, namely, the national and the European. There would not be anything preventing national law in this area but it would have to respect the European framework and the Irish legal framework. One of the issues on which we have sought clarity from the Attorney General's office is in respect of the Irish legal framework with respect, for example, to whether a body such as the proposed office of the digital safety commissioner could exercise extra-territorial jurisdiction as a matter of general principle where there is not a universally accepted principle of international law. In other words, in the case of something in respect of which there is not an international or a European norm, can the State reasonably impose its jurisdiction on a body that is established outside the State? That would be one aspect to bear in mind in this regard.

In terms of adding extra national measures, we can do that but they would have to abide, as Ms Sweeney and others mentioned, by the European framework relating to the e-commerce directive. If content is illegal, it is provided for under that mechanism. If somebody brings to the attention of a platform a matter relating to illegal content, that platform has an obligation to take down the content. If a matter is not illegal but might be considered to be harmful in some way - issues relating to cyberbullying might fall into that category in some instances whereby, for example, children are bullying each other online but that may be extremely harmful content, for example, revenge porn or whatever, that might be categorised as criminal in nature - it is trickier to deal with precisely because it is not a criminal matter. It may be harmful but it is trickier to deal with because there is not a universally accepted definition and it is not provided

for under the e-commerce legislation. If the definition as set out in this Bill sticks to criminal acts that are provided for, or are going to be provided for, it is probably on clearer legal ground than if it is going into less clear territory. We will have more insights when we get legal advice back from the Attorney General's office.

Deputy James Lawless: I thank the Chair and I thank the witnesses for their interesting presentations today. This is one of three pieces of legislation to be dealt with in this Oireachtas term. I congratulate Deputy Ó Laoghaire on proposing, drafting and bringing it forward. Deputy Howlin has a Bill on harmful offences and I have my Bill on social media regulation, on which some of the witnesses have been in attendance already and some are due to come before us in the near future. There has been a focus on the online space in this Oireachtas which is welcome. It is fast-moving and has been said already, some of the hearings that we had during the summer are almost obsolete now because of the events that have happened and moved on so quickly where steps have been taken both voluntarily and otherwise by the main stakeholders which is good to see.

It is a fast-moving space and one feature that those three pieces of legislation have in common is that they all relate to attempts at regulation. We probably all agree - although the witnesses may not - that self-regulation is not desirable or ideal. While it is welcome that attempts have been made at different times, it is always stronger if an independent third party body can try to impose that regulation.

On the specifics of the Bill, it looks good, where I have read through it a number of times, as well as having followed the Second Stage debate. Some of the feedback from today and previously goes to the heart of definitions and the devil is in the detail. The trick with drafting is always to get it precise enough that it can be enforced but broad enough, as Mr. Meade has said, to be technology-agnostic or platform-agnostic, in order that it can be long-lived and robust enough that, in five or ten years time, it can still be applicable.

There has been a lot of talk about the definition of harmful communications. It is probably one of the main definitions that Deputy Ó Laoghaire has indicated he may want to draft or fine tune as we move towards the next Stages.

One interesting matter that also got a mention in the submissions to the Law Reform Commission's reports and in previous studies in this area - the commission's principal report on this issue was in early 2016, I believe, to which I made a submission - was section 10 of the Non-Fatal Offences Against the Person Act 1997. This is what we call the classic harassment, which is what we might call the pre-Internet harassment. This would be the old stalking offence of knocking on someone's door or sending them postcards or harassing in more traditional ways.

There is a school of thought legally that section 10 could apply to the Internet as well. The stumbling block to date has been that the offence or activity must be repeated to bring it under the definition of section 10. Making a phone call or knocking on somebody's front door in a one-off action may not qualify in the traditional world. Doing it ten times or 100 times would qualify. There is a school of thought that says the nature of the Internet is something that is shared, so anything could be posted once, but it could be shared 100 if not 1,000 or 100,000 times. That might bring it under the definition of section 10, which would mean the action was repeated which might be sufficient to bring a prosecution as it stands.

