DÁIL ÉIREANN

AN COMHCHOISTE UM LEANAÍ AGUS GNÓTHAÍ ÓIGE

JOINT COMMITTEE ON CHILDREN AND YOUTH AFFAIRS

Dé Céadaoin, 25 Deireadh Fómhair 2017

Wednesday, 25 October 2017

Tháinig an Comhchoiste le chéile ag 9.30 a.m.

The Joint Committee met at 9.30 a.m.

Comhaltaí a bhí i láthair / Members present:

Teachtaí Dála / Deputies	Seanadóirí / Senators
Denise Mitchell,	Colm Burke,*
Tom Neville,	Máire Devine.
Anne Rabbitte,	
Sean Sherlock.	

* In éagmais / In the absence of Senator Catherine Noone.

Teachta / Deputy Alan Farrell sa Chathaoir / in the Chair.

Cybersecurity: Discussion (Resumed)

Chairman: I thank the witnesses and members of the committee for their presence. This morning we will hear from representatives of An Garda Síochána and from the Office of Internet Safety and CyberSafeIreland on the topic of cybersecurity with regard to children and young adults.

I welcome from An Garda Síochána Mr. John O'Driscoll, assistant commissioner in the area of special crime operations, Mr. Declan Daly, detective superintendent in the Garda national protective services bureau, and Mr. Michael Gubbins, detective superintendent in the Garda national cybercrime bureau.

Before we commence, in accordance with procedure, I am required draw the attention of the witnesses to the fact that by virtue of section 17(2)(*l*) of the Defamation Act 2009, witnesses are protected by absolute privilege in respect of their evidence to this committee. However, if they are directed by the committee to cease giving evidence in relation to a particular matter and continue to so do, they are entitled thereafter only to a qualified privilege in respect of their evidence. Witnesses are directed that only evidence connected with the subject matter of these proceedings is to be given. They are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person, persons or entity by name or in such a way as to make him, her or it identifiable.

Members are reminded of the long-standing parliamentary practice to the effect that they should not comment on, criticise or make charges against a person outside the Houses or an official either by name or in such a way as to make him or her identifiable.

I remind all our guests and visitors to switch off their mobile phones as they interfere with the sound system, making it very difficult to broadcast such matters, including our web streaming.

I advise our witnesses that any submissions or opening statements they have made or will make to the committee will be published on the committee website after this meeting. I understand witnesses will make a short presentation which will be followed by questions from members. I invite our first witness, Mr. O'Driscoll, to make his opening statement.

Mr. John O'Driscoll: I thank the Chairman. The Garda Síochána's modernisation and renewal programme 2016-2021 represents the first time the organisation has laid out its mission, direction, plans and challenges spanning a five-year period. The fact criminal activity changes and extends into new areas at a pace and that we have to react quickly and flexibly to cope with developments is stated in the document. In this regard, the Garda Síochána has recently made major changes in response to organised crime and security threats, and has new strategies to address other emerging crimes and security challenges. In particular, online child sexual exploitation is a constantly evolving phenomenon and is shaped by developments in technology, mobile connectivity, growing Internet coverage in developing countries and the development of pay-as-you-go streaming solutions, which provide a high degree of anonymity to the viewer and are furthering the trend in commercial live-streaming of child sexual abuse. Thus, it is necessary for the Garda Síochána to ensure it enhances its capacity to tackle the criminality involved, while being particularly alert to the vulnerability of its potential victims.

To a significant extent, responsibility for personal online security and protection rests with the user. However, as users get younger and are not as likely to be alert to cybercrime, espe-

cially in circumstances where the age of digital consent is to be lowered to 13 years, personal responsibility must also be supported by parents, teachers and responsible entities, including State agencies, such as the Garda Síochána. The issues surrounding unrestricted access to Wi-Fi are well publicised. Controls which existed at an earlier time in circumstances where children accessed the Internet at home or elsewhere under some form of supervision have been eroded by the prevalence of Internet cafes and mobile technology. It is now possible that a very young child can use a mobile phone to access the Internet over available public Wi-Fi networks and can search for or come upon pornographic or violent material with little or no parental control. Increasingly children are engaging in the sharing of self-taken imagery where they send nude and-or sexually explicit personal photographs of each other to other members of a chat group, utilising platforms such as WhatsApp or Instagram or other 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.

The modernisation and renewal programme sets out clearly that victims of crime will be put at the heart of the service provided by the Garda Síochána. In 2015, the Garda Síochána established 28 victim service offices across the country tasked with communicating with victims of crime and prioritising their needs. Protective services units, PSUs, 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. In 2015, through the creation of the Garda national protective services bureau, GNPSB, a number of units operating in various locations throughout the Garda Síochána were brought together to leverage their experience and expertise in investigating serious crimes against vulnerable people. The GNPSB 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, this bureau is responsible for working with other agencies to manage sex offenders in the interest of community safety. Among the specialist units now located within the Garda national protective services bureau, GNPSB, are sex crime management unit; online child exploitation unit; national child protection unit; sex offender management and intelligence unit; and the national SORAM office, which is a multi-agency office staffed by a members of An Garda Síochána, the Probation Service, the Child and Family agency and a representative from Dublin City Council housing section to manage sex offenders. Other units include the human trafficking investigation and co-ordination unit; the national victims office; and the missing persons unit.

Within the online child exploitation unit at the GNPSB a new unit has been created which is tasked with the identification of online victims of exploitation. Personnel attached to the GNPSB have received training to enable them to perform the role of specialist victim interviewers, particularly relating to children. Members of the Garda Síochána are often the first people victims of crime make contact with after a crime has been committed.

Victims of crime will often have had a traumatic and potentially life-changing experience and may be vulnerable and require help and support. However, while getting the first contact with a victim right is critical, so too is ensuring this care and attention continues as their case, which is incredibly important and personal to them, moves through the justice system. The Garda Síochána is acutely aware of the emotional and physical suffering of victims of child abuse and the fact their experience may make it very difficult for them to report the crimes they have suffered. They may also feel that their complaint will not be taken seriously or fully

investigated.

The online child sexual exploitation unit, OnCE, at the Garda national protective services bureau has responsibility for the enforcement of the provisions of the Child Trafficking and Pornography Acts 1998 to 2004 as well as the investigation and co-ordination of cases relating to the possession, distribution and production of child pornography and any related sexual abuse of children. The unit is also responsible for the proactive investigation of intelligence concerning paedophiles and their use of technology and the online targeting of suspects for the production, distribution, and possession of child abuse images on the Internet. New strategies have been developed to meet the ever-increasing challenges of cybersecurity and cybercrime. The modernisation and renewal programme sets out the intention of the Garda Síochána to expand its capabilities with regard to cybercrime through training with academic partners, increased investment in technology and people and regionalisation of the investigation of computer crime, which for many years was located within the Garda national economic crime bureau.

The Garda Síochána will establish a new national cybersecurity desk, NCSD, located at its crime and security section at Garda headquarters. It will liaise with national and international stakeholders, including the Europol national unit, ENU, Interpol national central bureau, NCB, police partners and security organisations such as the Europol EC3 unit, the European Network and Information Security Agency, ENISA, and Interpol.

It is also planned to establish a telecommunications and information technology security operations centre. This centre will include two separate dedicated units to deal with anomalies in information systems networks and provide cyber and forensic tools and infrastructure to support operational policing and State security activities.

The Garda national cybercrime bureau, GCCB, was established in September 2016, providing an enhanced structure within the 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. This bureau is tasked with undertaking the forensic examination of computer media in all incidents reported to the Garda Síochána. Furthermore, this bureau is given a role with regard to the provision of crime prevention advice to the public and the corporate sector regarding online offending and e-safety. This includes the provision of Internet safety advice.

Regional cybercrime investigation units, CCIU, are being established and such units are operating successfully on a pilot basis in New Ross, County Wexford and Ballincollig, County Cork. The regional units will provide computer forensic services locally under the supervision of the national bureau. With a view to further supporting the regional units, it is planned to develop and roll out first responder and triage capability nationally. These first responders will support the regional units and provide for a tiered level of capability nationally, with the Garda national cybercrime bureau as the top tier of support and capability.

The Garda cybercrime bureau, in conjunction with the Garda College, has developed a training module in the investigation of cybercrime for delivery to all students in the Garda College in Templemore. It is planned that other members of the Garda Síochána will be trained in cybercrime awareness and cybercrime investigation through our continuing professional development network.

The Garda Síochána will further its long-standing relationship with the centre for cybersecurity and cybercrime investigation at University College Dublin through the Garda computer

crime investigation unit and alumni who have undertaken courses of study at the university in the cyber domain. The Garda Síochána will also develop more educational partnerships with third level institutions and international institutions with expertise in cybersecurity to ensure the availability of cutting-edge knowledge throughout the organisation. We will look for opportunities to develop relationships and share expertise further.

In November 2017, personnel attached to the Garda cybercrime bureau will travel to Lyon, France to participate in specialist victim identification training relating to crimes against children, which training is being delivered at Interpol headquarters. This course will address the issue of the vulnerability of children arising from the availability of child exploitative material on the Internet.

Any adult, child, business or organisation using a connected device is vulnerable to cybercrime. Just as with offline crime, simple steps can often be effective in reducing the recognised vulnerabilities. Working in partnership with public and private sector stakeholders, the Garda cybercrime bureau will use the Garda Síochána's communication channels, "Crimecall", and public awareness campaigns to ensure that people are educated on protecting themselves from cybercrime. We intend to develop further our crime prevention activities in this area.

While it is not feasible to regulate or monitor the Internet in anticipation of all possible incidents such as cyberbullying, if a member of the public becomes aware of activity on the Internet which they suspect may be illegal, they can report it confidentially to *hotline.ie*. This is operated by the Internet Service Providers Association of Ireland with oversight by the Office for Internet Safety, OIS, in the Department of Justice and Equality. *Hotline.ie* provides the public with the means to report illegal online content such as child sexual abuse material and liaises with the Garda Síochána to have illegal content taken down.

The Office for Internet Safety, OIS, is responsible for developing strategic actions to promote the highest possible levels of Internet safety, particularly in combating child pornography. A dedicated website, *www.internetsafety.ie*, is supported by the OIS and provides information and links to other resources on Internet safety. In addition, it partners with experts to develop and publish a series of information booklets on Internet safety which are made available on the website and in hard copy.

