DÁIL ÉIREANN

AN COMHCHOISTE UM DHLÍ AGUS CEART AGUS COMHIONANNAS

JOINT COMMITTEE ON JUSTICE AND EQUALITY

Dé Céadaoin, 2 Deireadh Fómhair 2019

Wednesday, 2 October 2019

The Joint Committee met at 9 a.m.

Comhaltaí a bhí i láthair / Members present:

Jack Chambers,	Frances Black,
Catherine Connolly,	Martin Conway,
Peter Fitzpatrick,	Niall Ó Donnghaile.
Jim O'Callaghan,	
Thomas Pringle.	

I láthair / In attendance: Deputies Martin Kenny and Bríd Smith and Senator Colette Kelleher.

Teachta / Deputy Caoimhghín Ó Caoláin sa Chathaoir / in the Chair.

Business of Joint Committee

Chairman: I remind members to switch off their mobile telephones as they interfere with the recording equipment. I have not been advised of any apologies. We will now go into private session to deal with housekeeping matters.

The joint committee went into private session at 9.05 a.m. and resumed in public session at 9.40 a.m.

Online Harassment and Harmful Communications: Discussion

Chairman: The purpose of today's meeting is to begin a series of engagements on the issue of online harassment and harmful communications. We are joined by Mr. Michael Gubbins, chief superintendent, special crime operations, An Garda Síochána, and Mr. Pat Ryan, detective superintendent in the Garda National Cyber Crime Bureau. From the Irish Society for the Prevention of Cruelty to Children, ISPCC, Childline, we are joined by Mr. John Church, its chief executive. We are also joined by Professor Joe Carthy, director of the UCD centre for cybersecurity and cybercrime investigation, and Ms Caroline Counihan BL, the legal director of Rape Crisis Network Ireland. You are all very welcome, as are your colleagues who are guests in the Visitors Gallery. I will shortly invite you to make your opening statements and I propose to do so in the order in which I have just introduced you, if that suits. There is no hierarchy. It is just the order in which I introduced you. I first must draw your attention to the issue of privilege.

Witnesses are protected by absolute privilege in respect of the evidence they give to the committee. However, if they are directed by the committee to cease giving evidence on a particular matter and continue to so do, they are entitled thereafter only to qualified privilege in respect of their evidence. They are directed that only evidence connected with the subject matter of the proceedings is to be given and asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person or entity by name or in such a way as to make him, her or it identifiable. Members of the committee are reminded that under the salient rulings of the Chair, 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 caution our panel and visitors to ensure that their mobile phones are switched off. Will the chief superintendent be leading off?

Mr. Michael Gubbins: I will.

Chairman: Chief Superintendent Gubbins will make the first opening statement.

Mr. Michael Gubbins: This is the opening statement from An Garda Síochána to the Joint Committee on Justice and Equality. The report entitled The Future of Policing in Ireland provides a roadmap for an improved policing service in Ireland. This report identified that cybercrime and Internet-enabled crimes are proliferating fast and that Ireland is not alone in struggling to deal with the threat and that tackling cybercrime must be regarded as a core function of policing. A central tenet of the report on the future of policing in Ireland is that policing is not something the police do alone. Likewise, the solution to tackling online harassment, harmful communications and related offences will require the involvement of multiple stakehold-

ers across various Departments, An Garda Síochána and society in general, including parents, schools and employers.

The recent roll-out of the new operating model will enhance the investigation of crime through the delivery of a greater range of specialised services in local areas, such as the investigation of sexual crime, domestic violence, cybercrime, and economic crime. Each division will be provided with a detective superintendent who, along with trained investigators in specialist areas, will be responsible for local crime investigation. Complex or highly technical crimes will generally be dealt with at national level. This initiative will see the establishment of regional cybercrime hubs and trained first responders, who will support the regional units and provide for a tiered level of capability nationally, with the Garda National Cyber Crime Bureau, GNCCB, as the top tier of support and capability.

The Garda National Cyber Crime Bureau was established in September 2016, providing an enhanced structure within An Garda Síochána for the purpose of tackling cybercrime. The bureau has a national remit with regard to the phenomenon of cybercrime, and in particular, the investigation of online criminality. The Garda National Cyber Crime Bureau is tasked with undertaking the forensic examination of computer media in all incidents reported to the Garda Síochána. The Garda National Cyber Crime Bureau is currently supported by two regional pilot units, one based in New Ross Garda station, County Wexford, and the other in Ballincollig, County Cork. The Garda National Cyber Crime Bureau, in conjunction with the Garda College, has developed a training module relating to the investigation of cybercrime for delivery to all students attending the college. It is planned that other members of the Garda Síochána will be trained in cybercrime awareness and cybercrime investigation through our continuous professional development network.

An Garda Síochána will further its long-standing relationship with the centre for cybersecurity and cybercrime investigation in University College Dublin through the GNCCB and alumni who have undertaken courses of study at the university in the cyberdomain. The Garda Síochána will also develop more educational partnerships with third level institutions and international institutions with expertise in cybersecurity in order to ensure cutting-edge support is available throughout the organisation. The Garda National Protective Services Bureau, GNPSB, was established in 2015 and is a specialist team dedicated to making sure each and every complaint relating to child protection, human trafficking and domestic and sexual violence is thoroughly investigated and that such investigations are handled in an appropriate manner. In addition, the GNPSB is responsible for working with other agencies to manage sex offenders in the interest of community safety.

Increasingly, children are engaging in the sharing of self-taken imagery where they send nude or sexually explicit or both personal photographs of one another to other members of a chat group, utilising platforms such as WhatsApp or Instagram, or over social media such as Facebook or Snapchat. While this scenario has given rise to a form of bullying, there is an added danger when images are circulated outside the confines of friends or otherwise become available to third parties, who may then use them as a trap to engage with a child or set up fake profiles, using the images as bait. In 2015, the Garda Síochána established 28 victim service offices across the country which are tasked with communicating with victims of crime and prioritising their needs. Protective service units, which will operate within each Garda Síochána division, will assist in ensuring that relevant child protection, domestic and sexual violence incidents are thoroughly investigated and victims fully supported.

Any individual, adult or child, business or organisation, using a connected device is vulner-

able to cybercrime. Just as with offline crime, simple steps can often be effective in reducing these vulnerabilities. Working in partnership with public and private sector stakeholders, An Garda Síochána will use opportunities such as the Garda Síochána's communication channels, "Crimecall", public awareness campaigns and industry liaison to ensure people are educated on protecting themselves from cybercrime. The investigation of all the relevant incidents and the examination of associated computer media is dependent on the disclosure of a criminal offence. In cases involving the online safety of our young people, the primary offences are cyberbullying and sexual exploitation. In this regard, the relevant legislative provisions are contained in the Non-Fatal Offences Against the Person Act 1997, the Child Trafficking and Pornography Act 1998 and the Criminal Law (Sexual Offences) Act 2017.

The Garda schools programme is currently being updated. The Garda is working in partnership with Webwise to create modules within the Garda schools programme to be delivered to all primary and second level schools nationally, to include subjects such as cyberbullying, online harassment, consent and image sharing. The "Be in Ctrl" programme was launched in 2018. It is delivered to junior cycle second level students nationally. It gives students the opportunity to recognise and understand online sexual coercion and extortion and will give them the information on how to deal with and report these incidents. Three new modules are currently being created by Webwise and An Garda Síochána and are expected to be rolled out in 2020. These would deal with cyberbullying and online harassment in primary school, the impact of cyberbullying and online harassment and the harm and legal consequences that image sharing has. It encourages students on how to act responsibly when they encounter intimate content. This is for both the junior and the senior cycle.

A new information and education resource called "Lockers" has been designed, in conjunction with the Garda Síochána, to assist schools in coping with and preventing the sharing of explicit self-generated images of minors. Intended for use within the junior cycle social, personal and health education curriculum, "Lockers" is supported by a newly developed animation and six lesson plans, and includes an information section for school leaders. This 25-page section informs principals on the context for sexting among young people, the laws that can come into effect when underage sexting occurs and the implications for school policy. An Garda Síochána will continue to develop its capacity and capability to tackle online harassment, harmful communications and related offences, and in this regard will interact in an appropriate manner with all relevant stakeholders.

Chairman: I thank Chief Superintendent Gubbins. We will move on to Mr. John Church, chief executive of the ISPCC.

Mr. John Church: I thank the members of the committee for having us here today. The ISPCC is delighted to be in a position to support this important draft legislation and thank Deputy Howlin for introducing it and the members for considering it in committee. As the national child protection charity, I wish to present to members the ISPCC's perspective on how this Bill may pertain to children.

Research conducted for the ISPCC in 2018 found that almost half of children aged six to 18 years old were always online. The ISPCC's Childline service answers over 1,000 contacts every day from children. Many tell us about their experiences online. For example, a 16 year old girl told Childline she had sent images to a former boyfriend, who then shared them with others without her permission. With these images now circulating widely, this girl told Childline she could not face going back to school and was contemplating suicide.