My first question is whether any of the witnesses has a view of this as to the existing legislation like section 10 of Non-Fatal Offences Against the Person Act or other legislation that may

be out there, and are these sufficient or adequate? Has the DPP or any other agency brought charges of this nature to date? Have these types of issues come before the courts or received a sanction and, if so, under what legislation? I would be interested to hear the witnesses' expertise. If these issues have not arisen then what governance is in place? Is it the case that there is a vacuum of governance? If the existing legislation does not apply or has not led to any charges, what exactly is controlling the Internet space at the moment? If the answer is nothing then that is very worrying but is all the more reason we need to accelerate this Bill and others like it.

Moving on and staying with the Bill, it is very positive, strong and a very good idea. One thing that it does not appear to do is to create new offences. This may be deliberate. Deputy Howlin's Bill creates some offences. Perhaps the legislation can be dovetailed so that the offences in other legislation would come under it. In terms of sanctions, there has to be a carrot and a stick. While there is provision in the Bill to seek an injunction in the Circuit Court, which is useful, the Data Protection Commissioner has powers to bring prosecutions in court as does the Companies Registration Office. Perhaps that is something to be considered in Committee Stage amendments, if we get to that point. There are many examples of statutory agencies which can bring a non-Garda prosecution. Different Departments have similar powers. I might come up with some amendments in that regard myself, but I could also work with Deputy Ó Laoghaire. It might be worth adding to it. On the carrot and stick approach, the concept is that the digital safety commissioner role would not only involve enforcement but would also provide an independent and objective agency in debates like the one on the digital age of consent which raged a couple of months ago and which I do propose to reopen today. It got quite controversial at times. An external agency unconnected to any of the platforms or to any political party would have the status to make recommendations on issues like that. It would receive a good hearing and get good traction across the board. There is a great opportunity, as envisaged in the Bill, for the commissioner to perform that advocacy and expert role, which would be useful.

To recap, I ask about legislation. There is a question mark over section 10 and whether it could be applied at the moment. Are there existing legislative provisions which apply? If not, are we in a total vacuum? What is the current legislative framework around these kinds of offences, if they even exist at the moment, and whether they can be prosecuted? What has been the experience to date?

Chairman: Those questions are mainly for the Department. I might bring in Ms Cronin.

Ms Patricia Cronin: We have gone to the Office of the Attorney General to look for a definition of "harmful". We can bring section 10 to its attention, as referred to by the Deputy, and ask if it feels that is relevant. We will get a response there. The question of the DPP is perhaps more properly a matter for the Department of Justice and Equality. The Department is in the space of illegal digital content. I do not have the answer to be honest. We have gone to the Office of the Attorney General on various aspects of the Bill and await its advice. However, we did not ask about offences or sanctions. Perhaps Deputy Ó Laoghaire can discuss that.

Chairman: Does the Deputy want to come in on any of that?

Deputy Donnchadh Ó Laoghaire: Deputy Howlin's Bill addressed updating section 10 of the Non-Fatal Offences Against the Person Act. We supported that Bill. Section 10 is out of date and needs to be updated because it does not take account of the very significant changes which have happened. In relation to offences, Deputy Howlin's Bill and mine had their origins in the LRC paper published in early 2016. In drafting the legislation on foot of the proposals of

the commission, I was conscious of the fact that this is a specific proposal to establish an office and provide it with a remit. While I am open-minded about it, I am not sure this Bill is a suitable place to update section 10, notwithstanding my support for the principle of updating the law on criminal offences and on creating new offences. However, doing so in this Bill might complicate the work of establishing an office, providing it with a remit, and creating codes of practice and national minimum digital safety standards. While I am open-minded, my initial view is that introducing criminal offences in the Bill would enter into the area of creating criminal justice legislation. As such, our work could become complicated.