In November 2014, the Garda Síochána launched an initiative on the blocking of child sexual abuse material, CSAM, on the Internet in Ireland. The OIS has an oversight role in the operation of *hotline.ie* and the Garda Síochána blocking initiative. *Hotline.ie* is the confidential service for reporting illegal content on the Internet in Ireland and liaises closely with the Garda Síochána in carrying out this function.

The Garda Síochána signed a memorandum of understanding, MOU, with one large Internet service provider under which the service provider agreed to block access to CSAM based on information which we provide to it. The Garda Síochána continues to engage with other service providers with a view to establishing further MOUs.

The Garda Síochána provides crime prevention advice to the public and the corporate sector regarding online offending and e-safety. This includes the provision of Internet safety advice to schools, third level institutions through, for example, the Campus Watch programme, and the public, through media releases such as the recent pan-European mobile malware awareness campaign, and through regular information releases in the national publications and the "Crimecall" programme.

Section 3 of the Communications (Retention of Data) Act 2011, obliges Internet service providers, ISPs, to retain data for one year. However, there is no penalty for a failure to retain such data. Section 7 of that Act requires ISPs to comply with a disclosure request made by the Garda Síochána pursuant to section 6 of that Act. However, if Internet providers fail to provide the Garda Síochána with data pursuant to the Act, our ability to identify people involved in the sexual exploitation of children or the distribution of child pornography on the Internet will be restricted.

The investigation of all 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.

Lockers is a new information and education resource 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, SPHE, 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.

The Garda Síochána is involved in the development of a new Webwise campaign, provisionally entitled Exposed, for delivery through secondary schools as a follow on from Lockers. This new campaign will be designed to address the issue of the sexual exploitation of children through the use of technology and will incorporate the "Say No!" campaign launched earlier this year by Europol with the support of the Garda Síochána. The "Say No!" campaign, including a ten minute video clip, was launched to advise the public on sextortion, the threatened release of self-generated sexual images or information to extort money or to coerce a person to provide more images, engage in sexual activity, or to do something they otherwise would not do.

In 2010, the European Union set up a four-year policy cycle in order to create a greater measure of continuity for the fight against serious international and organised crime. The policy calls for effective co-operation among law enforcement agencies, other EU agencies, EU institutions and relevant third parties. The EU initiative gave rise to the European multidisciplinary platform against criminal threats, EMPACT. Europol has identified nine priority crime areas. For each one, a multi-annual strategic plan, an EMPACT project and an operational action plan are implemented. As a form of cybercrime, child sexual exploitation is one of the nine EMPACT priorities in Europol's priority crime areas under the 2013-2017 EU policy.

Europol's European cybercrime centre, known as EC3, supports the competent authorities in member states in preventing and detecting all forms of criminality associated with the sexual exploitation of children. The head of EC3, Stephen Wilson, spent the past few days with us in Dublin. It provides assistance and expertise in combatting the distribution of child abuse material through all kinds of online environments and tackles all forms of criminal online behaviour against children, such as grooming, self-generated indecent material, sexual extortion and live streaming on the web.

Fighting the distribution of child abuse material includes preventing and intercepting it and

stopping it from being shared through peer-to-peer networks as well as through commercial platforms. In this regard, EC3 is involved in the European financial coalition against commercial sexual exploitation of children online, EFC, a network funded by the European Commission composed of law enforcement, non-governmental organisations, NGOs, and public and private sector stakeholders.

EC3 is also involved in the virtual global taskforce, VGT, a collaborative partnership of law enforcement agencies, which have come together across the digital divide to combat online child sexual abuse worldwide. The "report abuse" button on the VGT website is an effective way to report suspicious online behaviour.

Co-operation at an international level has proved very effective in identifying victims of child sexual abuse and exploitation. In 2015 Europol hosted a victim identification taskforce, which resulted in 240 new collections of material being uploaded to Interpol's child sexual exploitation image database and the extension of the existing 100 collections.

In addition, Europol's project, halting Europeans abusing victims in every nation, HAVEN, supports EU member states in detecting and intercepting child sexual offenders travelling abroad to abuse children. The violent crimes against children international task force, VCACITF, is a select cadre of international law enforcement experts working together to formulate and deliver a dynamic global response to crimes against children through the establishment and furtherance of strategic partnerships, the aggressive engagement of relevant law enforcement and the extensive use of liaison, operational support, and co-ordination. The VCACITF, formerly known as the innocent images international task force, became operational on 6 October 2004 and serves as the largest task force of its kind in the world. It consists of online child sexual exploitation investigators from around the world and includes more than 69 active members from 40 countries. The task force hosts a five-week training session for newly invited task force officers, bringing them to the United States to work side by side with Federal Bureau of Investigation, FBI, agents in the violent crimes against children programme. The VCACITF also conducts an annual case co-ordination meeting where task force members come together in a central location to share best practices and co-ordinate transnational investigations between members. Ireland, through the Garda Síochána, is an active member of this group and engages proactively with Europol, Interpol and the law enforcement authorities in EU member states and further afield, relating to a wide range of initiatives with an international dimension which are designed to tackle child sexual exploitation. The Garda Síochána will continue to develop its capacity to tackle cybercrime with a particular focus on protecting children and young people from the impact of the criminality involved and in this regard will interact in an appropriate manner with all relevant stakeholders.

Chairman: I thank the assistant commissioner. I invite Deputy Rabbitte to put her questions.

Deputy Anne Rabbitte: I thank the assistant commissioner for his presentation. Was Mr. Daly at the Irish Society for the Prevention of Cruelty to Children, ISPCC, meeting in Dublin Castle last year?

Mr. Declan Daly: Yes, I was.

Deputy Anne Rabbitte: I clearly recall that presentation and I was highly impressed to say the least.

Mr. Declan Daly: Thank you very much.

Deputy Anne Rabbitte: I note that An Garda Síochána believes that personal responsibility must also be supported by parents, teachers and responsible entities. Does the assistant commissioner have any views on how personal responsibility can be fostered among these groups, particularly in light of the lowering of the age bracket to 13? What recommendations would An Garda Síochána make to protect these entities?

Mr. John O'Driscoll: Perhaps Mr Daly could give some examples of where we are engaged in initiatives, particularly where we have interacted either directly with schools or with people who will go to the schools and impart particular knowledge.

Mr. Declan Daly: The prevention side is very important to us. We do not want this type of crime occurring in our communities. It falls into two categories: education and awareness, which are key; and the more proactive initiatives, such as blocking, as mentioned by the assistant commissioner in his opening statement. In education and awareness, we are heavily involved with the NGO sector, for example, with Sport Ireland and the GAA, to enable their members impart the message of the dangers present on the Internet to parents and children. We are very proactive in passing this message to the communities. We give media interviews to get the message out. It is exceptionally important to us to send the message that the Internet is a valuable tool but that it has inherent dangers which children and parents need to be aware of. We work very closely with Webwise. We are involved in the Internet safety day on 6 February. That is all important to keep sending the message that children need to be safe, and what they need to do to be safe, on the Internet at a high and strategic level. On the other side, there is our detection and enforcement work.

Deputy Anne Rabbitte: How many staff work in the many units Mr. O'Driscoll listed?

Mr. Declan Daly: Does the Deputy want the online perspective?

Deputy Anne Rabbitte: Yes.

Mr. Declan Daly: From the online perspective, we have three sergeants, a detective inspector, seven detective gardaí and two more have been allocated to us and will arrive next week. That is in the national unit. We are lucky in that the online child exploitation unit acts as a sort of clearing house. That unit, with those resources, however, does not have the capacity to deal with all cases. We recognise that. We have certainly used all the resources of An Garda Síochána. In order to ensure that we have the best possible capacity to deal with this, we disseminate cases out locally for investigation.

Deputy Anne Rabbitte: Does that take into account the 28 divisional units?

Mr. Declan Daly: That is a new initiative. We are engaged in training them to give the specific specialisation in this field as well. If a case comes in to us from the FBI, for example, we will do some work around it to process and target the individual involve and then we will disseminate that out to the local detectives for investigation. We co-ordinate that case. We hold that crime until it is concluded.

Deputy Anne Rabbitte: Would Mr. Daly have a backlog of work in the caseloads in that sphere at present?

Mr. Declan Daly: We do not have a specific backlog. When the cases come in, we have

certain work that we need to do. We have to engage with a service provider to gather information, possibly on the location of it. From the time it comes in through our front door to the time it leaves our office, there is a period in which we have to process and disseminate that information.

Deputy Anne Rabbitte: Going back to the 28 divisional units-----

Mr. Declan Daly: The divisional detective service units, yes.

Deputy Anne Rabbitte: -----can Mr. Daly elaborate on the role they play in the community?

Mr. Declan Daly: What we in An Garda Síochána are looking for is a consistent and high-level approach to the investigation of sexual crime, including online abuse. We sit at the national level in the Garda national protective services bureau and we have rolled out divisional protective services units which mirror what we do and would bring that specialisation and that level of consistency throughout the nation for the investigation of sexual crime. We want all the crimes investigated to a high standard and we believe the specialisation will achieve that.

Deputy Anne Rabbitte: Has the Garda enough personnel on the ground to deliver that? Theoretically it sounds good but are there personnel on the ground in these 28 divisional units to mirror the service that is going on in HQ?

Mr. John O'Driscoll: In terms of what is already in place, the victims' units are in place in all the Garda divisions. The protective services units are being introduced and are on a pilot basis. At the centre, I am in charge of all the national bureaus in the crime ordinary section, aside from the security aspect of the State. In recent months, and up to next Friday, we will have received 180 additional staff.

The modernisation and renewal programme resulted in the creation of these new bureaus. The bureau that Mr. Daly is attached to did not exist until 2015. We brought together units that existed elsewhere. For example, human trafficking rested in an emigration bureau because that is where the first cases came to light but, because the focus should be on victims, those kinds of unit were brought into one bureau. Therefore, within Mr. Daly's bureau there are all those victim-centred units. The protective services units are operating in four locations as of today - two pilots in Dublin, one in Cork and one in Louth. Approximately six more will be created next year and we will have them in every division throughout the country shortly after that. However, the victims units are in every division and operating now. Then within the centre there is those listed dedicated units. Those are the units that are receiving the additional staff over recent months.