Online safety is an integral part of the ISPCC's policy work. We welcome the commitment by the Minister for Communications, Climate Action and Environment, Deputy Bruton, to establish an office of digital safety commissioner, an office we see as imperative for championing children's online safety. The ISPCC continues to call for the introduction of a long-term national strategy for online safety. The ISPCC is acutely aware of the long-term and devastating consequences bullying and cyberbullying can have on children. As cyberbullying can take place through any digital means of communication, it is essential that modern platforms are included in how this Bill defines "communications". Content which is shared online often has the potential to reach very large audiences, very quickly. Young people told the Law Reform Commission in 2016 that they felt practices such as identity theft, online harassment and the non-consensual sharing of intimate images should be made illegal. Through the ISPCC's work with children and young people, however, we are acutely aware of the need for an age-appropriate response to the proposed offences as outlined in this Bill. By their nature, children and young people do not have the maturity level of adults: they may exhibit a greater tendency to be impulsive and they may not fully comprehend the consequences their actions online may have. In accordance with the UN Convention on the Rights of the Child, the ISPCC would not advocate that children and young people under the age of 18 be criminalised for their behaviour. Instead, it is essential they are educated and empowered to act differently in future. Entry into the Garda youth diversion programme or similar may provide a more appropriate response. Relative and relatable online safety education, delivered via the curriculum on a regular basis at both primary and post-primary level, is a key component in preventing these activities occurring in the first instance.

While we appreciate we are here today to explore proposed criminal justice responses to online safety, we need to take this opportunity to reiterate our call for industry regulation as a fundamental response too. At present, industry regulation falls short of adequately protecting children online. The ISPCC cannot support an approach of self-regulation of industry over legal regulation. As the online world does not know borders in the same way as they pertain to the physical world, the ISPCC believes it is important to monitor international developments. The Criminal Justice and Courts Act and the Voyeurism (Offences) Act, as recently introduced in the UK, make the practices referred to as revenge porn and upskirting criminal offences. At an ISPCC event held in December 2018, the eSafety Commissioner of Australia outlined how the office has successfully assisted more than 1,000 young Australians to remove cyberbullying material. The office is equipped with regulatory powers to penalise and fine social media companies should they fail to remove such content. Children have a right to be protected and this protection extends to being online. Legislation and regulation which strives to make the online world a safer place for children must be duly considered, respecting the particular rights and needs of child victims and child perpetrators. We reiterate our point that such legislation, however, should not criminalise children and young people. The ISPCC views the education and empowerment of children to become civic online citizens as the ultimate goal for which to strive.

Chairman: Before I bring Professor Carthy in, I wish to make a point of clarification. It does not in any way take away from what Mr. Church has just put on the record. We are not in the process of addressing any specific legislation. I know that Deputy Howlin has tabled legislation, but this has been an identified substantive issue for address by this committee going back some time. It emerged from our work programme for substantive address in the widest possible way. There is no problem in referencing specific legislation that is before the Houses but that is not the purpose of our address, which is much wider. Speakers are entitled to address any legislation they think pertinent to the process. I invite Professor Carthy to make his presentation.

Professor Joe Carthy: I thank the committee for the invitation to attend here today. In the interests of time, I will keep my submission brief. I will concentrate on two issues I believe are important in this area. The first is regulation. There is no history to show that a lack of regulation or self-regulation in any industry has worked. We are relying on self-regulation very often in the cyberworld, which is a grave error. Automobile legislation offers a very good model for the cyberworld. Every car in the country is required to have a number plate, which can be used to identify the owner. A similar system in the cyberworld, where users could be identified would greatly diminish instances of cyberbullying, cyberstalking, hate speech and so on. If we could legislate in this key area it would make a significant difference. I accept the details would have to be worked out very carefully. First, social media platforms and online providers would have to register their users and the users would provide appropriate evidence of identity. In the case of minors, parents or guardians would be responsible. Second, users or parents who can show that they have been bullied, harassed or abused on a social media platform, should be legally entitled to find out the identity of the user carrying out the inappropriate behaviour. That one simple measure would make a significant difference in this area. I accept there is an international dimension but other countries would look to Ireland to set a lead and Ireland could pursue it at an EU level.

Computer users have a responsibility as well. Again, the automobile industry offers an example in that we must have a national car test, NCT, on our cars. We cannot put an unsafe car on the road. If we have a computer system there is an obligation on us to have appropriate anti-virus software installed in order that our computers cannot be hacked, our information cannot be stolen or, equally important, that our computers cannot be infected by malware, which allows them to partake in attacks on computers on the Internet, unbeknownst to us. That is a widespread problem. Thousands of Irish computers are currently infected by such software. The regulation could be such that if one is going on the Internet, one must ensure one has appropriate anti-virus software on one's computer.

In terms of keeping children safe, the concept of a digital safety commissioner is valuable but we must make sure the office has the correct mandate and the resources to carry out the tasks assigned to it. We also need public awareness campaigns. Again, to return to the automobile situation, the Road Safety Authority has a fantastic public awareness campaign and a similar campaign is required in terms of cyberawareness for parents and children. Digital literacy education must be improved at primary level so that all children and teachers are aware of the risk and dangers of using computers online.

Chairman: I thank Professor Carthy. The final speaker is Ms Caroline Counihan from the Rape Crisis Network Ireland, RCNI. I invite her to make her presentation.

Ms Caroline Counihan: Thank you very much, Chair. The RCNI is grateful to have this opportunity to share its views on online harassment, harmful communications and related offences with the committee. Our clients of all ages are now reporting to us more and more forms of online sexual harassment and harmful communications of an intimate nature. Effective regulation, via the criminal justice system and otherwise, generally has not kept pace with developments in online technologies and the almost universal use of Internet-accessible devices. Many forms of online sexual harassment and harmful communications are covered by the Criminal Law (Sexual Offences) Act 2017 and related legislation on child pornography but there are wide gaps in the criminal law as far as adult victims are concerned. To us, these forms of sexual harassment are a form of sexual violence, and should be regarded as seriously as contact sexual offences. Their impacts on their victims are just as grave and potentially far

reaching. Accordingly, we think it is appropriate to describe this behaviour as image-based sexual abuse. It is difficult to compile an exhaustive list of all the forms which this might take. They include sextortion, deep-faking, flashing, what is commonly but inaccurately referred to as revenge porn, and perhaps most disturbingly, the recording and distribution of videos of acts of sexual assault and rape. They need to be addressed urgently to deter and where necessary, punish, perpetrators of grave harm through online technologies.

There have been some very encouraging positive developments in recent years, not least the Bill introduced by Deputy Howlin, which is based mainly on the relevant provisions in the draft Bill in the Law Reform Commission's Report on Harmful Communications and Digital Safety. The RCNI broadly welcomes this Bill and would like to see it progress as quickly as possible. In particular, we welcome the inclusion of section 4, concerning the distribution of intimate images without consent, which will address that form of image-based sexual abuse consisting of the one-off sending of intimate images online to third parties. The current law on harassment covers only persistent communications made directly to the victim. To give another positive example, the Law Reform Commission also put forward the idea of a digital safety commissioner's office, which would be responsible for regulating online service providers' procedures and practices, especially in respect of take-down of harmful material. This has also found expression in proposed legislation, such as the Digital Safety Commissioner Bill 2017, a Private Members' Bill put forward by Deputy Ó Laoghaire.

We refer briefly to some of the principal recommendations RCNI makes in its full submission. I hope it is in order to state that the recommendations refer to the Harassment, Harmful Communications and Related Offences Bill 2017, which is a Private Members' Bill. It is recommended to consider separating the current proposed section 4 of the Bill into three distinct offences: generation of intimate images without consent, alteration of images to make them appear to be intimate images without consent, and their storage, distribution, publication, sale, etc, also without consent; to ensure that the wording of any offence or definition used in any offence covers originally innocent images of the victim that have been altered to appear to include intimate images of third parties, in order that it cannot be argued by the defence that the genitalia, anal region, etc., of the victim are not in fact depicted in the intimate image in question; to include, as has been done in Scotland, separate voyeurism related offences, to cover viewing victims without consent in intimate settings, installing equipment to record intimate images of them, recording such images, and storing, distributing, publishing or selling them, in each case without consent; to create a new offence of producing and distributing audiovisual images of acts of sexual violence without consent and attach significant penalties to it, an activity that should be an offence whether it takes place online or offline; to consider criminalising the intentional or reckless impersonation of others, real or fictional, in online interactions, which can be extremely harmful in a sexual context; to include a review clause and give responsibility for carrying out the review to the digital safety commissioner or a similar official, pending the creation of a new digital safety commissioner's office or a similar body, responsibility for which should be given to the Department of Communications, Climate Action and Environment; and to include provision to hear cases related to online harassment, harmful communications and related offences, *in camera*, ideally irrespective of whether their content amounts to image based sexual abuse.