The argument is also relevant to the view I take on the definition of “harmful communication”. I spoke on last occasion we met about what that might involve. I outlined that in general it would include distribution or publication of an intimate image of another person taken without consent, or threatening to do so; taking or distribution or publication of an intimate image of another without consent; distribution or publication of intimate material where it seriously interferes with privacy or causes alarm, distress or harm to the other person; the distribution or publication of a threatening, false, indecent or obscene message to or about another person for the purpose of causing alarm, distress or harm to the other person, or where it is done persistently; and persistently communicating with a person in circumstances in which it seriously interferes with the other person’s privacy or which cause alarm, distress or harm and any other inchoate behaviours related to the same. I am working on the drafting with regard to how it would be structured. We should be looking at behaviours. I take on board the point made about consistency with the e-commerce directive. When we ask the commissioner to take down material, we should outline to him or her, and the providers, the behaviours. We should not ask them to adjudicate at the point of takedown on whether something is illegal because there are behaviours that are close to the line. They might have to be removed quickly and for the person involved to get redress. We should look at behaviours rather than seek to state that certain matters are illegal and that the illegal content should be removed. They are required to do that anyway under the e-commerce directive. We should target behaviours. I agree with the point made about an independent external agency. It is important and it is the principle on which we are all largely agreed. I made the point at the previous committee meeting that the organisation is constantly in communication with the providers and platforms but it also receives complaints when they are unhappy with how the providers and platforms are addressing matters. They will be the first to know of the changes in abuse and harassment and all these harmful communications. They will be in a strong position to advise Government on any future criminal justice or policy approaches for example in the Department of Education and Skills. All of that kind of stuff changes. The curriculum might change with the NCCA. It would be in a strong position to do that.

Chairman: Does anyone else want to comment on that?

Deputy James Lawless: Before we move on, the representatives of the platforms would know if they have been before the courts. It is probably something they would be aware of. Have any charges been brought under section 10? Have the platforms been involved, not necessarily as a defendant but perhaps as a third party? Have any of the platforms been in the court? Are they aware of any existing legislation in an Irish context being used in this area to date?

Ms Niamh Sweeney: I am wary of getting into a conversation about section 10 of the Act given the Deputy is a lawyer and I am not. I am not aware but I would have to check. My understanding is there is a view that section 10 applies online but it has not been tested in many instances. As Deputy Ó Laoghaire said, I think it was the ambition of the LRC, with its draft

Bill which Deputy Howlin has moved forward, to make it more explicit. As I said earlier, we would be supportive of it where it is clearly defined and practical for the digital environment. That is where one has to ask what harassment is because there are very different views on what the threshold is for different individuals. Platforms would need very clear guidance on where that line is drawn so they would have legal certainty.

Mr. Ryan Meade: I am not in a position to provide legal commentary on section 10. I do not have specific cases that were before the court. As I said in my opening statement, our view is that what is unacceptable offline should be unacceptable online. Similarly, if there are offences that are clearly defined and which apply offline we support ensuring there is a corresponding offence online. We support the spirit of ensuring that if there is an offence of harassment that it also apply online. If there are any particular gaps in that, we think it would be worthwhile addressing.

In terms of cases before the courts, we have procedures for law enforcement to engage with us when it comes to gathering evidence for offences and so on. I can provide some more information on that at a later date if the committee wishes. If there is a clear offence, we can co-operate to help prosecution.

Deputy Eamon Ryan: It has been a most important discussion. Mr. Church gave the horrific example of the young girl whose images were shared by a former boyfriend. It is shocking. There is wider concern that during this ten-year increase in the demand for online services, there has also been a significant increase in the incidence of depression and other psychological problems among our young people. A lot of reports I read, and I must admit I have spent the past hour frantically reading as much as I could on the Internet via my own device, show a correlation between the increasing levels of depression, anxiety and other mental health difficulties among young people and the increase in the time young people are online. The harm might not come just from the obvious graphic terrible example but in all sorts of subtle ways, such as exclusion or other mechanisms that affect mental health. Do the witnesses make this direct connection? Everything I have read from the various psychology sources shows an increasing level of depression, anxiety and mental health problems, particularly among young girls it would seem, so that we can make the correlation with the increased use of online services particularly on mobile phones.

Things have developed a lot recently with the passing last month by the European Parliament of the revision of the audiovisual media services directive. I presume it is a foregone conclusion and that the Council will approve it before Christmas. I understand that approximately 80% of all online content is video. Did Ms Cronin state in her contribution that we are looking for regulatory bodies to manage some of this? Given that the BAI is involved in the audiovisual media regulatory environment, and given that the report from the European Parliament had similar issues of concern to what we have here and it very strongly focused on the effect of online media services on young children, if we are looking for an institutional body to house regulation, the BAI might be suitable. We could look at the Data Protection Commissioner or creating a new agency but the BAI might be best placed, given that it is so versed in audiovisual media. What is the difference between online media and broadcast media? For young people the vast majority is online. I am interested to hear the views of the witnesses on this.