Deputy Anne Rabbitte: Are these the units in Phoenix Park?

Mr. John O'Driscoll: No, these are in Harcourt Square. In the budget, provision was made for a sum in the region of €80 million to build a new headquarters for all of our national units. Those units based in Harcourt Square, which is where special crime operations is located, include the national bureau of criminal investigation, the national economic crime bureau, the national protective services bureau and the Criminal Assets Bureau. The Garda national drugs and organised crime bureau is in Dublin Castle. All of these developing bureaus will go to a new headquarters in approximately five years' time on a site which is being developed opposite Heuston Station where we will have state-of-the-art facilities. As I stated, in the capital end of the budget, provision was made for that project to go ahead.

Deputy Anne Rabbitte: In the presentation reference was made to various legislative measures. I am concerned that some of them seem dated. Do they allow the Garda to do its job? I refer particularly to the Child Trafficking and Pornography Acts 1998 to 2004 and the Non-Fatal Offences against the Person Act 1997.

Mr. John O'Driscoll: With regard to that aspect I had the head of the EC3, Mr. Steven Wilson, in my office the day before yesterday. He spoke to every member of the cybercrime bureau who was available on that day. I asked him how we measure up to other countries. The way the definitions in the legislation were framed is fairly robust. There are certain aspects of them - Mr. Daly will give one example - where we might need an adjustment due to certain developments in the type of criminality involved but the Acts, because of the way they were developed, have proved workable in many regards up to now. Clearly, there is the prospect that as matters develop we will need additional legislation, particularly in regard to our power to search where people perhaps have a device which we would look upon as a phone but which is now more or less a computer rather than merely a phone. Mr. Daly developed on that in a conversation we had recently about a possible improvement in legislation that we would seek in that regard.

Mr. Declan Daly: Our legislation is internationally recognised as strong. For example, our definition of child pornography covers texts and cartoon images depicting children. In other countries, the legislation only includes images. Our legislation, in terms of definitions, is strong. Clearly we, in An Garda Síochána, would always look - I suppose we would be greedy - for additional tools.

The following are some of the areas where we have been engaging with the Department of Justice and Equality in terms of new legislation on issues that we see may assist us in combatting online child abuse. With regard to search warrants, we would look for an amendment to the legislation that would allow us to obtain passwords of persons when we are conducting searches. Another would be the development of a production order that we could serve on a service provider and thereby recover information rather than going through a warrant. These are additional tools that would assist us. As the assistant commissioner states, a phone is no longer just a phone, it is a computer-enabled device. For those who have such a phone in public areas, our legislation is weak in terms of search. We would look for additional powers to maybe search without warrant so that we can cover that. Much of the material we are finding is not on a home computer, it is on a phone. We must seek to change the legislation and view a phone in terms of it also being a computer.

Deputy Anne Rabbitte: With Brexit and other issues that may arise, do the witnesses see challenges for their unit in looking at the protection of children in terms of trafficking, etc? Can they foresee or are they planning for any of the problems ahead with the coming of Brexit?

Mr. John O'Driscoll: We engage with many law enforcement authorities outside the EU, in particular the FBI, because many service providers are based in the US. We would often be notified by the FBI that there is a case that we might have an interest in. We work closely with third countries outside of the EU.

In terms of Brexit, we have examined many possibilities and areas where there may be difficulties in terms of our interaction with the UK in a different scenario. I suppose the operation of the European arrest warrant is probably the area of most concern there. It is an issue which has been discussed. I have looked at the outcome of discussions on it, for example, in the House of Lords, where that subject has been addressed. We are acutely aware that this may be an issue coming down the tracks but until we know the shape of the Brexit arrangement, it is difficult for

us to address the issues. In this area we are very much involved with countries outside the EU and that co-operation will continue. We co-operate through Interpol with the non-EU countries. The level of co-operation with the UK authorities will continue post-Brexit.

Deputy Anne Rabbitte: Last week, Dr. Geoffrey Shannon gave the committee an excellent report on this area. What is Mr. O'Driscoll's view on the establishment of a digital safety commissioner? Does the Garda regard its role as being the digital safety commissioner at this time?

Mr. John O'Driscoll: This area needs co-operation between all interested parties that have an input. If this creation improves the co-ordination, we will certainly play our part. I have been involved in many areas in the past, including human trafficking and prior to that drugs. As with many areas, often at an early stage of development we put too much effort into the policy end of it. When that went off somewhere else and other people were dealing with other aspects and leaving it to us to deal with the law enforcement, it was a better arrangement. It would be better to leave the enforcement and investigation to the Garda national protective services bureau and the examination of computer equipment to the Garda national cybercrime bureau.

Deputy Anne Rabbitte: Would the establishment of a digital strategy commissioner be a good idea?

Mr. John O'Driscoll: I can see positive aspects to that.

Deputy Tom Neville: I welcome the witnesses and thank them for their informative presentation. The education programmes they mentioned are quite good, particularly at secondary schools. Will there be an equivalent programme for primary schools? They indicated that new recruits will be trained in these areas in Templemore. What specific areas will be covered in that training? What are the top three challenges the Garda faces in this regard?

Mr. John O'Driscoll: Mr. Daly can respond on the educational aspect and our input into the training courses.

Mr. Declan Daly: The Deputy is correct that education is vital so that children are aware of the dangers. That is why we have worked so hard and put so much of our effort into that. We have given several lectures and talks. I recently gave one to prospective primary school teachers in St Patrick's College. It is difficult to go into classrooms because the children are very young. We are certainly very open to assisting any educational entity. We put a lot of work into sports clubs through Sport Ireland and the GAA in particular. We have given talks to a number of clubs so that their safeguarding officers are fully aware of the dangers on the Internet and that they can recognise cyberbullying and other offences.

The Deputy mentioned training in Templemore. Let me split that into two. As well as the academic training on legislation and procedures they get from Garda College staff, colleagues from my office attend to give practical guidance over a two-day period to all students and probationers. They also get practitioner training that gives them information that is grounded and current. As part of the roll-out of divisional protective services units in February 2018 we have modular training involving about seven or eight modules. The next module on that training is specifically designed for online child abuse. We will bring in our own experts. Dr. Shannon has agreed to assist us with that. We will have a mixture of our academic trainers, our practitioners and outside stakeholders to ensure we have a full and valued course. That is for the participants in the divisional protective service training.

The Deputy asked about the challenges. One of our big concerns relates to self-taken im-

ages. We work very closely with other NGOs, including the Irish Society for the Prevention of Cruelty to Children. We have had very close relationships with it in trying to combat that.

As the Internet is borderless, one of the challenges is gathering evidence from outside the jurisdiction. We have the mutual legal assistance treaty which helps us in that, but it can sometimes be very slow. Our interaction with other police forces is very important in gathering that information.

The third challenge probably relates to peer-to-peer information sharing. Those are the three challenges that jump to mind straightaway.

Mr. John O'Driscoll: The developments in technology and the capacity of our cybercrime bureau to interrogate modern technology is a challenge into the future. We can plug into entities such as the EC3 unit in Europol. In the course of my conversations with the head of that centre, Steven Wilson, in recent days, he offered us the use of particular equipment from that unit if needed. It is something that we do not have in this jurisdiction and, indeed, that the majority of countries do not have. Particularly where abuse of children is being conducted live in another jurisdiction, trying to get at the culprits is very difficult and can only be addressed through international co-operation.

Deputy Sean Sherlock: I thank the assistant commissioner and his colleagues for attending today. How many gardaí work in the Garda national protective services bureau?

Mr. Declan Daly: A total of 67.

Deputy Sean Sherlock: How many gardaí work in the online child exploitation unit?

Mr. Declan Daly: There are three sergeants.

Deputy Sean Sherlock: That is three people in total.

Mr. Declan Daly: No. There are three sergeants and seven detective gardaí.

Deputy Sean Sherlock: What is the total number, including civilians?

Mr. Declan Daly: Including civilians, it is 11.

Deputy Sean Sherlock: That brings it up to 78. How many people work in the Garda national cybercrime bureau?

Mr. Michael Gubbins: A total of 34 people work in the Garda national cybercrime bureau, of whom five are civilians. There is one superintendent, one inspector, six detective sergeants and 21 detective gardaí. I have two regional units. I have one member in New Ross and two members in Ballincollig.

Deputy Sean Sherlock: I ask Mr. Daly to repeat those numbers.

Mr. Michael Gubbins: In the Garda national cybercrime bureau, based in Harcourt Square, there are 34. We have a pilot unit in New Ross with one Garda member.

Deputy Sean Sherlock: I am trying to get a sense of the overall numbers. For the pilot programme in New Ross and Ballincollig, are they extrapolated from the numbers Mr. Gubbins has outlined?

Mr. Michael Gubbins: No, they are in addition.

Deputy Sean Sherlock: How many are in Ballincollig and New Ross?

Mr. Michael Gubbins: There are two in Ballincollig and one in New Ross.

Deputy Sean Sherlock: That is three.

Mr. John O'Driscoll: Civilianisation can make a very important input. We have a business case that is being considered at the moment arising from which we expect some people with expertise to be added in to that bureau from among those 500 civilians who have been promised.

Deputy Sean Sherlock: I want to speak to the issue of resourcing. The numbers are quite finite. Given the scale of the challenge it could be argued that the numbers are quite small. What is the business case being made for additional resources? Is such a business case being made?

Mr. John O'Driscoll: Aside from the resources the Deputy has heard about, in a scenario where an investigation takes place and organised crime is involved, all resources within my special crime operations section are made available. It might be the economic crime bureau that has huge resources added one day and lately, because of organised crime, people from national surveillance units and all aspects of the organisation can come together at short notice to supplement the organised crime bureau aside from its own staff. For example, many people have viewed online the incident that happened in Tallaght yesterday. The amount of armed personnel that could be gathered in that scenario in a very short time were certainly not confined to those available in Tallaght.