I thank members for their patience. RCNI thanks the committee most sincerely for taking the time, through the submission process and hearings, to consider these most important issues for all survivors of this form of sexual violence and all those at risk of it.

Chairman: I thank Ms Counihan and each of our contributors. To answer her question, it is wholly in order to refer to any proposed legislation. It just so happens the committee had signalled the matter a long time ago but we finally had the opportunity to discuss it. Regrettably, we had to defer it a couple of times but we are now sitting down to address it.

Deputy Colm Brophy: I thank our guests for their contributions and for appearing before the committee. I have a general, observation-style question. I always defensively preface the following point by insisting I am not in favour of censorship, restriction or anything like that but I seek our guests' views on a matter. Further guests will come before the committee and I would also like to hear their views. Legislation reflects the actions of people, and whether they do something that could be deemed an offence or whether an offence needs to be created. The core problem is that some platforms are completely unregulated. There is an insane, wild west scenario. It is impossible to imagine television, radio or newspapers uniformly stating that even though they broadcast, transmit or publish something, they have no responsibility for it. For some reason, however, long after the birth of the Internet and such platforms, we continue to tolerate, not just in our country but internationally, the notion that large, multi-billion euro, profitable corporations can continue in this fashion. That is the heart of what we have to grasp.

The reason I commented on censorship is that when I make the next point, people might say, "My God." I am not in any way a fan of what the Chinese Government or other totalitarian regimes do in restricting the ability of people to post on or access the Internet. Given that large corporations continue to interact in such jurisdictions, however, there must be a way, whether through delay, content monitoring or responsibility, that we can bring some of that to the wild west that currently operates in the western world. One measure we should move towards is the notion that victims would have the right to sue platforms. If there were a few substantial settlements, the providers would move quickly. What are our guests' views on that? Do they believe litigation and so on will have to be at the heart of reform in how we will deal with the matter in the next ten, 15 or 20 years?

Chairman: Where will the Deputy direct his question?

Deputy Colm Brophy: I would like to hear a range of views. It might be difficult for An Garda Síochána to comment on legislative matters but I would like to hear responses across the board.

Chairman: I will take our guests in reverse order and give everyone except Ms Counihan a moment to think. I know she is ready to answer.

Ms Caroline Counihan: I will do my best. To address the Deputy's final point, I fully agree victims should have the right to sue platforms and that a few hefty settlements would soften the cough of those online platforms that have not been as careful in exercising the due diligence we would expect of them to protect people from serious harm. Nevertheless, I must qualify that by stating it is not a bad thing in itself because it still puts too great an onus on the victim. What will happen is that people will say they cannot face such proceedings, that they do not care about the money, and that all they want is for the content to be taken down and reversed as far as possible. They will say they want the process to happen in peace and privacy, quickly and cheaply. The process has to work for victims.

In our various submissions to the committee, we have argued strongly that the role of the digital safety commissioner should include oversight of companies to ensure they keep up to certain standards. The commissioner should oversee any take-down procedure and there should

be a right of appeal to the commissioner if there is any failure in such a procedure. Ultimately, the process should be backed by civil sanctions. I would not rule out the idea, as a last resort, of making directors of rogue Internet service providers criminally liable for indefensible failure to take down harmful material where it has been notified to them. The existence of a criminal offence would make them sit up.

Professor Joe Carthy: I concur completely with the Deputy's comments. It is ridiculous that any software provider in the world can produce a new application, launch it on the Internet and allow people to use it without any measure of its safety or of how it protects the data of the people involved. Software designers are allowed to make their software do whatever they want with impunity. We do not allow such practice in the aviation or automobile industry. Definite controls are needed in that regard. The Deputy is correct that billion-dollar companies make billions of dollars every year. There is a cost of doing business and the cost for the automobile industry is that its cars must be safe, adhere to pollution standards and so on. I would argue that there is a cost of doing business in this space, namely, people should regulate the content and ensure it is legal in whatever way that is defined by countries. There is no technological reason for not doing so. I would argue that it is a legislative matter. The automobile industry offers an excellent example. Although this situation is not something that we can fix quickly, we have been dealing with automobile legislation for 100 years and every year we tweak it a little. We need to do the same in this context, but we need to start somewhere. We probably will not get the legislation right initially, but we need to keep tweaking it over the years. I agree with the Deputy.

Chairman: Would Mr. Church like to contribute?

Mr. John Church: I will give the angle from the child's perspective. I always cite Childline, which is like a barometer of what it is like to live under the age of 18 years. We listen 24-7, 365 days per year. We constantly get children ringing us about online issues, but they do not say that they are ringing about an online issue, as children do not talk about online or offline. This is the space they are living in and they are active in it every single day of the week. Half the children between six and 18 years of age are online every day, but that figure is 94% for 16 to 18 year olds. This is their life. This is where they are living.

Self-regulation does not and will not work. That ship has sailed. I welcome the Minister's position on this matter, and we would actively support it. In Australia, there is an interesting concept of co-regulation. Getting representatives from the platforms around the table and having an adult and mature conversation is the only way to go. From speaking to the larger platforms, I know that they are spending millions of euro on trying to tackle this, but they were not set up with the express objective of protecting children. They are commercial operations. We are talking about YouTube, Snapchat and Instagram, but this issue extends way beyond them. We are getting calls every day about new games that are launching and apps, including smaller ones, some of which require in-app purchases. To use the Deputy's phrase, it is the Wild West. The only way we can tackle this is through actual regulation. I always use the analogy of how every other form of media that we look at is regulated. Thanks to the Broadcasting Authority of Ireland, someone cannot put certain images up on television or outdoors. Why are we allowed to do so online?

Deputy Colm Brophy: Exactly.

Chairman: Would Mr. Gubbins like to add anything?

Mr. Michael Gubbins: I agree with the three speakers so far. To address a technical element, the apps allow people to communicate directly and instantaneously. I have three kids, so I have seen the use of these apps.

Turning to the point about censorship, it is nearly impossible. For example, if I rang Professor Carthy on the phone, a delay could not be placed on it and I could not be told I could not say something. WhatsApp, Snapchat and so on have the same function as a phone call.

Regulation and legislation are important, but everyone around the table will agree that we must work with the industry and talk to the young people. The ISPCC is in attendance, but not just children should be involved. Adults also have to be involved in and informed on these matters. I have had numerous phone calls over the years about someone whose friend was in a bit of difficulty because of something that had happened online. This issue crosses all age groups. Children are very vulnerable and have to be protected, but there are other cohorts of people we must look after as well.

Deputy Colm Brophy: While I take on board the comments about the involvement of young people and working with them on all of the issues outlined in the responses, including through the innovative programmes that the Garda outlined, I am of the view that this comes down to a mindset change. The latter is something that we do not address often enough. Anyone can set up a successful business that sells drugs. There is no regulation or anything. It is just illegal, which is why such businesses are not set up, but one could sell drugs and make large amounts of money. In the case of what we are discussing, though, we are in a strange situation wherein it is claimed that, because someone can build a technology with peer-to-peer or end-to-end encryption, he or she should be able to do it. There may be some social good in certain contexts. For example, we have seen protest movements around the world and people who are involved in trying to tackle unsavoury regimes using technology for good. Having also seen the level of damage being done, however, we must be able to do something. I am 50 something years of age, and Mr. Church's statistic about how virtually every aspect of 16 to 18 year olds' lives is online is frightening. Deputy Jack Chambers is much younger than me, but many of us present probably grew up prior to the age when everything was available online - every photo of every birthday, every family moment, everything we did in school, etc. That is terrifying to people who did not grow up with it, as is knowing that companies can use and exploit it or facilitate people who want to harass, bully or harm others. I hope that we move to regulate it and that there will be a penalty for the perpetrators, but the people actually making the billions of euro will get to walk away scot-free and live a lifestyle thanks to something that has caused endless harm. At a certain point in 20, 30 or 40 years' time, we as a society will look back on this period aghast that we put up with this and said that we had to do so because there was no way around it.

Chairman: I do not think there is any need to put what the Deputy has just said to the panel.

Deputy Colm Brophy: No.

Chairman: I anticipate a concurrence. I thank the Deputy.

Deputy Jim O'Callaghan: I thank our guests for attending. Just so that they are aware of what we are doing, we will ultimately produce a report on the issue of online harassment and harmful communications. Obviously, we will make recommendations on legislative changes, but we are not limited to that, since it is not as though we are a legislative group.