I am keen to hear from the companies on last month's report of the European Parliament. Paragraphs 20 and 21 of the report call for the use of encryption and much greater parental control mechanisms to protect young children. Paragraph 21 states personal data of minors processed in the framework of technical child protection measures should not be used for com-

mercial purposes. Does this not call into question the companies' entire commercial approach in the processing of minor's data in particular? It must change. As Tim Berners-Lee said yesterday, the companies are damaging the Internet and causing a threat to it and all the immense benefits it brings, and their commercial model must change. How can the companies live up to the direction from the European Parliament in the new audiovisual media services directive if they do not know with absolute certainty the age of the child being dealt with? We have heard in previous evidence that the current mechanisms they have in place clearly do not do this and the companies cannot tell if a child is 13, 15, 16 or eight. They can say they do but they do not have effective commercial mechanisms to do it. Does the new directive mean they must set in place new mechanisms to guarantee knowing the age of the minors who are on their networks so they can live by the commitment not to use the data for commercial purposes? How can they do this if they do not know whether the person is a minor? In this regard, Ms Cronin said age verification looks like one of the key new regulatory requirements we will see. I do not have the exact wording but if I read her submission correctly the inclusion of age verification may well be one of the new regulatory measures we will seek to put in place. I would welcome that, given the evidence Mr. Church and others have presented here on the health implications of the use of some of these services.

Mr. John Church: I will respond first. The short answer is that there is no research to prove that correlation. However, as I said earlier, we take many calls every day. It is 1.05 p.m. now and Childline has probably received over 500 calls today. I am only three months in the job so I am new to this and much of my time was spent listening and shadowing some of the calls. I only relayed one case example today but there are hundreds. What we are seeing, as well as from talking to the volunteers online, are behaviours that are causing significant issues for the child. As the Deputy described, they are subtle things such as exclusion by not being invited to a party or not being part of a WhatsApp group, which in effect is bullying. I mentioned earlier that we will have to start considering how we should categorise those calls. If a child mentions in a confidential call that he or she is subject to online bullying, that is categorised as online bullying but far more conversations we are having with children every day are about issues they are having relating to online issues. We would certainly love to see far more research around that and whether it is a correlation. Intuitively, I would agree with the Deputy but there is no research that I know of to show that.

I also mentioned that we are seeing a slight decrease in telephone calls. Incidentally, it is young boys who are calling online, which is interesting. One would tend to think it would be girls calling because they are sometimes better at conversing, but the boys appear to find the online calls a great source of support. We are seeing a switch from calls to online chat and this has forced us to upgrade our online platform, which we are launching next week. With the launch of that platform we can get into many more in-depth conversations and that is when we will start gathering a great deal of research around this.

Ms Alex Cooney: I regularly talk to teachers and principals and they are definitely seeing the fallout in the classroom, with children coming in tired or falling out over cyberbullying incidents or gaming. There is a clear dynamic. I spoke to a principal yesterday in preparation for anti-bullying week next week and he said that in the ten years he has been a principal the change has been stark. Obviously, in the early years as a principal he was dealing with bullying but the amount of online instances he now has to deal with is just incredible. That has an impact on the schools each day. As our survey showed, teachers are dealing with this in the classroom all the time. Anecdotally, therefore, there is good evidence.

A survey published in the UK this year found that girls who were using social media at ten years of age for an hour a day are far more likely to have social and emotional problems at 15 years of age. That was a five year longitudinal study, so some evidence is starting to emerge. The children we are talking to are all in primary school and they largely value popularity over privacy. They do not really understand the ramifications of sharing all sorts of things such as dick pictures, intimate images and children being told to kill themselves because of the colour of their skin or because of the way they look. There is a great deal of harmful communication and the online-offline balance - how one treats people in real life versus how one treats them online - is not well understood. That is why we keep returning to the education piece.

Ms Patricia Cronin: To bring the Deputy up to speed, the AVMS was finalised at a meeting this morning. In terms of the scope of it, as the Deputy mentioned a regulatory body will have to be established. As he said it will either be a new one or an existing one. Clearly the Broadcasting Authority of Ireland, BAI, is in the frame for that. Because this is such a new area, we in the Department are taking the opportunity to travel and meet with many other member states to get a sense of their approach. It is a big area. The audiovisual media services, AVMS, directive will clearly be of particular significance to Ireland because of the platforms we have here. We are therefore keen to learn from other member states about how they are managing. We met with representatives from the UK, which I know is about to depart. We will also be going to the Nordic countries. We really want to go very broadly on this to make sure that we get it right because how to regulate this space is a very significant decision.