Deputy Sean Sherlock: I appreciate that point. I am trying to ascertain what the numeric strength is and I recognise that other resources are deployed as needed. Will Mr. O'Driscoll give me a perspective on how the relationship with Internet service providers, ISP, of Ireland works with regard to a notice and take-down procedure? The Hotline, as I understand it, will serve an ISP with a notice of removal or take-down. Mr. O'Driscoll referred to a blocking mechanism. Maybe this is a false analogy, but it is a bit like when I block somebody who is abusive to me on social media, such as Twitter of Facebook, it does not necessarily stop the activity. How is the activity investigated? It is one thing to block it, but how is it stopped and investigated? How do gardaí investigate, since their jurisdiction is the Republic of Ireland and the crime may be transnational? What is the nature of the investigation and how are crimes investigated subsequently? Is it merely a blocking mechanism or is it subsequently reported to other jurisdictions? For those instances that happen in Ireland, specifically, how many investigations are under way at present and how many cases are before the courts for this type of activity?

Mr. John O'Driscoll: I ask Mr. Daly to address that.

Mr. Declan Daly: The blocking works slightly differently. The blocking initiative operates from Interpol's "worst of" list. Interpol looks at websites and decides which are the worst of them. At any one time, there are a number of such websites. The companies that block them block their customers' access by DNS poisoning so customers cannot get to them. That is very advantageous to us. If one considers online paedophilia as a pyramid, for example, the users are at the wide end at the base. The blocking will take some of them out which frees us up to deal with the high-end users, including producers and distributors. We are very keen on that. Other users who may be drifting into child pornography immediately come to a stop page which says

that due to An Garda Síochána and the ISP, that user is now blocked. That may be enough to prevent a person from moving forward which is obviously a good thing.

Deputy Sean Sherlock: How many sites are hosted in Ireland?

Mr. Declan Daly: Very few. I cannot say they are totally absent but most of these sites are overseas. It is a very rare phenomenon.

Deputy Sean Sherlock: Can Mr. Daly say if it is in fives or tens?

Mr. Declan Daly: I cannot say that but I can come back with a figure. I do not know if we have any. The figure is very low. The vast majority of sites are overseas.

Deputy Sean Sherlock: How many cases come before the courts?

Mr. Declan Daly: I will have to come back to the Chairman. I do not have those statistics.

Deputy Sean Sherlock: The witnesses made a statement on the Communications (Retention of Data) Act. There is a specific section in their statement, "However, if internet providers fail to provide the Garda Síochána with data pursuant to the Communication (Retention of Data) Act 2011, our ability to identify people involved in the sexual exploitation of children or the distribution of child pornography on the internet will be restricted". Is there a lacuna in the law relating to this? Have there been incidences where ISPs have refused to yield information? I am trying to get a closer interpretation of that statement.

Mr. John O'Driscoll: The problem is that we might not know what ISPs could have prevented. That is the scenario that I would be talking about there. Mr. Daly might address whether there are or have been cases where we have later discovered information that they could have given us. He might have knowledge from investigations.

Mr. Declan Daly: Our relationship with ISPs is generally very positive. We look for a lot of information from them. I have to be very careful here because I do not want to give away any tradecraft about how we discuss these investigations. It is important that we do not educate other people. There are times when, for technical reasons, information may not be available to them and therefore they may not get it. In my experience, I have not come across any case where they wilfully refused to give information. They may not have it and may not be able to get easy access to it but I do not have any information to pass to the committee today which says that any single company has wilfully, deliberately failed to disclose information.

Deputy Sean Sherlock: We would all acknowledge that the work of the Internet Service Providers Association of Ireland and Hotline is laudable and proactive. There are mobile telephony and Internet service providers. The witnesses made a very pertinent point about how technology has moved on. A phone is no longer merely a phone but it is also a computer. Does the Communications (Retention of Data) Act as it relates to this subject matter pertain to mobile telephony too with regard to the retention of data?

Mr. John O'Driscoll: A problem is that much of the material is not retained on the phone but can be accessed in the cloud, so to speak. The legality of that and the question of who owns what is in the cloud is very technical. I am not equipped to answer it. Maybe Mr. Daly is, following investigations.

Deputy Sean Sherlock: My point, to be helpful, is that it would be very good to have a perspective in order for this committee to make determinations and recommendations.

Mr. Declan Daly: I have to be exceptionally careful so that I do not reveal tradecraft. The information we generally get from the service providers relates to IP data. That is probably the safest way to leave that.

Senator Máire Devine: I know there is a big emphasis on child pornography and grooming by adults. I am quite interested in the children's aspect of it, with regard to sexting and the exposure that children risk when they do that. The witnesses state that children do not really understand cybercrime and cyberbullying, especially if they are younger. There is a question of how to address that with children. The witnesses addressed borderless Internet. It is infinite so it will grow and grow. Education is the key word. We talked about education for those going into secondary schools and trying to manage the primary schools somehow. We need to train young people. We have not had young people in here to give their presentation. I have a presentation from Comhairle na nÓg which has created an excellent document about cyberbullying, and I will invite its members here at some stage. We need them to be at the heart of it. It would be helpful to train young people, perhaps secondary school children in transition year, and make them ambassadors. They could go into primary schools with age-appropriate information. It would empower them, get them recognition in their own school and also in primary schools. It would be helpful because access by children to it is increasing. It is an ever-growing issue. We need to include children and put them at the centre of it. They have great ideas and solutions. It will empower, give them a voice and allow them to be the mammies and daddies to younger children.

Another issue, which I have raised previously, is that we need to make much more use of the journal children get at school which has their classes, diaries and dates in and which parents sign off on. We could put something in. I have a cyberbullying chart drafted by Comhairle na nÓg. It is very simple. It is addressed to all young people reminding them that their digital behaviour can affect others and that they should treat others as they would like to be treated. It tells them to take responsibility for their actions on social media, that all actions have consequences and they should think about the potential impact of their actions and make good choices. We should consider something like that. It makes the children who will become our young teens and adults more aware. The difficulty I see is getting the information out there. We are aware of it but I am not sure how aware of it I would be if I was not on this committee. We should get the information out in the simplest way using material that is already there. We do not need to reinvent the wheel. We should get those messages out using the cheapest way with material people use every day. I want to emphasise that we should involve our children.

There are many aspects to staff resources which I have addressed. Pornography or grooming by adults is not the only concern. The difficulty comes in when it is child-to-child or young teenager-to-young teenager. Will the witnesses comment on that? How is it dealt with?

What are the witnesses' views on passports being withheld from convicted paedophiles? A priest is working on this issue and hopes to have it enacted. If it was to go ahead, I think we will be the first country in the world to do it. There are serious implications.

Mr. John O'Driscoll: It is Fr. Cullen.

Senator Máire Devine: Yes. Will the witnesses take my point on board about the involvement of our young people? They have great knowledge and resources.

Mr. John O'Driscoll: Having worked in the drugs area, I know one has to be very careful about going into schools. I have two people involved in primary schools at home in my own

house. How it is delivered to each age group is very important. We need to give the professionals and teachers the information and let them convert it into the best format for each age group, whether five year olds or 13 year olds. As they get older, we can become more involved. There is one initiative involving gap year students in secondary school which Mr. Declan Daly will talk to the committee about when I am finished speaking. It is important. We all know how important vetting is. Vetting applies to people who put their hands up and wish to get involved in this area. One has to be careful in case there is an ulterior motive. We have to be very careful when getting children involved in educating other children. There are all kinds of difficulties but we will explain the initiative to the Senator.

The Senator mentioned passports and the taking of passports from people who are suspects. Such people can be-----

Senator Máire Devine: Convicted.

Mr. John O'Driscoll: -----subject to bail conditions. In terms of convicted people it is an issue that could possibly be explored and it might be put in legislation in a more defined way. Restrictions on travel could potentially also be part of a sentence imposed. It is an area that could be advanced further. I appreciate how the priest who has raised the issue in the Philippines where he is working, sees what is happening and the impact it has on children when people are coming from the European Union and other countries.

I am not sure if I have left anything out but I will let Mr. Declan Daly speak to the committee about particular initiatives in that area.

Mr. Declan Daly: The Senator is correct. Children are very important and their views are very important. We can do what we can and we can give talks and lectures. I do not know how successful it would be if it was a group of children doing that. We are looking at an initiative with transition year students with the Irish Society for the Prevention of Cruelty to Children. We will empower them with the knowledge and as part of their transition year programme they will go back to their class and impart that information peer-to-peer. We are very supportive of that. A number of schools have indicated they will do the testing. It will take time to develop because we have to be sure we are getting the right message across and that there is permission from parents. It is something we are working on with the Irish Society for the Prevention of Cruelty to Children.

We are also very active with Webwise. It has a number of information streams on its website for different ages and for parents. That is also important. There are a number of other organisations. One does not have to be totally internet proficient to go and find them. One can get the information quite easily whether it is for a parent, a six year old or a teenager. It is all there.

The Senator mentioned child-to-child pornography and grooming. The Garda Síochána, when we are dealing with this crime type, is not here to criminalise children for taking images. It is for somebody who posts an image online. The role of An Garda Síochána is not to criminalise that child; it is to support the child. We introduced an initiative with Tusla about two years ago with regard to self-taken images. There is a co-ordinated approach. The committee can imagine the shock if a child posts an image online or sends a naked picture to somebody who the child believes is in America or some other jurisdiction and that he or she is sending it to that person in a closed environment and it is then on fire online. The committee can imagine the shock for that family and child when we go to that house. We have a co-ordinated approach with Tusla. An Garda Síochána deals with the criminal element to make sure there are no other

issues in the home. Tusla operates on the welfare side. It has been a very successful initiative to deal with that. It is very shocking for them.

On child-to-child pornography, the issue is education. We have had cases where images are circulated in schools. In many of the cases we have had like that, the schools have been excellent. They come in strong, which is very important. There is a message there. A child who holds a pornographic image of another child is committing an offence. Children need to be educated about that. There are problems there for that child especially if they distribute the photo.

Deputy Denise Mitchell: I apologise for my late attendance. I read the witnesses' presentation. I want to touch on apps such as Snapchat and WhatsApp. It seems that bullying can happen indirectly when there are private groups set up and people would be unaware it is happening. I want to talk about Snapchat in particular. If somebody uploaded a video or a photograph, it can be taken down. They are automatically deleted after a short period. For a victim, it is very difficult to supply the Garda with proof it has happened. How do we go about that? It is obviously very distressing for a person if threats are being made and they go to the Garda and do not physically have the proof to show. How do we overcome that? I welcome everything the witnesses have said about the initiatives they have in place. From a parent's perspective, if something is happening like that with my child and I go down to my local station, which is Coolock Garda station, and go up to the garda at the desk, what training does that garda have in this area? Is there anybody in that station who could talk to me about it? If we are going to do this, we have to see that it is taken seriously at a local level in our station. Will Mr. Daly address some of those issues?