I agree with virtually everything Deputy Brophy stated. A part of the problem in a discussion about the Internet is that it can be broad, given the panorama of the Internet. As such, I would like to examine one or two specific issues and probe how to deal with them. Ms Counihan and Mr. Church raised an example - a woman under 18 years of age who is in a relationship consents in that relationship to intimate photographs being taken, but the relationship breaks down and her ex-partner subsequently posts the photographs online. Could we probe this example for a while? I would like to see how we might deal with it. That would give us a good roadmap for how to deal in general with these issues.

It appears to me that her right to privacy has been breached. Had those photographs been published in a newspaper, the courts would hold under the European convention and Irish constitutional law that the consent to the photograph being taken was a consent that was given in the context of a private relationship between her and her partner at the time. If her privacy has been broken - I believe it has - the difficulty that she faces at the outset is that, in order to give effect to that breach of privacy, she probably has to go to court. Do the witnesses believe it is necessary for us to put on a statutory basis the right to privacy that this woman has, which is a constitutional and convention right but is not given expression in Irish statute? I will turn to the criminal aspects subsequently but in terms of the civil aspects, does Ms Counihan believe that there should be a law of privacy that sets out the woman's right?

Ms Caroline Counihan: I would love it. It would be helpful. Fair play to Deputy Howlin, who did this in his Bill. However and wherever it is done, though, it is important that the principle of consent be referred to everywhere. Of course the woman consented to those photographs or videos originally being taken in a private context, but it must be clear that that does not imply a general licence to broadcasting them to all and sundry or even to one other person.

Deputy Jim O'Callaghan: Our law makes provision in this regard but, unfortunately, the woman or girl in that situation is probably not aware of that. If she wants to invoke the law, she has to go to a court where she will have to reveal her identity. She will have to describe the events that took place so there will probably be a report about in the newspaper, which would put her off. Does Ms Counihan agree?

Ms Caroline Counihan: Deputy Howlin's Bill contains an element of anonymity under section 11. That should definitely stay in and should be added to by an in camera provision. That section does go some way towards safeguarding her privacy. Professor Clare McGlynn makes the point in her critique of the same section that anonymity should begin before charge which would ensure that people would not be deterred but would be encouraged to come forward. The whole criminal justice process, though it has improved in recent years, is still very difficult for victims and survivors of sexual violence. It takes a very long time as well and the delay-----

Deputy Jim O'Callaghan: I am sorry to interrupt but I will be looking at the criminal aspects of this later. What happened to that woman should be criminalised but in terms of any civil remedy, at present her only option lies with our privacy laws. In that context, who has breached her privacy?

Ms Caroline Counihan: The person who shared the images without her consent.

Deputy Jim O'Callaghan: Does Ms Counihan agree that if the images are posted on a social media site, the social media company itself has also breached her privacy?

Ms Caroline Counihan: Yes, I agree.

Deputy Jim O'Callaghan: If those photographs were published in a national newspaper, then the newspaper would be liable for breaching her privacy. Part of the problem is that technology companies do not believe they are publishers. A newspaper is obviously a publisher but technology companies claim that they are not publishers but are servicing their communities. There are online communities and the companies are just facilitating them.

Let us look at this now in a criminal context. At present, the act in question is not criminal. Potentially, it could be harassment but Ms Counihan is probably right in saying that there is no persistence to it, unless the repeated posting of the images could be viewed as persistent. However, under the criminal law, I think it would be extremely difficult to secure a prosecution. Would Ms Counihan agree?

Ms Caroline Counihan: Unless the victim was underage, in which case it could be prosecuted under the statutes mentioned by Mr. Gubbins earlier like the Child Trafficking and Pornography Act or the Criminal Law (Sexual Offences) Act. There is a range offences there that would capture this kind of activity if it is done in respect of a victim who is underage. The difficulty is with adult victims.

Deputy Jim O'Callaghan: Say it is an adult, a woman over 18-----

Ms Caroline Counihan: If it is a one-off incident, there is nothing that really captures it.

Deputy Jim O'Callaghan: Do our guests agree that the law should be changed to criminalise the type of behaviour I outlined in the example?

Ms Caroline Counihan: Yes.

Deputy Jim O'Callaghan: Who does Ms Counihan think is the offender in terms of that prospective offence?

Ms Caroline Counihan: Clearly the person who deliberately shared the images without consent; there is no question about that. The question then is to what extent criminal liability should be attached to social media companies.

Deputy Jim O'Callaghan: Let us take the example again. If the images were published in a newspaper and they related to a child, the newspaper would be criminally liable, would it not?

Ms Caroline Counihan: Yes, it would be liable because it would know by virtue of editorial control. The difficulty with an ISP is that it will not necessarily always be put on notice that this has happened. It will not necessarily know. Technically, I do not know if it can know at the same instant that the images are shared. Does that sharing automatically come to the attention of some monitoring system?

Deputy Jim O'Callaghan: It would be extremely difficult to hold a social media company criminally liable for the posting online of an intimate photograph when what makes it criminal is the fact that consent was not given by the woman in the photograph.

Ms Caroline Counihan: Yes, but if the company is put on notice and fails to act with due expedition for no good reason, then criminal responsibility should not be ruled out. It may not be the case that every single event is dealt with; it may be easier and more effective for more people to deal with it by way of a take-down procedure backed up by civil sanctions. Ulti-

mately, I do not see why these companies should not be criminalised if they do not take down material that they have been put on notice as being harmful.

Deputy Jim O'Callaghan: To go back to the example I gave earlier, let us say the ex-partner posts the intimate images online without the woman's consent but does so from an anonymous social media account. At present, is there any mechanism, other than An Garda Síochána going to court or to the social media company, for identifying the person who committed the offence?

Ms Caroline Counihan: I do not know the answer to that but I do not think so.

Deputy Jim O'Callaghan: If one looks at it from a civil point of view, the woman's privacy has been breached. If one looks at it from a criminal law point of view, if we introduce a new offence then the criminal law would have been breached. It seems to me that the mechanism to give effect to her remedies and criminal liability is an online regulator. If we look at it in the civil law context, the woman should be able to make a complaint about these intimate photographs to an online regulator, confirming that she did not give consent for them to be posted online and requesting that they are taken down. The benefit of that, from her point of view is that unlike with the law of privacy, she does not have to disclose her identity by going to court. An online regulator in that context would assist her in getting a remedy.

Ms Caroline Counihan: Yes, I think so. My feeling is that if it is done properly, that has the potential to be the quickest, safest, most private and most effective way to get the images taken down. It will enable something to be done quickly. Survivors really do not need the extra trauma of delay and uncertainty and, in the civil context, expense of court proceedings.

Deputy Jim O'Callaghan: In fairness, from the social media company's point of view, there is a benefit in having an online regulator in that instance because it means the company is spared the expense of being brought to court. It is informed through an efficient mechanism at an early stage that there was no consent for these intimate images to be online. If the company does not comply with that, then civil liability kicks in.

Ms Caroline Counihan: Yes.

Chairman: Does Deputy O'Callaghan want me to direct any of his questions to the rest of the panel?

Deputy Jim O'Callaghan: Feel free, if anyone else would like to come in on the discussion.

Chairman: The discussion between the Deputy and Ms. Counihan is very illuminating but if anyone else would like to come in-----

Mr. John Church: I would like to add to what has been said. I could not disagree with anything that Ms Counihan and Deputy O'Callaghan have said thus far. The right to privacy is definitely an issue but as I said earlier to Deputy Brophy, the platforms are putting a lot of money and resources into this area. I met representatives of Facebook recently. That company employs approximately 30,000 people worldwide whose sole job is to take down inappropriate images. Recently I read that something like 2.6 million inappropriate images were removed in one quarter, that is, in a three month period. As I said earlier, these platforms were not set up to protect children. They were set up to make a profit and while they are extremely beneficial to many people and add to effective communications, we would not let our road network run riot, with no lines in the middle of the road, no rules and no traffic lights but we are letting the

equivalent happen with the internet. Let us be clear, the ISPCC is not seeking to shut down the internet. We talk to children every day and we know that the vast majority of both children and adults view the internet as extremely beneficial. My own children use it every day to study for exams. It is extremely beneficial but as with roads, which are also very beneficial, we need laws and rules. The only way to do this is to have a proper regulator with teeth. In the context of all other forms of media, the Broadcasting Authority of Ireland is a potential home for an e-safety commissioner for Ireland, if only to send out a message to the platforms that they are being watched.

Deputy Jim O'Callaghan: I agree with Mr. Church. To return to the example I gave, what Professor Carthy suggested in his paper would probably have a significant impact in deterring the woman's ex-partner from posting the images because, under the professor's proposal, he would have to disclose his identity and she would be able to identify who it was. She would still have the difficulty of disclosing her identity, but it would assist her considerably if there was a requirement for his identify to be disclosed.