On age verification, the directive itself refers to protecting minors and the general public from certain audiovisual content and about protecting the general public from content, including advertising, the dissemination of which is a criminal offence. These offences are terrorist-related offences, child sexual abuse material offences, and offences of racism and xenophobia. The model proposed in the directive is one of co-regulation between the platforms and a regulatory body. Part of that means that we will have to look at age verification and parental controls, because the Deputy is right, the directive does refer to minors. We have 21 months to transpose the directive so we really are going to be very thorough in how we do this and we will try and get it-----

Deputy Eamon Ryan: Broadcast advertising is controlled on the basis of time. Ms Cronin would agree that the current system does not provide for online video streaming, where time is not as relevant. We do not have an effective mechanism for age verification. Does Ms Cronin agree?

Ms Patricia Cronin: That is certainly something at which we will have to look in the context of the AVMS directive. It is an area at which we will be looking.

Chairman: I will bring in Facebook and Google to-----

Deputy Eamon Ryan: To get the companies' view on it.

Ms Niamh Sweeney: I will address each of the issues the Deputy raised in order. There is not a huge amount of research on the well-being front. We recently commissioned some in the UK through a think tank called Demos. One of the main findings coming out of that research and other research is that it is less about the amount of time than about what is done with that time. Passive scrolling of content can be damaging in some cases whereas meaningful interactions can actually boost a sense of well-being. There is, however, a dearth of research in the area and we are trying to address that. It can be seen that Instagram in particular has a very

strong focus on well-being. It has a whole section dedicated to it. It has introduced certain tools to help one limit one's screen time and to keep track of what one is doing. Apple has a report which one might see flash up on one's phone if one uses an iPhone. This report gives one a sense of how many notifications and how much screen time on average one has had per day. Facebook is also looking to roll out tools based on time spent online and well-being. I had thought that they would be rolled out by now. We are waiting for confirmation of when that will happen but it is something we are thinking about.

I must admit that I do not know which European Parliament report the Deputy was referring to.

Deputy Eamon Ryan: It was a text adopted on 2 October on audiovisual media services when it was agreed-----

Ms Niamh Sweeney: Is the Deputy referring to the directive itself?

Deputy Eamon Ryan: It was a foreword to it.

Ms Niamh Sweeney: We are looking ahead to how it will apply to us. We are actually meeting with the BAI on Thursday, even though it is a little early for that. It asked if we would meet so that we could start to get a handle on some of the challenges ahead if it does end up in that situation. The guidance that will follow the actual directive in terms of determining the principal purpose of a service when it comes to video-sharing platforms should be issued sometime towards the end of the year. A lot of this will only take shape when those guidelines come out.

The issue of age verification is a challenge. It is something I have talked about here before. One change that came about on our side on foot of the "Dispatches" programme, which the Deputy will recall we were before the committee to talk about on 1 August, is that prior to "Dispatches" we used to act with respect to underage accounts when we received a report - and I would encourage everyone here to report to us if they know of anyone under 13 who is using Instagram or Facebook because we will take action - whereas now, if we have any reason to believe that the user is underage, we will checkpoint that account. This means that the person must provide identification to regain access.

There was a question about advertising and our commercial model. Those under 18 years of age are protected from certain types of advertisements on Facebook and advertisements for gambling, alcohol, certain health products such as diet pills and dating apps will not be surfaced to them in their newsfeeds. I take the wider point about the commercial model. In general, it is an advertisement-funded free service and it does not give me much wriggle room to make concessions in respect of the model today.

Ms Rachel Madden: I will address three matters, the first of which is parental consent. As Mr. Meade mentioned, last year we launched Family Link whereby a parent can stay in the loop while his or her child uses his or her device or accesses his or her Google account. The parent can set digital ground rules and screen-time rules, such as a bedtime rule or daily device limits, and a parent can manage the apps their children can download, as well as restrict websites and so on. We prohibit personalised advertisements for users who have accounts managed with Family Link and the same is true in the case of YouTube Kids, our product for young people who want to use YouTube. We have other restricting policies in which there are no advertisements for food and beverages or for health and beauty products. Any advertisers using Google

services cannot specifically target anyone under the age of 18.