Mr. John O'Driscoll: The creation of the local protective services unit is very important in that regard and will be manned by people who have the necessary training in this area. It will be at a local rather than national level. Currently, anyone who encounters a case of that nature at a local level has access to the national unit. We interact with and, if needs be, take over such investigations regularly, and we provide advice. Because of the extent to which it is growing and it is a new form of criminality, it requires new forms of policing. That is the motivation for our modernisation and renewal programme creating local units of that nature. We already have the victims units in place throughout the country. As Mr. Daly has noted, we must interact with other bodies, such as Tusla, which might be better placed and have the expertise needed to deal with people who have been victims of this particular type of crime. Mr. Daly might address the earlier issue.

Mr. Declan Daly: Deputy Mitchell mentioned the issue of the evidence having gone. Anyone who has been a victim of any kind of exploitative activity, even if they believe that the image may be gone, should report it. Mr. Gubbins is more of a specialist in this than me, but in every computer device a digital fingerprint is left. That is not to say we can find it in every case but the important thing is to report the incident. Anyone who thinks that the evidence is gone from their phone, that they or their parents may have deleted it, should still report it.

On training, as the assistant commissioner, Mr. O'Driscoll said, ours is a very specialised area. It is difficult to have every garda trained in something so specialised. That is one of the reasons why we have the divisional protective services units, so that in every division there are people who are specialists in the area, and in the future there will be local specialists there. Currently, the biggest role in our office is advising members. To use Deputy Mitchell's scenario, if one calls to a local garda station, the garda on duty might say that it is not his area but then he will ring us and we will give him the information or we might take over the investigation or have oversight of it depending on its seriousness. The important thing is for people to report.

The Europol Say No campaign is very clear, not only on this but on all sexual crime, and that is what we encourage.

Chairman: I have a number of questions that follow on from that point. I will not refer to a deficit in training because that infers wrong-doing or omission, but there might be a difference between the specialised service that the bureau provides to the individual garda on the street, in the car, at the front desk of the station. I am concerned that there could be circumstances where a child has been subject to online harassment, bullying or been subjected to or shared imagery that is beyond their years, where a garda might not be forthright in dealing with it by phoning the bureau. I do not have any specific examples of this but I am aware of instances, both personally and second-hand, where regrettably a crime is reported and there is a shrug of the shoulders with an attitude that what is being reported is minor. That concerns me and it is a legitimate concern regarding training considering the seriousness of this field in which the bureau operates.

I am satisfied to hear of the roll-out and the broadening of the unit. I have a question regarding training and another relating to the availability of professionals, non-sworn members of An Garda Síochána, who support the activities of sworn members. Are there professionals who are non-sworn members within the witnesses unit? Is there a proposal to bring them in?

The assistant commissioner will forgive me, his opening statement was quite lengthy, but I cannot recall if he referred to 140 units or locations in relation to broadening scale of the unit and the services it provides. Will he clarify the matter?

I will come back with some further questions.

Mr. John O'Driscoll: Training is undoubtedly a huge challenge. When people of our vintage joined An Garda Síochána, there was a law book which was a certain size where now one has tiers of books. While we are talking about the internet and cybercrime, much of the training can now be delivered in a different format. Apart from training, there is also access to others within the organisation through the garda portal. For instance, I was in charge of a unit in human trafficking where we put our documents on the portal and advised people as we trained them that there were documents on the specific types of trafficking cases. Similarly in this area, the portal has become a significant resource which is accessed by members daily. All the headquarters directives and training material can be made available there. The fact that the garda training college was closed for several years during the recession means that it is taking time to get through all the various types of training that must be developed and delivered to people within the organisation. We have a huge number of new recruits coming in, I think some 800 are promised next year, all of whom will get the up-to-date training.

On the civilian input, we have a Government undertaking that there will be 500 additional civilian staff next year. Special crime operations to which I am attached has already submitted its business case and is developing others. In relation to the cybercrime bureau there are already considerations regarding specific expertise and as I understand they are ready to go in the recruitment of personnel. Mr. Daly might be able to identify the types of areas in his unit where they have sought civilian input, in addition to which there will be direct civilian input through Tusla, with its staff in the bureau in the future.

Mr. Declan Daly: On training, our specialist training is international, from the FBI to Europol. All our staff are trained internationally, they go to Germany for ten days on a specialist training course. They are trained to a very high standard and pass it down. We also have a civil-

ian employee who tracks all our cases. We have sought to take all the administrative functions from detectives so that they are doing what they ought to be which is detecting crime, and using those civilian resources for administrative purposes and tracking not only our own investigations but all online investigations and we can be sure that nothing is falling through cracks, such as the examples which the Chairman gave. That resource has been in place since January 2017.

Chairman: I can give an example of a particular crime that might be committed. Take an individual, specifically a child, who requires particular medical or social care so Tusla would be involved in this instance. In Mr. Daly's experience, even since January 2017, has there ever been a scenario where a member of his division was not available to a garda attempting to support a child who has been the victim of online sexual exploitation or otherwise elsewhere in the country, primarily because the call-out happened in the middle of the night or something like that? In respect of his division's interaction with Tusla, has there been a scenario where it has been in contact with Tusla but has been unable to get the resources necessary to support a child or family who has been subjected to online abuse in a timely manner?

Mr. Declan Daly: We in the Garda national protective services bureau work very closely with Tusla. I would go as far as to say that never in the history of the State have we been so well partnered. We are discussing co-location. We already have within our unit a dedicated resource from Tusla. Again, that is really positive. Any advancement in that area is great. I cannot say that I have had experience of cases such as the Chairman has just outlined. In terms of the services which Tusla provides, we work closely with it and it provides its services. If it decides that it will not supply services, that is a matter for it. There are difficulties there but we have huge interaction with Tusla on cases.

The Children First guidelines talk about the level of interaction. In the new Children First guidelines for 2017, we have introduced additional engagements from the ground level, where the garda and the social worker engage, to where an inspector or sergeant engages with a team leader, right up to where a superintendent engages with a principal social worker. In addition, there is the more strategic element, which includes my role with the national management for Children First and the assistant commissioner's role as co-chair of the strategic liaison committee. We have built a very robust engagement pathway with Tusla, which is very important. In respect of those cases which occur in the middle of the night when our unit might not be working, it is not just about offences online. There are cases of contact offences. That happens. It happens in cases of domestic violence and in other areas. That is what our front-line troops and first responders are there for. They are there to hold that line and then pass the case to specialist units.

Chairman: I have one last very brief question. The Communication (Retention of Data) Act 2011 provides for a penalty should an Internet service provider, ISP, fail to hold onto information for evidentiary purposes. There is a fine associated with that Act. Has the unit experienced any difficulties with ISPs in respect of the retention of such information? If so, does Mr. Daly believe the fine is sufficiently large to warrant the ISPs retaining the information? The second question is irrelevant if the answer to the first is "No".

Mr. Declan Daly: The difficulty with the retention of data is the 12-month period. That is the real problem. It is too short. We get cases that are, essentially, already closed because we cannot get the information. That is really the whole problem with that legislation in a nutshell.

Chairman: That has clearly been identified in the past. I thank Mr. Daly. Did Deputy Rabbitte have a follow-up question?

Deputy Anne Rabbitte: It is a different question. It is particularly for Mr. Daly, or perhaps Mr. Gubbins. I will reference Snapchat, which two of the ladies spoke about earlier, and the likes of Sarahah which came along during the summer. That was a particularly worrying app for parents because, once it was downloaded, it allowed the user to be tracked anonymously on Snapchat and allowed people to post faceless comments about him or her. When an app like that becomes available, what is the role of An Garda Síochána in informing the public and making us aware? What is its role in telling parents that the app is red-flagged and not really suitable and in asking parents if their children are aware of it? How quickly does An Garda Síochána intervene?

Mr. Declan Daly: In the case of apps such as Snapchat's Snap Map and so on, awareness is very important. At the time it came out there was a flurry of activity and we were involved in education about it. Webwise has very good advice on the app on its website. We also gave advice on it on our own website. I do not know why children want to have all these friends. They want to have online friends. It is a problem for us. Children might have 1,000 friends but they do not know 1,000 people. They let their guard down online and, because their guard is down, potential offenders or paedophiles will enter that space to try to exploit them. The whole idea is to educate them that they should limit access to their friends. All those apps allow for certain controls. For Snapchat and Snap Map, an account can be closed off so that it is only visible to oneself and one's close friends. It also has a setting for more open visibility.

Really it is a matter of education for parents. When they are downloading the app and having that conversation with their child, they should be giving that education. For example, it now seems to be common for children to get a phone around the time of their confirmation. I wonder how many of the phones given out during the confirmation period come with a discussion or advice from the parent or somebody else. We would certainly advise that. No child should get a phone without accompanying advice. The parent does not have to have a huge knowledge of the Internet. Our parents have always told us that we should not talk to strangers and that applies online as well. If one takes the scenario of parents in their living room looking outside and seeing their child talking to a stranger, they would challenge the person or talk to the child. It is exactly the same online. The message is do not talk to strangers.

Deputy Anne Rabbitte: I thank Mr. Daly.

Chairman: I thank our witnesses for coming in and giving us their time. We are running a little bit behind schedule so I propose that we go into private session for a moment in order to change witnesses.

Sitting suspended at 11.07 a.m. and resumed at 11.12 a.m.

Chairman: I welcome representatives from the Office for Internet Safety and CyberSafeIreland. Specifically, I welcome Ms Siobhán McCabe, assistant principal officer, and Ms Eileen Leahy, principal officer, and from CyberSafeIreland, Ms Alex Cooney, chief executive officer, Ms Cliona Curley, programme director, and Dr. Maggie Brennan, scientific adviser. They are all very welcome.

Before we commence, in accordance with procedure, I am required to draw the witnesses' attention to the fact that by virtue of section 17(2)(*l*) of the Defamation Act 2009, they are protected by absolute privilege in respect of their evidence to the committee. However, if they are directed by the committee to cease giving evidence on a particular matter and they continue to do so, they are entitled thereafter only to a qualified privilege in respect of their evidence. They

are directed that only evidence connected with the subject matter of these proceedings is to be given and they are asked to respect the parliamentary practice to the effect that, where possible, they should not criticise or make charges against any person or entity by name or in such a way as to make him, her or it identifiable.