Professor Joe Carthy: Absolutely. The offence mentioned by the Deputy is at the very serious end, but there are a host of offences at the less serious end which could be dealt with. Many people post because they are anonymous and can say whatever they wish about individuals. I am sure committee members are familiar with this. The people in question would not make the posts if they could be identified and there was some regulation that allowed their identification. Also, it would be appropriate for every company to have a take-down mechanism such that a person's first port of call would be the company to tell it that there is material on its platform about him or her and that he or she wants it to be taken down immediately before he or she would have recourse to a commission or something like it. The commission should have a mechanism to do this quickly. If the company did not respond, someone's next port of call would be the e-commissioner. The companies have the money to put these facilities in place and it should be part of their process.

Deputy Jim O'Callaghan: What would their response be to Professor Carthy's proposal that only a person who identified himself or herself could establish a social media account with them?

Professor Joe Carthy: They would probably object because it would cost them money. They would have to verify, etc. That is, I argue, a legitimate cost of doing business. If one wants to enter this space, it will cost him or her to enter. We are dealing with people's privacy and have seen the problems.

Deputy Jim O'Callaghan: I thank everyone for the answers, but on the term "harmful communications", we must also be careful that we do not include within it issues which are considerably less serious than the example I gave to Ms Counihan. Where does one draw the line? Obviously, people should be entitled to say they hate Fianna Fáil and Fianna Fáil politicians.

Professor Joe Carthy: Absolutely.

Chairman: Perhaps they should even be encouraged.

Deputy Jim O'Callaghan: That is rich coming from a Shinner. Where does one draw the line? There is an element of subjectivity in the definition of harmful communications.

Professor Joe Carthy: It is quite simple. If someone says something about a named individual in a communication, or a recently deceased individual, because there are nasty people

who troll those who have just died and whose families are put through extreme hardship, there is a right to know who is speaking about him or her.

Deputy Jim O'Callaghan: Do they?

Professor Joe Carthy: I think the person does.

Deputy Jim O'Callaghan: If there was somebody in a house in Dublin last night saying he could not stand Jim O'Callaghan, am I entitled to know that?

Professor Joe Carthy: If the post is going to be seen by every one of the Deputy's constituents and those who may be deciding whether they should vote for him and they see this reliable Member-----

Deputy Jim O'Callaghan: Is it because it is published that they have a liability?

Professor Joe Carthy: Yes.

Chairman: The Deputy will not mind if I will bring in Mr. Ryan who wants to add something.

Mr. Pat Ryan: I have been head of the Garda National Cyber Crime Bureau for the past six months. One of the issues, even in terms of regulations, is that time is of the essence with reference to content that is posted on social media websites. As Chief Superintendent Gubbins stated, it is like making a telephone call. It is instantaneous. One of the bigger challenges we will have is that the content may not reside in this jurisdiction. When something is posted online, it does not take long for it to be on other social media websites. That is also a challenge for An Garda Síochána. In bureau investigations I have seen the difficulties in getting evidential data which is online. That is something that will need to be considered in any future proposal or regulation. The key message from me is that time is of the essence in order that if something happens in this jurisdiction, it can be taken down quickly. Also, there should be no delays because once something is online, it can be anywhere.

Deputy Jim O'Callaghan: I thank the Chairman. I have gone on a bit too long.

Chairman: I thank the Deputy. Before I bring call the next Deputy, I want to flag that as this is one of our substantive issues to be addressed, we will be publishing a full report with recommendations. I am putting members and the panel on notice. We would like the panel to join us for a group photograph at the end of the session. If Deputies are heading off to fulfil any other engagement or responsibility, I ask them to keep an eye on the monitors and join us at the end of the meeting.

Deputy Martin Kenny: I thank the delegates for their contributions. I want to tease out the issues a little. It was stated correctly that there were some pieces of legislation. I note that Deputy Donnchadh Ó Laoghaire has a Bill, as does Deputy Howlin. A number of Deputies have brought forward legislation to deal with some aspect of the subject. While that is part of it, our work involves looking at the bigger picture to see how it can be added to, expanded and turned into something which will be robust and strong enough to deal with these issues. I am aware, as the previous speaker said, that there is an international dimension as the material goes outside the jurisdiction. We do not how one would reach a platform based, for example, in Azerbaijan. That is one of our difficulties.

I return to the key points and the example Deputy Jim O'Callaghan gave or a similar case.

While there is a civil case a person could take against an individual who has posted the piece of information or image and there may also be an element that could constitute a criminal case, the difficulty most people have is that, as regards the ability for it to be shared and the responsibility of those who share it, the company involved steps back and leaves the individuals involved to fight it out among themselves. The company gets away without having to take any real responsibility.

There are a couple of points I want to make. On traceability, surely there is a sense that there is almost a fingerprint for each individual engaged on the Internet. We all hear, at least anecdotally, that all of the companies are geniuses at being able to trace and know everything about every part of our lives and that they engage in all of this analysis to determine whether we like country and western music or opera, or whether we are into this, that or the other. From our interactions with others, they can almost identify people. If they are already doing this, mainly through the use of artificial intelligence and various algorithms, it suggests that it would not be that difficult to to identify each individual, even where someone uses a false name and identity. From his or her interactions with others, they will get to know who a person is and what is what. In being able to find out his or her identity, is there a case for making a company responsible for being able to identify each person?

The example of the automobile industry was given. For instance, if any of us here produced a piece of electronic equipment, we would have to send it away to be tested to obtain CE certification to indicate that it was valid and could be sold and used. Surely if any of us here produced an app, there should be an authority somewhere where it would have to be tested to ensure it was fit for purpose and use. Is there an international example of such an agency - An Garda Síochána might know - that does this or is there any effort at European level to do it?

Chairman: I will start with Chief Superintendent Gubbins.

Mr. Michael Gubbins: I will have a go at answering that question. I will come back to what Professor Carthy stated about people having to prove who they are and their identity.

In the nature of the business my colleagues and I are in, people do it on a regular basis, but they use a false identify. No matter what we put in place, people will always find a way around it. We must take this into consideration. It impacts on traceability. From what we have seen in some cases, people will generally create a new account to accommodate some of their criminal activities online. It will not be personal, for example, to Michael Gubbins. Such people will create a pseudonym when they go online, so there will be no history to support their identification. The Deputy spoke about companies' responsibilities. He is right. I always look at the privileges and responsibilities of those big service providers. They are big companies that make big money and they support a lot of employment, but they have a responsibility to protect citizens and their users, whether in Ireland or abroad. We are here in this room this morning but those companies are not. Some of what we are looking at is a new phenomenon. We need to talk to these companies. The Deputy is right to say that many clever people work for them. We need them to face the issues that have developed as a result of their products. The Deputy spoke about CE marking for cars and other products. Because of how these service providers' applications facilitate us - and it might be one application today but another in the future - we need to be able to identify issues and ask them how they can help and what they can suggest in that regard.

There are competing demands in the area of privacy of data and retaining information. Companies might be headquartered in Ireland but the data for which we are looking might be

somewhere else. We then need to use mutual legal assistance treaties to get those data. It can take a while to get through that process and, when the request is responded to, the data might not be there so the next step might not be available to us. As a result of GDPR and so on, it is less likely that data will be available to help us with our investigations. As Detective Superintendent Ryan said earlier, time is of the essence. There is probably an opportunity for Ireland to take the first step in working with these bigger companies to find solutions as many of them have headquarters here. We need to push it out, rather than looking outside and bringing it in. Let us start at home first.

Chairman: Before I go back to Deputy Kenny, now is an appropriate time to mention that representatives of these companies will be sitting in Chief Superintendent Gubbins's seat next week.

Mr. Michael Gubbins: Right, that is good.

Deputy Martin Kenny: The chief superintendent is saying that there are no international examples of this. It is a matter of starting from scratch.

Mr. Michael Gubbins: We are starting from scratch. Law enforcement works with various service providers. They give us training, they tell us what is available, they tell us how to understand the information they provide, and they tell us how to get it. They are also involved with bodies such as the Virtual Global Taskforce with regard to images of child abuse. They also report imagery to the National Centre for Missing and Exploited Children, NCMEC, which is based in the US, and those cases are then forwarded to various countries for investigation. With regard to this particular phenomenon, we have to tell them about our problems and identify ways to work more closely with them.

Deputy Martin Kenny: The chief superintendent has made the point that the Internet is instantaneous. That is what is brilliant about it. One pushes a button and gets one's information immediately. It is a little bit too much of us to expect these companies to be able to detect when somebody posts a false or hateful comment or an offensive image and to take it down immediately. With regard to the period of time they have to do so, however, people have told me that in some instances untrue, dangerous and terrible stuff about them has been left online for months on end. It can sometimes stretch to years despite those affected continually asking and pleading with these companies to take it down. Even when An Garda Síochána brings the problem to the attention of the companies the content is sometimes left in place. Is there a need for additional legislation to force the providers to remove such content? The legislation about which we are speaking goes some distance towards that end. How do the witnesses feel about it?