Deputy Eamon Ryan: The fundamental problem is that Google cannot verify the age of a person.

Ms Rachel Madden: Absolutely. That is a very important issue and something we think about a lot internally. We want to strike the right balance whereby we can confirm someone's age but without asking him or her for additional information, such as a copy of his or her passport or Government identification. If a person aged under 16 tries to set up a Google account, we will ask him or her to get his or her parent to use Family Link.

Deputy Eamon Ryan: What will force Google to change? Will the YouTube business model not have to change from being free and paid for by advertising so that Google will know a person's age? There is no protection otherwise.

Ms Rachel Madden: We are definitely thinking a lot about verifying age in a more robust way. Our current mechanism is to direct people to Family Link but I acknowledge the concerns and there is definitely more we can do.

Deputy Eamon Ryan: We could do with Facebook improving the level of well-being comments, such as those from the community of people who like and follow me.

Senator Tim Lombard: The Bill brought forward by my colleague from Cork is very important. Deputy Ó Laoghaire certainly has his finger on the pulse. The issue of definition will be the deciding factor in the context of the Bill and we will need to see the Deputy's work on that aspect at some point. The criteria are very important and, while he provided a brief outline, I would welcome the text when it is ready because it will give us the basis on how to move forward and guide us as to how implementable the Bill will be. Future-proofing will also be a major issue because the Bill will need some longevity. We have seen dramatic changes in the industry in the past three or four years and I am sure there will be more changes in the years to come. How will we frame it to make sure it is future-proofed?

Ms Quill referred to the issue of European legislation versus national legislation. Can the Department provide an up-to-date view on how domestic legislation will affect a global giant based in Ireland? If the Bill is enacted, will it be for the 4 million people of Ireland or given that a company might have its European headquarters here, will we be policing that company's entire European network? Are we going to be stuck with legislation which will look to solve an Irish issue? Unfortunately the global content will still play a part. How can we police the global content? We all have friends from all over the world. How will this interaction happen? If one posts something in another jurisdiction and then travel to this jurisdiction, who polices that content? Is it policed in the place where it was posted or where it was received? How does that all tie together? We are operating as a global entity.

I have mentioned the advertisements we see on Facebook and Google at this time of the year. Now that Halloween is over, Christmas advertisements have started to spring up on my iPad, which my daughters use on a regular basis. The advertisements are about Christmas shopping, Santa Claus and so on. Is that the market the companies are targeting? I am referring particularly to Google Kids, which is very popular in my household, and similar websites. Is there a major drive for commercial gain from that platform through the children using it? The first 30 seconds of whatever they watch is going to be an advertisement about something. Is that an issue that must be addressed? It is quite pervasive. The shopping list for Santa is done

already because of those advertisements. Is that a big issue we should look at and address? Do the witnesses feel that that kind of information should be screened?

Ms Triona Quill: I would distinguish between European legislation, such as the audiovisual media service directive referred to by my colleague, and this domestic legislation. European legislation applies throughout the European Union. For example, we will regulate Facebook and Google, insofar as they fall within that directive, for all content throughout Europe because those companies are established here. However, the digital safety commissioner Bill is national legislation. If content impacts on an Irish citizen but the company involved is not established in Ireland there are real concerns about how, or if, it could be brought within the scope of this legislation. We have sought advice on this matter from the Attorney General, because extra-territoriality is a factor. Irish law may not reach into that area for those companies. Unless Europe legislated for something similar to a digital safety commissioner, it will have no reach under this legislation. Europe is moving more in that direction in terms of criminal and illegal content - a new terrorism regulation is being discussed at the moment - but it has not begun discussions about content of this nature. There are certainly extra-territoriality issues to be considered in respect of this Bill, and a discussion to be had as to how far it can or should apply under Irish law.

Deputy Donnchadh Ó Laoghaire: I thank Senator Lombard for his kind words. We have come a long way from the county council and discussions about who is responsible for cutting ditches and verges.

Senator Tim Lombard: I am still working on that.