Members are reminded of the long-standing parliamentary practice to the effect that they should not comment on, criticise or make charges against a person outside the House or an official either by name or in such a way as to make him or her identifiable.

I ask our guests to switch off their mobile phones as they have a tendency to interfere with our broadcast systems, including our webcast and sound quality. I advise the witnesses that any submission or opening statement they have made or will make to the committee will be published on the committee website after this meeting. I understand our witnesses have prepared opening statements. In the interest of time, I ask them to keep their presentations to within five minutes. I call Ms Leahy of the Office of Internet Safety to make her opening statement. She will be followed by our guests from CyberSafeIreland.

Ms Eileen Leahy: I thank the Chairman and members for the invitation to discuss child Internet safety. I shall first set out the functions of the Office for Internet Safety and our role in this area, including progress the office has made since its establishment.

The office was established in 2008 on foot of a Government decision as an executive office, that is, on an administrative basis, within the Department of Justice. Following its establishment, its operational focus has been in the following four areas: awareness-raising and information activities; co-ordinating the EU safer Internet programme for Ireland with four partner bodies; oversight of takedown procedures for child sexual abuse material, CSAM; and developing strategic actions to promote the highest possible levels of Internet safety, particularly in respect of combating CSAM.

To expand on each of these a little, we seek to promote awareness of Internet safety and to highlight its importance for parents, children and all young people. We try to encourage appropriate conduct on the Internet, not only by raising awareness about preventative actions but also by giving advice on how to respond when individuals are affected by misuse. In this regard the office publishes a series of booklets on Internet safety particularly aimed at providing guidance to parents on filtering, social networking and cyberbullying. These booklets are very popular with schools and parents, and in 2016 we issued more than 40,000 of them. They are also available via our dedicated website, *internetsafety.ie*, which publishes information for parents and guardians together with links to many other useful sites, in particular to our four partner bodies and the helplines associated with them. In addition, we liaise with the Garda schools programme in the supply of awareness-raising materials for their visits to schools, including materials for the EU-wide Safer Internet Day held in February of each year.

Regarding our role in EU safer Internet project funding in Ireland, we partner with four organisations, and we very much work on a partnership model with them - the National Parents Council Primary, the Irish Society for the Prevention of Cruelty to Children, ISPCC, the Professional Development Service for Teachers, PDST, which I think has otherwise been referred to as Webwise, and *hotline.ie* - in channelling funding to initiatives in the area of child safety. These bodies focus, respectively, on helping parents, providing a helpline for children, specifically through the Childline service, raising awareness on Internet safety in schools, and the provision of a reporting service for illegal content. Funding for Internet safety comes under the connecting Europe facility budget envelope and attracts grant funding at a rate of 50% with

matched funding from each of the relevant project partners. We are now in the sixth round of this EU funding programme. To date Ireland has received approximately €3.4 million in funding. However, it must be noted that the European Commission has indicated that it is not in favour of extending this funding beyond 2019.

A key area of our work relates to the *hotline.ie* reporting system and takedown procedures. This reactive facility is operated on a voluntary reporting basis by the Internet Service Providers Association of Ireland. The activity can vary but, for the most part, it relates to CSAM, which is otherwise referred to as child pornography. The *hotline.ie* service notifies the Internet service provider which then removes the material. This is what is referred to as the notice and takedown procedure. In parallel, *hotline.ie* also notifies An Garda Síochána which investigates sites hosted in Ireland or links with the appropriate authorities in the relevant jurisdiction. As an additional measure, An Garda Síochána signed a memorandum of understanding in November 2014 with one company, under which the company agreed to block child sexual abuse material, CSAM, as per a list supplied by it. The Garda continues to engage with other companies with a view to establishing further such arrangements and it works with police forces internationally to seek out such activity continually, and with some very welcome success.

In terms of strategic actions, the office is guided by the Internet safety advisory committee, which is chaired by an industry expert and comprises representatives from An Garda Síochána, the Office of the Data Protection Commissioner, academia, industry and the four partner bodies that I have already referenced. Its terms of reference include advising on all aspects of Internet safety and acting as the national stakeholder forum, as required under the EU funding commitments. The committee meets twice yearly.

I hope I have given sufficient information to help the committee understand our role. My colleague, Ms McCabe, and I are happy to address any questions or comments members of the committee may have.

Ms Alex Cooney: I thank the Chairman for the invitation to address the committee today. We recognise that the Internet is a powerful and ubiquitous resource in Ireland today. It plays a hugely important role in all of our lives and can provide a beneficial educational resource for children. While the Internet brings us opportunities that we could not have imagined 20 years ago, it also brings risks, particularly for children. The Internet was not designed with children in mind. It is not always a safe and secure environment for them to be in. Social media apps and games are designed to encourage their users to use them compulsively and to share personal information extensively. These are environments that many adults struggle to understand and manage effectively, never mind their children.

As children access the Internet from an increasingly young age - seven years in Ireland - we are seeing more problematic incidents arising from its use at home, at school and in the press. Children are spending many unsupervised hours online. Our latest survey of 650 children found that 16% were online for more than four hours a day. Children are sharing too much personal data. Many children we spoke to admit to not using privacy settings. Some 12% of the children we spoke to had featured in a YouTube video, despite that being a particularly public platform. In one class alone, we found that 17 of the nine to ten year olds had featured in videos.

The health and well-being of children is being adversely impacted through their overdependence on social media for social and emotional support, with verified adverse consequences for their self-esteem and wider mental health. Cyberbullying is a growing problem in schools across Ireland and is often the reason we are called into a school in the first place. Children are

being exposed to inappropriate and harmful content. A 2017 report by the NSPCC in the UK found that 28% of children aged 11 to 12 years had looked at pornography online. Of great concern in the context of the report is that over half of the 11 to 16 year old boys surveyed found what they had seen to be realistic.

We are also concerned about the sexual abuse and exploitation of children online. We are aware of several cases that have come to the attention of Irish and international law enforcement, each involving hundreds of victims of sexual extortion and grooming. We are equally concerned about problems of self-generation of sexual imagery by children at increasingly young ages and with the associated problems of peer-on-peer abuse that can result from this behaviour.

What can we do to solve the problem in Ireland? We need Government leadership. Two weeks ago, the UK Government introduced its Green Paper on Internet safety for consultation. This paper's stated intention was to make the UK the safest place to be a child online. While we can debate the value of the range of measures it proposes, there can be no doubt that the UK is much further along in its discussion on how to keep children safe online. We need to be having these kinds of conversations in Ireland, led by our Government. At the moment it is difficult to know where responsibility for children's online safety and well-being sits. Is it with the Department of Education and Skills, the Department of Communications, Climate Action and Environment, the Department of Justice and Equality, the Department of Health, or the Department of Children and Youth Affairs? Should it sit with a separate body comprising cross-departmental representation?

We need prevention. We strongly believe that the most effective response is prevention through education. We must equip our young Internet users with the skills and knowledge that they need to navigate the online world safely, responsibly and in ways that are respectful of others. This provision cannot be offered unsystematically, as it is now, to those children who are lucky enough to live in a location where an online safety expert is available. This provision must be made available to all children in every corner of the country, wherever a child may be online. Digital literacy that encompasses online safety education will need to become the fourth pillar of our education system, alongside reading, writing and arithmetic.

We need awareness. We must ensure that parents are engaged in their children's online lives. Too often, parents tell us that they feel overwhelmed or challenged or that they simply do not know where to start. "My child knows more than I do", is a common refrain on feedback forms. We need parents to understand the risks and to address those risks at home in an ongoing fashion. We need a national awareness campaign targeting parents that creates social norms around online safety, much in the way that we have had over the years with road safety and healthy eating campaigns. We must get to a place where no parent can say, "I did not know any better."

We need to respond effectively. Even with the best will in the world, things will still go wrong. Children's photos and videos will be shared without consent and some will go viral. Inappropriate contact will be made with children and bullying will happen. We have a duty of care to ensure that, when children are harmed online, the child at the centre of it all is protected and supported in the best way possible. The best way we can do that is by ensuring that the response is timely and appropriate and that the helpline to which the child or parent reaches out is equipped to offer sound advice, support and resources; that the teacher, social worker or garda dealing with the issue has the skills and knowledge he or she needs to work sensitively with parents and children to safeguard the child effectively and minimise harm and anxiety; and that

the social media platforms and telecoms companies are highly responsive to children's needs and that the takedown rate, where needed, is fast.

There is no way that any one organisation can solve the issue of online safety for children in isolation. CyberSafeIreland, as the Irish children's charity for online safety, is willing and ready to lend its expertise where it can add value, but ultimately we must work together to deliver solutions. The Government must lead the way in tackling this issue by showing clear leadership, by creating a national strategy and a task force on online safety for children, and by appointing a digital safety commissioner and resourcing his or her office appropriately.

We must invest in education. We must ensure that every child benefits from a good education on online safety, digital rights, citizenship and well-being and that, when things go wrong, the child at the centre will be effectively protected. We need to be doing so much more to respond comprehensively to this issue. Problems of online safety are becoming increasingly urgent for children and parents around the country. They have the potential to impact on the future of every online child in Ireland.

We are encouraged that the Joint Committee on Children and Youth Affairs has invited us and others to speak on these issues. We hope that this interest will translate in time into greater leadership on and investment in keeping all of our children safe online.

I thank the committee for the opportunity to speak today. We look forward to the members' questions.

Chairman: I thank the witnesses for their contributions. At the last committee meeting, we agreed in private to write to the Taoiseach to inquire as to that jurisdiction and ownership to which the witness referred. It is an important point. The letter was sent this morning or yesterday. It will most likely warrant a response within a few days and I hope to be able to bring it back to the members thereafter. We will see what sort of response we receive in terms of the appointment of the commissioner.

I call Deputy Anne Rabbitte.

Deputy Anne Rabbitte: I thank both groups for their presentations. I will start as I started with the representatives from An Garda Síochána earlier by asking the Office for Internet Safety how many people work in the office.

Ms Eileen Leahy: There are two members of staff.

Deputy Anne Rabbitte: How many are involved in CyberSafeIreland?