Mr. Michael Gubbins: One finds that most of these social media companies will quote their community rules. If one asks for something to be taken down, they will say that it does not breach the rules. As a country and as citizens, we have to challenge those community rules. The committee will have an opportunity to address this next week, but I do not think that will get us where we want to be. It will have to be regulated and legislated for.

Deputy Martin Kenny: The other-----

Chairman: If any of the other witnesses wish to add to what Chief Superintendent Gubbins is saying, I invite them to take the opportunity.

Mr. John Church: I will make a couple of points and will try not to repeat everything. The Deputy makes a very interesting and valid point about traceability and fingerprints. Many intel-

ligent people are able to figure out who we are. I am not about to open the debate on the digital age of consent again, but the big issue we have is that children and young people, by their very nature, lie about their age to get onto these platforms. There needs to be a greater onus on the Facebooks of this world to verify that age. Many 13 year olds want to go into the discos where the 16 year olds are. It is absolutely normal behaviour for children and young people. There should be more of an onus on the companies in that regard. In my opening statement, I made reference to the industry event the ISPCC ran with Technology Ireland, a trade association under IBEC. The industry was present at that event. We talked about the whole concept of safety by design and about encouraging, rather than forcing, platform and app developers to take child safety into consideration in this regard. We talked about the idea of a CE-type mark. That idea came up. To the best of my knowledge, mobile phone operators in the UK are forced to issue phones set up as if they were to be bought by children. There are small measures that could be taken that would play a big part in protecting children.

Deputy Martin Kenny: I thank Mr. Church. That is fine.

Chairman: I thank Deputy Kenny for his contribution.

Deputy Catherine Connolly: I thank the witnesses for their presentations, which I have read. Common themes emerge, such as the lack of borders and harmful information spreading very quickly to very large audiences with no mechanisms to deal with it. There is a gap between legislation and the platforms as a result of how quickly they develop. There is a huge gap in legislation. I thank the Law Society for its submission, in which it points out that we rely on the Post Office (Amendment) Act 1951 to deal with some of these issues. It is a terrible subject and difficult to listen to. I may come back to the ongoing training being provided to gardaí to deal with these very difficult subjects. No amount of legislation will sort this, although legislation is needed. It is clear that legislation should always be a last resort. Of course we need punishment for people who offend, but education is a very significant element as well, as are mechanisms that can deal with these issues very quickly so they do not progress further. We might look at that next week.

I thank the delegation from An Garda Síochána for its opening statement. It says, "It is planned that other members of the Garda Síochána will be trained in cyber crime awareness". When will that planned training start? It is crucial.

Mr. Michael Gubbins: The current position is that all new-----

Deputy Catherine Connolly: I understand that; I read that. That refers to gardaí in training. What training is to be provided to gardaí in service?

Mr. Michael Gubbins: We are working with the Garda College on the development of an elearning programme.

Deputy Catherine Connolly: Has that been rolled out?

Mr. Michael Gubbins: It has not been rolled out yet.

Deputy Catherine Connolly: When will it be rolled out?

Mr. Michael Gubbins: It will be next year at this stage.

Deputy Catherine Connolly: I understand that the work of the Garda is very difficult, but why is that being delayed? It is essential.

Mr. Michael Gubbins: It is essential. We have a lot on and we just have not got it finished yet. The Garda National Cyber Crime Bureau is a small bureau. Much of its work and resources go into the examination of seized computer media relating to child sexual abuse material.

Deputy Catherine Connolly: Would it be fair to say that the bureau needs more resources to deal with this area?

Mr. Michael Gubbins: Additional resources are always welcome.

Deputy Catherine Connolly: As is more training. It is not just welcome, it is-----

Mr. Michael Gubbins: It is necessary.

Deputy Catherine Connolly: It is absolutely essential if we are serious about doing this.

Mr. Michael Gubbins: It is recognised in the new operating model and the Commission on the Future of Policing in Ireland data. Regional hubs will be established, which will feed into a national hub. First responders around the country, those who carry out searches and so on, will be trained in cybercrime issues next year.

Deputy Catherine Connolly: I had the privilege of listening to the Garda Commissioner talk about this, so I am aware of all that. It is worrying that we must wait until next year.

Mr. Pat Ryan: May I add to that? By the very nature of cybercrime, it changes every day.

Deputy Catherine Connolly: That is right.

Mr. Pat Ryan: My bureau is currently updating all content to ensure it is relevant and captures all new forms of cybercrime.

Deputy Catherine Connolly: How many staff members does the bureau have?

Mr. Pat Ryan: The bureau is made up of 32 people in total.

Deputy Catherine Connolly: It has 32 staff members. How many staff are required to do the job effectively?

Mr. Pat Ryan: We have a plan, which has been approved by the Garda Commissioner, to bring our numbers up to approximately 120 over the next two years. That will facilitate staffing for our regional cyberhubs too.

Deputy Catherine Connolly: What provisions are made for training gardaí for this difficult work?

Mr. Pat Ryan: We need constant training for the work that we do and to be kept up to date with the latest threats and trends. A number of members are undertaking a master's degree in computer forensics and cybercrime investigations in UCD. We also work with the European Union Agency for Law Enforcement Training, CEPOL, which has a new cybercrime academy, and regularly attend its training sessions. There is specific training on computer forensics for the toolsets that we use to carry out our investigation.

Deputy Catherine Connolly: Does Mr. Ryan have statistics relating to cybercrime about the gender of the perpetrators and victims?

Mr. Pat Ryan: I do not have the information with me.

Deputy Catherine Connolly: Does Mr. Ryan have access to the numbers? Could we have access to them to understand this?

Mr. Pat Ryan: We have statistics but the most significant issue that I have seen since I joined the bureau is the under-reporting of this type of crime. We can only give statistics about crimes that have been reported to us that we are actively investigating. There are difficulties in getting the bigger picture across the jurisdiction, especially about what we are talking about now. The level will be difficult for us to understand. There is a significant issue with under-reporting across all cybercrimes.

Deputy Catherine Connolly: I think everybody would agree with Mr. Ryan, not just about cybercrime but all crime. It is especially low when it comes to sexual violence. I would have thought we learned from that. We have spent a long time in the Dáil trying to get a second SAVI report to establish the prevalence of sexual violence. We are all fighting and speaking from the same book. What has An Garda Síochána done and what resources has it committed to obtain accurate knowledge and facts? What can the witnesses direct me to so that I can see what is happening with crime online?

Mr. Michael Gubbins: I cannot give the Deputy anything this morning. I will take her question away and come back with an answer because I do not have the facts or the figures. I would have to utilise the Garda analysis service to help me with that. Mr. Ryan and I can probably speak anecdotally about what we see coming before us. With child abuse imagery, one will generally find that males are the offenders. There is a mixture of offenders and victims, both male and female, involved in online harassment.

Deputy Catherine Connolly: Perhaps Mr. Gubbins could come back to me with that. I appreciate that. Have service providers, which will be coming before us in the next two weeks, provided the Garda with any breakdown of the types of problems they encounter in the Garda's co-operation with them?

Mr. Michael Gubbins: No. Our main work with them is on training and to see how we can develop better relationships with them. We are looking for data or information to assist us with our investigations, and it is either here in Ireland or it is not. They will only give us what they can because we are investigating something in Ireland. Other than that, we have to use a mutual assistance request. We have not got a breakdown from service providers about the crime types that occur on various platforms.

Deputy Catherine Connolly: I try to avoid social media as much as I can, so in that sense I am no expert. A separate problem to the one we are talking about today is the shocking amount of time young people spend online. I think it is ironic that the companies making a fortune seek to provide an education space for their own children that has none of those distractions. I am asking the witnesses not to be anecdotal even though I am. That is what I read. The facts are essential so that we can come to terms with this. It is a balancing act between freedom of expression and privacy.

Mr. Michael Gubbins: If I take off my Garda hat and put on my parent's hat, the Deputy is right that kids spend an inordinate amount of time on social media and the Internet, either watching movies or communicating with their friends. That is the medium through which they communicate today. As a parent, I have done my best to have a conversation with them about the privilege of having access to this instantaneous information and communication and to understand how they use it and behave on it. They are the same rules as one would apply if meet-

ing a person in one's house or elsewhere, including not being rude to them or displaying images of them. We have had some interesting conversations over dinner following from things I have seen at work. I cannot reiterate enough the importance of parents taking responsibility and having a conversation with their children about balance and how to behave online. It should be no different from how they behave if I or their mother was in the room.

Deputy Catherine Connolly: I agree with Mr. Gubbins. There is no doubt about that. We all have parental responsibility. We are meeting the companies in the next two weeks. This meeting is to assist us in establishing the problems, their extent and how we strike a balance when writing up our report. Statistics are vital in that regard.