Deputy Donnchadh Ó Laoghaire: I take on board the point that was made about the definition. The value of this process is that it allows for discussion and for the teasing out of those issues. The committee will get a draft, and I repeat to any of the organisations that are here or that are listening in that it would be valuable to hear their views on what the definition should be or any ideas they have about the specific drafting. The point regarding its future-proofing is important. That is the reason this legislation is largely focused on the principles, procedures, structures and so on rather than necessarily going into specific technologies or forms of communication with respect to defining - as we have to do - what is harmful communication and also in terms of the harm that it does. The legislation will have to be revised at later Stages, as in the case of any legislation, but it outlines the framework and principles well.

Regarding the point on jurisdiction, as I addressed it substantially at the previous committee meeting, I will not go over the full text of what I stated on that occasion. The extra-territorial effect of this Bill is not particularly radical. It is limited to situations where the communication affects an Irish person ordinarily resident in the State and the means of communication used in connection with such harmful communication is within the control of an undertaking or company established under the law of the State or where such harmful communications affect an Irish person ordinarily resident in the State where the means of communication are within the control of an undertaking established under the law of another state and where a court established in this State would have jurisdiction to give notice of service in that respect. This Bill is not particularly out of line with other legislation in place in this jurisdiction in terms of its extra-territorial effect, and I can send the Senator correspondence on that.

Undertakings would have certificates of compliance if they are compliant with sections 4 and 5. It would be desirable for any significant platform undertaking to be seen to be compliant and that users, and particularly parents, would be aware that it was compliant. If an undertaking

is based outside this jurisdiction and it wants people in Ireland to use it, it will have to develop standards to reach the level of a certificate of compliance. It would be possible to give notice and to initiate proceedings. Some difficulties probably need to be sorted out but process involved in attaining a certificate of compliance is a value in that regard.

Chairman: I call a representative of the social media platforms to address Senator Lombard's questions on advertising. Who would like to respond to those?

Ms Rachel Madden: I noticed all the Christmas advertisements on television on 1 November. I was in Dundrum on Sunday and saw all the Christmas decorations, and thought the season is here.

Most of our services are ad-supported. We made the decision to offer YouTube Kids as a free app so that everybody could have access to it. As I mentioned, we have stricter advertisement policies but there are content creators who invest a good deal of money and time in trying to develop the spun and educational content. We have to find a way to fund them. In Ireland, there is YouTube Premium, which I believe is approximately €11.99 per month. That carries over to YouTube Kids, so one can get a non-advertisement version of YouTube Kids under a subscription service. These are important questions and we are trying to strike the right balance with the policies we have developed for YouTube Kids while also being able to offer the app to as many people as possible.

Ms Niamh Sweeney: I am sorry, I have forgotten the question but I think what the Senator were driving at was the kind of advertising that----

Chairman: That children-----

Ms Niamh Sweeney: All advertisements that are placed on Facebook are reviewed either through human review or automated review for the nature of the advertisement but we are agnostic as to the product or service being sold. There is no particular courting of a certain type of advertising.

Chairman: Does anyone else have anything to add before we conclude?

Ms Niamh Sweeney: I would like to add something. It refers to the 1 August hearing of the committee. I want to correct the record on one matter. It is a small issue. I do not know if it will be of major concern to the committee but at one point in time when Deputy Dooley was asking us about training materials being used at our outsource partner, CPL, for the training of content reviewers, we had been given to understand that the PowerPoint decks that were being used had been changed. As part of the investigation we have carried out in that interim period, we are now clear that they were not changed. It was hard to figure out the context of some of the material that was being shown in the programme because we did not have the before and after story. That was an example that had come up in the course of somebody's work and they were taking a second look at it as a team. It was not part of the normal training materials that had been produced. I just wanted to make sure that this was corrected on the record, because we did give the impression that it had been changed and that was not the case.

Chairman: I thank Ms Sweeney for that. I thank all the witnesses for coming before the committee today. It was a very good exchange. The committee will publish the opening statements and the submissions received to the Oireachtas website. If there is any further information that the witnesses want to pass on to the committee we would greatly welcome it, especially around those definitions of harmful communication, and anything else the witnesses feel

6 NOVEMBER 2018

would be relevant to our work on the Bill. The statements and submissions will be published on the website. Is that agreed? Agreed.

The joint committee adjourned at 1.30 p.m. until 4 p.m. on Tuesday, 27 November 2018.