Ms Alex Cooney: We are three founders. Two work day to day on it. Dr. Maggie Brennan is our scientific adviser.

Ms Cliona Curley: We also have three trainers, volunteers and a board.

Deputy Anne Rabbitte: How many volunteers are involved?

Ms Cliona Curley: There are some who help us on an *ad hoc* basis with particular marketing campaigns or things like that. We have two who are currently helping us with research.

Deputy Anne Rabbitte: Does the Office for Internet Safety believe the current takedown procedures are sufficient?

Ms Eileen Leahy: It is something that has been developed during the period of our engagement with the partner bodies. It is working effectively as a reactive measure through the ISPAI.

Deputy Anne Rabbitte: When Ms Leahy talks about the partner bodies, is she talking about the four groups she works with or various Departments?

Ms Eileen Leahy: I am talking about the four specific groups we work with under the EU safer Internet programme.

Deputy Anne Rabbitte: From reading the presentation, I have a concern that funding will cease in 2019. What alternatives will be put in place? Have budget requests gone in? How will we keep the office open?

Ms Eileen Leahy: The EU has worked from a model of helping member states to build on this area. Initially it was at a funding level of approximately 70%, which then dropped to 50%. The EU wants it to become a sustainable model with countries funding it themselves. The Green Paper published in the UK looks at a levy on the service providers. That is one model. While the EU has flagged that, it equally recognises it cannot completely pull the plug without something being there to continue the work. Nobody wants there to be a complete drop in this because it has to be around. The focus is on awareness and education as a key part of it.

Deputy Anne Rabbitte: I compliment Ms Leahy. I received one of the 40,000 booklets that were produced. They were brilliant. I rang in to get more of them but I could not. That is not a fault or anything like that.

Ms Eileen Leahy: I will make a note of it.

Deputy Anne Rabbitte: The quality and presentation was fantastic. They were of a very high standard. There should be one for everyone in the audience, including kids in schools. They were fantastic. I do not know if 40,000 hit the mark of everyone in the audience, but as a parent with three kids in that age bracket, I thought the quality and content ticked all the boxes for a parent and child. I compliment the work done on it. I would love to see it rolled out to more people. Funding is an issue.

Ms Eileen Leahy: They are the hard copies that issued. They are also all available on the website so people could have accessed them that way.

Deputy Anne Rabbitte: That is a fair point. What is the office's opinion on the proposed office of a digital safety commissioner? I have asked everybody who came in last week and this week the same question about the digital safety commissioner. What is Ms Leahy's view on it? Where does she see the role fitting in?

Ms Eileen Leahy: The recommendation on the digital safety commissioner follows from a number of reports in this area. There was a report by the Oireachtas Committee on Transport and Communications in 2013. Then, under the Department of Communications, Climate Action and Environment, which had a different name at the time, the Internet Content Governance Advisory Group, ICGAG, report made a number of recommendations. The Law Reform Commission has quite a substantial report from September 2016. There are a number of common themes in all of those reports and, based on our experience, we largely concur with them. There is a need for more awareness-raising and more targeted formal education programmes. We are told this through our partner bodies as well. An integrated oversight office on a statutory basis would be important. The Office for Internet Safety is within the Department of Justice and

Equality. It was a good start. The Department will always retain that focus on the criminal law aspect and will develop it and take advice from An Garda Síochána and the other players in the judicial system in terms of what needs to come forward. The two staff do not have an investigative role; their role is not in that sphere. We are very much dependent on the partnership we have with other bodies. The regulated takedown system and the criminal element of it would probably remain with the Department of Justice and Equality.

The strengthened advisory group is something that has come through in all the reports. We have an advisory group which works but all the reports recommend it should be much broader and that it should include a youth voice and more industry partners. The UK strategy and Green Paper is very much along the same lines. What the UK has currently is much broader than what we have. That is something that comes across. We also need the development of a national strategy that encompasses all of that. As CyberSafeIreland acknowledged, which Department one goes to is an issue. We are all involved in it. It is a whole-of-Government issue.

Deputy Anne Rabbitte: A whole-of-Government issue dealt with by two staff.

Ms Eileen Leahy: I suppose its future has to be thought out.

Deputy Anne Rabbitte: If we are to look at it at this time, it is a whole-of-Government approach across many Departments with two staff dealing with it. I give credit to what the office is doing but we are asking an awful lot of two people. There are huge expectations on the wider public.

Ms Eileen Leahy: Following from the Law Reform Commission report, the Government gave approval to the drafting of a Bill on the justice side for some of the specific offences. It also gave approval for a digital safety commissioner of Ireland to be established and for the proposal to be referred to the Cabinet committee on social policy and public service reform because it requires a whole-of-Government response. That was in December 2016.

Deputy Anne Rabbitte: I have one last question for Ms Leahy. I am just going through my notes here. Earlier when we had representatives from An Garda Síochána, I asked whether they believed the legislation was strong enough for them to do their job. One of the representatives said the legislation is good but we need to incorporate wording on mobile phones. Is the Department working on that? Who is working on it?

Ms Eileen Leahy: The people in the Department of Communications, Climate Action and Environment are the people with a direct connection to the mobile phone network. The Department of Justice and Equality works closely with the Garda in terms of any criminal law that needs to be developed.

Deputy Anne Rabbitte: Is that being developed at this time?

Ms Eileen Leahy: Yes. They are working through the LRC recommendations on those offences.

Deputy Anne Rabbitte: I thank the witnesses. I will move on to the representatives from CyberSafeIreland. I have listened to them a number of times on the radio. I love the work they do and how they present it. As a parent, the information is fantastic. It is like a red light every time because it brings home to roost what one is doing, as a parent, if one gives a mobile phone to a child or lets a child access one's own mobile phone. The message is very strong. I would like to hear a little bit more about the Green Paper in the UK. It was referenced in the presenta-

tion. CyberSafeIreland believes if we want to make children safe online, we should be going down this route. What points did the witnesses pick out from this Green Paper as an ideology we should focus on?

Ms Alex Cooney: Its stated intent to ensure the UK is the safest place for a child to be online is an important one. Dr. Maggie Brennan will go into the range of measures more but what we liked is that the UK is talking about making social media companies more accountable. It is a voluntary code of good conduct. There are questions about how effective it will be. There is also talk about expanding the curriculum and the content of the curriculum so the subject is covered more effectively in schools, which we think is good. There are some good measures proposed.

Dr. Maggie Brennan: One of the proposals in the Green Paper is that the sex and relationships education provision in the UK curriculum be extended in order that relationships and sexual education courses are provided in every school in the UK. One of the proposals in the Green Paper is that this would encompass awareness-raising and education specifically around how to conduct sexual relationships and other forms of relationships in the online space. It is a neat proposal and we would welcome it. It is very sensible in the context of what happens when one goes into schools and talks to children about the kinds of problems they are facing, the sorts of issues that arise around self-generation of sexual images, and what happens for children when they lose control of those images. There is a whole series of new educational messages to be relayed to children around consent and what it means to share a sexual image as opposed to consent to a sexual act, because that is a permanent record of the act and there is potential for exploitation and abuse. There is also a whole series of new messages to be delivered to children around boundaries, what it means to establish a relationship boundary in the online space and how to respect another person's privacy. While we welcome the suggestion that sex and relationships education within schools would begin to encompass those online issues, which are distinct from the ones that existed previously, we would like to see better specification of what would be provided for in the curriculum, and the Green Paper was scant on that.

Deputy Anne Rabbitte: I have another question for Dr .Brennan. She also mentioned the Road Safety Authority, RSA, and health promotion campaigns. I think there is a need for a particular campaign. There is no point in hearing about it when Snapchat maps or Siri comes out. I think I heard Ms Curley talk about it on the radio recently. There is no point in hearing about it whenever a particular app becomes available. We need to have awareness all of the time because children have access to those portals all of the time. Who do the witnesses envisage as being charged with this particular campaign? Whose remit should it come under and how would the campaign be devised?

Ms Alex Cooney: One of the plans we have is to try to initiate a national awareness campaign targeting parents, as we referenced in our presentation, something along the lines of healthy eating or road safety where we instil in parents the basic information around keeping their children safe online. One of the things we try to do with parents is demystify it and explain that one does not need to be a technical genius to address this at home. One needs to take some simple steps and engage with one's child. Having regular conversations is really important.

We are planning to start that campaign but we would like to work in partnership with bodies that will allow us to reach a much wider audience. It could come under the Department of Education and Skills or the Department of Communications, Climate Action and Environment. I do not know where the responsibility should lie at Government level, possibly with Tusla, but it needs to reach every parent, it needs to be a really simple message and it needs to be resourced

in order that parents can easily find out more information if they want. At the moment we find that the parents who come to our sessions are the ones who are already worried, so in a way they are not really the key parents we are trying to get to, the ones who do not have that awareness, whose children are online and who are not engaged or are not concerned about it. It is really important that there is a joined-up approach.

Deputy Anne Rabbitte: I agree.

Deputy Tom Neville: I thank the witnesses for coming in today. The representative of CyberSafeIreland suggested a task force for online safety should be established. Would that be separate from the proposed digital commissioner and, if so, who would be best placed to be a member of a task force?

The CSO age bracket for monitoring Internet usage is from 16 to 29 years of age whereas the EUROSTAT, statistical office of the EU, age bracket for Internet usage where children are concerned is 15 years or under. Do the witnesses feel there are sufficient data on the topic discussed today with regard to children and young people given the discrepancy in age brackets?

Ms Eileen Leahy: I might ask my colleague Ms McCabe to respond as she has been involved with Professor Brian O'Neill on a number of the research projects he has initiated at EU level in this area.

Ms Siobhán McCabe: The particular pieces of research are Net Children Go Mobile and Risks and Safety for Children on the Internet: The Ireland Report. The latter covers children from nine years of age to 16. There is Irish research contained in it as well as comparisons with the broader EU, so that is a very useful set of data which will hopefully be built on over time in order that we have comprehensive evidence on which to base our actions. I can supply copies of that report if that is useful for members. There is a lot in it. There is a synopsis version as well as a longer version.

Dr. Maggie Brennan: I will start with the question on research and the availability of statistical information. A concern is that if we are to begin to establish task forces and to develop policy that is appropriate for the needs of Irish children in relation to online safety, the required information should be there to inform that policy. I am a great believer in evidence-driven policy. A risk in this space is that we do not want to be led only by the examples of good practice that exist and are available from other countries because there are very specific needs and trends that present for Irish children in terms of their online use and digital behaviours that need to be addressed in a case-specific fashion.