Moving away from statistics for a moment, I have questions for Ms Counihan on another topic, the name of which I hate, that is, revenge porn. The Rape Crisis Network Ireland, the National Women's Council of Ireland and the submission from the solicitors have all raised it. There is a different expression that I think captures it much better. Will Ms Counihan elaborate on that?

Ms Caroline Counihan: We tend to say "image-based sexual abuse". Some people among us would say "image-based sexual violence". Image-based sexual abuse is a term that is favoured, as far as I know, by former Senator Jillian van Turnhout. I think it was introduced by Professor Clare McGlynn from Durham University, who also made a submission.

Deputy Catherine Connolly: That is right.

Ms Caroline Counihan: I think that captures much better the harm that is done by this online harassment and harmful communication.

Deputy Catherine Connolly: Does anyone else here have a difficulty with stopping the use of the term "revenge porn" and instead using this other language, which has less implicit blame of the victim?

Mr. John Church: I thank the Deputy for making us think about it. We will change our language as a result of that.

Deputy Catherine Connolly: I thank Mr. Church.

Mr. Michael Gubbins: From a Garda point of view, the term for years was "child pornography", and it has become "child abuse material" in our vernacular in recent years. We have moved away from using the word "porn". It is within the legislation, so we have to refer to it then, but when we are describing imagery, we use "child sexual abuse imagery".

Deputy Catherine Connolly: I thank Mr. Gubbins. My background is in law. I think Deputy O'Callaghan mentioned this matter too. In one of the submissions, the witnesses referred to harm to the person as a way of defining the crime. Would they be able to elaborate on that? I had a little difficulty with the subjective nature of it.

Ms Caroline Counihan: The Rape Crisis Network Ireland sees the real effects. People come in to rape crisis centres, use helplines and email us.

Deputy Catherine Connolly: I have no doubt about that and I fully accept the harm. How does one define that within legislation?

Ms Caroline Counihan: I would be inclined to frame it as broadly as possible through a

definition which includes, but is not limited to, psychological, economic or career harm. It does not involve direct physical harm but can involve just about every other kind of damage to any other area of a person's life. In the context of intimate partner violence, the mechanism by which the harm is caused and the nature of the harm is sometimes entirely individual and personal. For instance, in a pattern of coercive control, an abuser will often know exactly what will drive his victim mad and distress her the most. Because he knows her situation, he knows exactly what to say to her boss to cause her untold problems at work. I am in favour of a broad definition. Abuse is very often individually tailored to the circumstances, particularly in a long-term abusive relationship. One cannot be too definite. We have to be broad.

Deputy Catherine Connolly: I understand that. We might come back to this. The submission from the legal profession makes a similar point. It argues that the focus should be on harm inflicted and that consideration should be given to defining harmful content. I have no problem with that.

Ms Caroline Counihan: However, I will half contradict myself and note that there is another school of thought. The Scottish legislation is a good example. It advocates shifting the focus from the level, nature or anything to do with the harm inflicted on the victim and onto the intention of the perpetrator. Does that person have subjective intention to cause harm?

Deputy Catherine Connolly: It is a tricky area.

Ms Caroline Counihan: It is a tricky area.

Deputy Catherine Connolly: We need to come back to that. My last question concerns other models. New Zealand, Australia and Scotland have been cited in the other presentations. Has an Garda looked at that? Have its members visited those jurisdictions?

Mr. Michael Gubbins: No. One of the questions concerned cyberstalking. Section 4A of the UK's Protection from Harassment Act 1997 concerns "Stalking involving fear of violence or serious alarm or distress". That might address some of the Deputy's questions in that regard. Here, most of the criminal offences around harassment are covered by the Non-Fatal Offences Against the Person Act 1997, while in the UK stalking would seem to be encompassed under 4A of the Protection from Harassment Act 1997.

Deputy Catherine Connolly: Is anyone more familiar with the New Zealand regime? No. I refer to the calls for a digital safety commissioner. This suggestion came from the Law Reform Commission, and all of the witnesses endorse it. Would that be separate from the office of the Data Protection Commissioner, Ms Helen Dixon? Is there a need for another office and another official?

Professor Joe Carthy: Absolutely.

Deputy Catherine Connolly: Can the witnesses tease that out for me? Why?

Chairman: Would Mr. Gubbins like to answer?

Mr. Michael Gubbins: I will be brave. Ms Dixon's office concerns data. To some extent the digital safety commissioner would conflict with the Data Protection Commissioner's role. The Data Protection Commissioner is concerned with how we manage information and data and whether we should or should not keep it. The digital safety commissioner would actually look for information to help him or her to protect citizens. There is a slight conflict, so they

should be two separate entities and not rolled into one office.

Chairman: I thank the witnesses. I ask the chief superintendent to furnish the statistics and information to the clerk to the committee when he gets the opportunity. We will circulate them to Deputy Connolly and all other members of the committee.

Deputy Jack Chambers: I thank the witnesses for their very comprehensive presentations and submissions. I wish to follow up on the point my colleague, Deputy Connolly, made. We have many suggestions for legislation. Deputy O'Callaghan mentioned codifying the right to privacy. Others have mentioned verification of identity, which is important. Has any country brought those moving parts together in any way? We are at a very primitive stage in addressing this. The witnesses are all nodding their heads, which I will take as confirmation. Mr. Gubbins made an interesting point, which follows what Professor Carthy said. One issue that seems to arise from the get-go is that a false identity can be used to create an account or multiple accounts. If we legislated to require age verification, it would mean that the publisher, that is, the account holder, could not hide behind anonymity. That seems to be a huge issue across all social media platforms. A lot of these problems proliferate through fake accounts. It could be simple legislation. The problem arises in making it cross-jurisdictional and regulating it. Do the witnesses have any thoughts on that?

I believe that if people express something, they should stand by it, whether it relates to what we are talking about today or is potentially defamatory, as Deputy O'Callaghan mentioned. If a journalist writes something, it is published in a newspaper and the journalist stands over what he or she has written. It seems that on the Internet, the majority of difficulties arise from accounts that nobody can track or verify. Do the witnesses have any thoughts on how to deal with that properly? Professor Carthy mentioned registration. I note that Government services require proper verification of identity. How do we deal with that?

Professor Joe Carthy: It is fairly straightforward. In Ireland, a person cannot apply for a driver's licence without proving that he or she is of the appropriate age. If Ireland does something, other countries will follow. We are waiting for countries to take sensible steps in this. Jurisdictions around the world are at a primitive stage, but if Ireland adopted sensible legislation, other jurisdictions would see that it makes sense and would follow in our footsteps. It is not a technological difficulty. The companies that appear next week will make all sorts of protests about it, but this could be a very straightforward mechanism. It can be solved by the technology in a very straightforward way and it would make a huge difference. We cannot overstate the difference verification would make. We should also remember that most of the people on the Internet are sensible people who do sensible and good things. Not everybody has a fake account. A small subset of the population is misusing the Internet. I would not want to give the impression that everyone in the population is using the Internet in an inappropriate manner, but unfortunately a significant number of people do and inevitably anonymity exacerbates the problem.

Mr. Michael Gubbins: I agree with Professor Carthy up to a point. We could pass legislation requiring users to verify their age and identity, but as my colleagues and I find every day, there are false IDs, passports, and driving licences. People will figure out a way around giving their correct age. They will produce something that verifies an age and an identity but they will find a way around this if they want to. Verification will address situations where somebody loses their head and does something wrong. If that person has not hidden his or her identity, we will be able to pursue them. It will make a dent. However, anyone that is seriously intent on hiding their identity will figure out a way around it despite legislation and verification.

Mr. Pat Ryan: It is fair to say that whatever system we put in place will have to be very robust. Young people and teenagers are very tech-savvy nowadays. It would be a huge challenge, as the chief superintendent said.

Deputy Jack Chambers: The problem is that now all people need to do to establish they are of a certain age is to click on a button. There is no barrier to people wanting to set up a fake account. There need to be at least some soft measures. This would remove an element of what we see. I agree that it would not be absolute.

Regarding the cross-jurisdictional approach, are the witnesses aware of anything in the European context that involves trying to restrict what we are seeing or is it still siloed within nation states?

Professor Joe Carthy: I believe it is still siloed.

Deputy Jack Chambers: I know many companies reside here. Have the witnesses had any engagement with them about piloting the verification process? Have there been any informal discussions with any of the witnesses about a feedback loop from the witnesses regarding difficulties? Do they have engagement or collaboration with companies to flag up their concerns or have companies even been open to that?

Mr. John Church: I am a member of the National Advisory Council for Online Safety, which is under the Department of Communications, Climate Action and Environment. Google, Facebook and Vodafone are members of that council. Age verification does come up. It is acknowledged by some platforms that it is a challenge but so far, there has been no desire to fix it.

Deputy Jack Chambers: What is their standard response? Is it that they are community service providers and do not-----

Mr. John Church: -----yes, and that it is not possible to fix it overnight. Mr. Gubbins mentioned this as well. It is a fact of life that children will find their way around it but where there is a will, there is a way. The reason for not doing it is commercial. The reason for doing it is more of a civil and child protection issue. I set up a Revolut account the other day and had to go through a number of things to verify that I was the right person. There is a way if the companies want to do it. The issue is that an awful lot of users would fall away and then advertising revenue would fall away as well so perhaps these companies have to operate under a different model with less revenue. There is a thing.

Deputy Jack Chambers: Probably a lot of their share price is skewed based on fake accounts. An issue that goes beyond here is that of fake news, much of which is centred in countries that probably have less regulation than we would have. Many of these issues could be resolved with a verification process because we would see a levelling of people. As Professor Carthy said, the majority of people are there to have a community platform. Many residents' associations have internal groups where everyone knows each other and is properly verified. The external manifestation of many of these platforms involves anybody and everybody and the same individuals behind multiple accounts. There is no technological difficulty but a commercial one. There is a lot of discussion about corporation tax in an Irish context but we have a responsibility in the global context to properly regulate these entities because they constitute a platform of significant harm, as the witnesses have all noted. It has to happen regardless of whether it is through legislation, co-operation or regulation. I thank the witnesses for their submissions and information.

Senator Frances Black: I thank the witnesses for their presentations. Deputy Chambers covered many of the questions I wanted to ask. This area is a minefield. As Deputy Connolly said, it is very upsetting to hear about what is happening. We know what is happening and we know about online abuse. We hear stories of children being bullied online and suicides. I am a grandmother with two very small grandchildren - two beautiful little girls. I often think "my God, what's ahead for them?" To think about what can happen to children between the ages of six and 18 who are online is pretty shocking.

Some of the recommendations in Professor Carthy's presentation were very interesting. His presentation was really powerful. As he notes, it is quite simple. It is not rocket science but I imagine there would be a significant backlash from the big corporations because Professor Carthy's suggestion will have an impact on their profits. I know what that is like in here and what such a battle can look like and about trying to get as much support for what one is trying to do. I know Airbnb has a system where someone registers for an account and must provide a scanned version of his or her passport to verify his or her identity. That is one example of how it works. The companies will come before this committee next week. What does Professor Carthy think they will say about this? What will be their protests? He mentioned that they will protest against it so what will they say? I hear what An Garda Síochána is saying but at the end of the day, it is like road safety. What will the companies protest about? What are their arguments against it?

Professor Joe Carthy: They will probably argue that they are multinational companies, must abide by laws in different jurisdictions and that it is not possible to tailor their systems to one small country with 4 or 5 million people when they have 300 million people across the world. They would argue that if they were to do this for every country, it would not be possible for them to do so. That would be the most logical defence if I was sitting in their place.

Senator Frances Black: Would I be right in saying that this would be their only argument?

Professor Joe Carthy: I cannot see that they have any legitimate argument apart from the cost of doing business. There is a serious cost here but there is an argument that this is the cost of doing business.

Senator Frances Black: Have any studies been done on children or young people and their relationship with social media? I am not just talking about children. I am referring to us all. One hears about the really strong connection - almost addiction. They are almost addicted to it. We can all get caught up in it, including me.

Professor Joe Carthy: Mr. Church is probably better placed to address that question. The Internet is a very valuable resource. The Senator expressed worry about her grandchildren. They are coming into a world where they have access to such rich resources from the Internet for their education and development. We are looking at the bleak side today but there is a hugely positive aspect to this and it would be a pity for us not to-----

Senator Frances Black: We are only talking about the bleak side today.

Professor Joe Carthy: Mr. Church might be better able to address the Senator's last question.

Mr. John Church: I echo Professor Carthy's comments. The Internet is mostly positive. We conducted some research in 2016 and 2017, although it may have been in 2017 and 2018. I must check. Among other things, we asked respondents about length of time spent online and

the material they accessed. We also asked parents about their involvement. Some findings were of great concern. While something like 60% of parents played an active part in most of their children's online engagement, quite a significant percentage of parents did not. When probed, it emerged that they probably feared the technology. They were not familiar with the technology and it was a topic with which they did not wish to deal. It was easier to just hand the tablet over and allow it to become another babysitter.

Senator Frances Black: Yes.

Mr. John Church: On the positive side, we found that the vast majority of content accessed was of educational benefit and only a small percentage was of concern. We did ask if any child experienced what we would call cyberbullying or harassment and we have all that information. It is now in the public domain so we are happy to share it with the committee if that would help.

Senator Frances Black: That would be great.

Mr. John Church: To the best of my knowledge, I do not think it has been done in Ireland. There is a programme to do it on the National Advisory Council for Online Safety. It has been done in the UK. To the best of my knowledge, it is unique information and is quantitative as well as qualitative.

Senator Frances Black: That is great. I thank our guests for their presentations. Deputy Connolly spoke about what An Garda Síochána is working on at this time and it sounds as if there is a lack of resources. This should be one of the top priorities going forward. It is a minefield and it is difficult but people being bullied online is one of the most worrying trends we must face. I sometimes see it happening online and it is horrible. I cannot imagine what it is like for young people who are bullied and the mental health issues that result. The bullying can be by means of sexual abuse or mental abuse and it is awful. People have been driven as far as suicide because of it. It must be a priority for An Garda Síochána and I look forward to hearing what the Garda will do in that area. It is something that should be looked at in terms of resources.

I would like to know what language should be used. We can ask young people to be careful about what they are doing online and tell them not to smoke or drink too much but I would love to educate myself and get to the core of how to manage the conversation that must be had with young people. That is a vital conversation and I do not have the expertise. I can tell young people to be careful and to mind themselves or ask them what is going on and try to monitor them but I would love to be more educated. I imagine most parents and grandparents would love to know more so as to try to protect their children and grandchildren. I thank our guests.

Chairman: It occurs to me, before I bring our session to a close, to ask if there is a concluding comment or piece of wisdom, even a question for next week's session, that any of our guests would like to suggest? If our guests were in our places and their seats were occupied by representatives from Facebook, Twitter, Google and the Internet Service Providers Association of Ireland, would they have any final comment to make before we draw to a close? Have we covered everything?

Professor Joe Carthy: To follow up on Senator Black's comment, it would be interesting to understand what action representatives of these companies would consider appropriate for their company to take if one of their children was a victim of bullying or harassment.

Ms Caroline Counihan: Mr. Church mentioned the idea of safety by design and building

safety in from the very beginning of an enterprise, in co-operation between law enforcement, Internet service providers, victim support organisations, organisations such as the ISPCC which support children and, in this country, the National Advisory Council for Online Safety. The idea is that everybody gets around the table and explains what should not be included in the design of a new programme, application, or form of communication on the Internet in the first place. Let us not even nip it in the bud but, rather, make sure there is no bud to nip in the first place. I would like to know what the attitudes of the representatives from the tech companies would be to that.

Mr. John Church: I would ask the representatives of those companies the very question the committee asked us, which I could not answer properly, namely, what are the barriers to proper age verification?

We also spoke about education. The point was made that this is not purely about the legislation, but also education and starting to teach children how to be safe online from an early age and to teach a parent how to have that conversation. We counted 29 different organisations that are going into our primary and post-primary schools and probably teaching 29 different curricula. It should be on the curriculum for the Department of Education and Skills.

I agree that the platforms are, to some extent, very educational tools but what are they doing in order to turn the conversation, switch it around and educate children? A glut of funds is being thrown at various organisations by Google and Facebook. Is that just a box-ticking exercise or is it a true attempt at educating our children?

Mr. Michael Gubbins: People have spoken about safety by design and it is something that the industry and supply chain for network devices are looking at. Security by design means baking in the appropriate considerations from the beginning. We are all at the start of this. Somebody referred to the wild west earlier on and it is a bit like that because we are at the start of this.

It is worth remembering that there are vulnerable adults out there, as well as children, who have got themselves into a predicament and are worried and stressed. Senator Black spoke about people who have taken their own lives. Children are important but we also need to ask what responsibility those companies have for their adult users.

Chairman: It only remains for me to thank Chief Superintendent Michael Gubbins; Detective Superintendent Pat Ryan; Mr. John Church, the chief executive of ISPCC; Professor Joe Carthy, the director of the UCD centre for cybersecurity and cybercrime investigation; and Ms Caroline Counihan, representing Rape Crisis Network Ireland. I thank them all for their participation and for sharing their valued expertise and knowledge. I also thank the members of the committee who participated. I invite our guests to join committee members for a painless photograph. We will do likewise with those who will be with us next week.

The joint committee adjourned at 11.30 a.m. until 9 a.m. on Wednesday, 9 October 2019.