I believe a lot of the work that has been advanced by Professor Brian O'Neill, who sits on our board, has been done with the support of the European Commission under the aegis of broader programmes such as EU Kids Online that was spearheaded by Professor Sonia Livingstone and currently the Better Internet for Kids initiative, which again is a European Commission-funded initiative. The kinds of information such reports provide and the reports we do based on our own research are important. It is broad and sweeping and gives us a sense of the scale of the use and the kind of apps and services they are using and the associated risks, for example. What it does not tell us, however, and which is a permanent gap in terms of most of the research evidence in this space, is what children themselves need. One of the things that makes our own research stand apart is that we are very concerned to listen to what children are telling us rather than just surveying them and seeing how many nine to 16 year olds are using WhatsApp or any other messaging service. That does not give us very useful information from

a targeting perspective in terms of targeting messages and speaking to and responding to the issues that are being faced by children. In terms of the sufficiency of the research evidence in the Irish space, it is great that we have the statistical information that is available to us, but I have a concern that it does not dip low enough in terms of the lower age bracket at which children are starting to use the Internet. We know that children are online at a much younger age than, for example, nine years. We need to know more about their experiences, what it is to grow up as an Internet user in Ireland and to bring the child's voice to this debate as well.

In terms of the task force, who should sit on it and where it might sit in relation to the office of a digital safety commissioner, that is an open question. I worked in the UK for a number of years for the National Crime Agency's child exploitation and online protection command in a research and policy role, and at that time the Home Office established a task force for child protection on the Internet, which is now the UK Council for Child Internet Safety. That sat within and across the justice and home affairs area at the time but it has now expanded beyond that, in particular with the increasing issues around children's Internet usage. It is not so much a criminal problem anymore. It still is a criminal problem in terms of the kinds of imagery that are being generated, but it is also a social problem that extends into all sorts of issues relating to education, in particular in the prevention space.

Regarding who would sit on the task force, many of the stakeholders have already been named, such as the telecommunications industry, representatives of academia and representatives from the charitable sector, which is particularly the case in Ireland because so many of our preventative responses rely on that third sector at present. Obviously, there would be representation from the appropriate Departments. I believe a cross-departmental body would be preferable. The role in respect of the commissioner would have to be advisory. There would have to be some independent advisory body that is advising the commissioner rather than sitting within the office of the commissioner. There must be independence because the issues I am discussing are complex, social, nuanced and dynamic. They change and therefore the relative roles of the stakeholders in this task force will change over time.

Ms Cliona Curley: Collaboration is key. We can make sweeping statements that the Government and technology companies must do more, but unless we collaborate and get together the people who are talking to children, the people who are running the technology companies and the people who are trying to lead in the Government, it will be very difficult to come up with practical solutions that will work.

Dr. Brennan mentioned including a child's voice in all of this. That is critical. As an Internet safety charity, we know what our key messages are to children and parents, but if we were not talking to children all the time, we would not understand why their behaviour is not changing on hearing these key messages at the level they are currently getting them. For example, one of the messages we give to children is that they should not share their passwords. They will nod and say they will not share them. However, when they are asked how many of them have shared a password, many will put up their hands. Unless we ask them why, we will not understand why they share their password. It will be for something such as all of them being on Snapchat. There is a feature in Snapchat where a person can be on a Snapstreak and the children are regularly into this. If I snap Deputy Rabbitte every day, we can keep a Snapstreak going, and the higher it gets, the more kudos I get. Children love this and they are all over it. As a result, if they are going on holidays or their device is not available to them, they will share a password. Unless we all have that understanding, it is very hard to ensure that the key messages get across to them.

Ms Alex Cooney: To add to that, we are rolling out a behaviour change assessment. We want to measure the extent to which children are understanding and applying what they have learned in the session. We have to understand whether our materials are being effective. We keep our group sizes small in order that the session is engaging and there is a great deal of discussion. It is thematic and tailored towards their needs. However, we must ensure that it is resonating and changing the way they use the Internet. We are rolling that out now.

Deputy Sean Sherlock: I thank the witnesses for attending the meeting today. This is an insightful discussion and it builds a deeper understanding for members of the committee. I wish to get a sense of the nature of the collaboration. There is the ISPAI, the Garda, CyberSafeIreland, the Office for Internet Safety and so forth. There are myriad organisations. What level of collaboration takes place? There are a finite number of actors in the field but what level of real collaboration is there at present? Perhaps the representatives of CyberSafeIreland will respond to that first. Do the witnesses have a genuine critique of the system as it exists?

Ms Alex Cooney: We believe there is no joined-up approach. It would greatly facilitate a response if key stakeholders were regularly talking, looking at solutions, bringing different expertise to the table and using that expertise effectively. Certainly, we talk to one another and we try to reach out to others. There are efforts but everyone is busy and under-resourced, which is a key factor. However, we must have a far more joined-up approach.

Ms Eileen Leahy: The Internet safety advisory committee in the format it has had up to now has included the various representative bodies. The number grows over time, but there has not been a mechanism up to now to expand it. Perhaps what is being touched on in the reviews of the area is how to broaden that. Webwise, as a partner with us and one of our advisers, has a youth panel, but there is no youth representation on the committee.

Deputy Sean Sherlock: I am glad the witness mentioned Webwise because I intended to ask about the office's relationship with same. The witness speaks a great deal about education and continuing professional development, CPD, in schools for teachers. There is a conflict in my mind around this. I am a parent. Is there an onus on the parent to have the primary responsibility in respect of educating his or her child about Internet safety? To say that I have mental blockages about using the technology and so forth is not really sufficient in this day and age. A parent teaches his or her child the safe cross code, road safety and all sorts of other safety mechanisms. I have a perception, and the witnesses can correct me if I am wrong, that sometimes parents will say that it is the role of the school through the Professional Development Service for Teachers, PDST, Webwise and so forth to educate their children on Internet safety. Webwise does not necessarily reach every school and not every teacher has taken up the CPD. Representatives of Webwise have appeared before the committee. If the CPD is not inculcated within the teaching and academic institutions as a core subject, it is likely that there will be a great deal of slippage in this regard. What is the witnesses' perspective on that? I believe every teacher should be equipped compulsorily, but how do we marry the role of the teacher with the role of the parent? I am sorry if I am a little long-winded but the witnesses understand what I am saying.

Ms Cliona Curley: There are two issues here: the role of parents and whether they feel equipped to take on this issue and the role of teachers. I talk to parents all the time, but as Ms Cooney said, the parents who come to our talks are not necessarily the parents we most needs to reach. We find there is a lack of confidence. Parents are really struggling and do not know where to start. It is so tempting just to wish the Internet away and to wish one did not have this problem in parenting because it is a huge challenge. The reality is that they must deal with it,

and they must be equipped to do so. Parents need more support and they need to have confidence. They do not have to be technical experts but they must have the confidence to take on their primary role of safeguarding their children and empowering them to use technology in a healthy way. They must be comfortable enough to have the conversations, set the rules and monitor what their children are doing.

Deputy Sean Sherlock: There is a role for schools. The school is probably the primary institution with which parents will interact in respect of their children up to the age of 18 years. We are talking about distilling this down and creating a platform nationally whereby parents voluntarily interact with schools and the programmes are delivered through that. Parents go to parent-teacher meetings. There is no reason that on one night per year there could not be outreach programme, for example, for every school in the country. It would only require two or three hours. Parents would interact with each other thereafter and natural collaborations would begin to build up through parents interacting with each other. If it were to be distilled down to community level, it would not take a massive amount of resources or money to do that.

Ms Cliona Curley: Obviously the school is the focus point for education. If we were to take a community approach like that, which we would support, the school is the natural central point for that. There is material available. There are some excellent Professional Development Services for Teachers, PDST, and Webwise materials. Many teachers whom I meet do not know about these., yet no parents I meet know about them. Perhaps the materials are not available but it is also the case that many teachers are not using them because they do not have the level of confidence, not necessarily to teach them but to have the conversations with the children which will arise. They do not know about Snapchat. They do not know about the apps the children are using. They are terrified of the questions. They do not even want to go there. Some would describe themselves as quite tech savvy and they are interested and motivated, but they are just not using the same technology as the children. That is what we really need to address. How do we find a way to do so? We have looked at this issue over the past couple of years and we have recommendations on how this could be done. It is probably unrealistic to expect every teacher out there not only to be tech savvy enough or to have the confidence to be able to address this issue, but also to spend the time to develop a level of expertise which allows them to advise a principal on issues that are coming up, to be able to talk to parents about it and to deliver talks to parents. We have a different idea which Ms Cooney will speak about.

Ms Alex Cooney: To emphasise the point Ms Curley was making, in our survey over the last academic year we found that 69% of teachers we spoke to did not feel equipped to teach online safety in the classroom.

Ms Cliona Curley: That is an increase.

Ms Alex Cooney: That is a significant increase on the previous year, when the figure was 64%. The sample size of teachers was much bigger this year. Materials may be available but if teachers do not feel equipped to teach them there is a gap. We need to upskill our teachers. So-----

Deputy Sean Sherlock: I hope Ms Cooney will forgive me for cutting across her but time is limited. The one thing I have noted is that teachers need access to materials. Ms Cooney is, in effect, saying that it is not only about access to materials but about the confidence to be able to-----

Ms Alex Cooney: To deliver them.

Deputy Sean Sherlock: -----have the pedagogical skills and understand the content in order to deliver it. That is certainly an issue which this committee could take forward. I am very conscious that the Chairman has to progress the agenda. I want to speak very specifically about the research component of this issue. These are straightforward questions. Are funding lines available through the Irish Research Council for the area the witnesses have spoken about?

Dr. Maggie Brennan: There are none that I am aware of.

Deputy Sean Sherlock: There is no bespoke funding line. Are there any funding lines from industry? For instance, is there any funding from the bodies represented by the Internet Service Providers Association of Ireland, which is a global body, or from any of the top global Internet-based companies, nine out of the top 10 of which have facilities in Ireland? Has Dr. Brennan, or anyone from the academic side, approached these companies and told them that they need to start cutting checks? Forgive me if I mix up qualitative and quantitative research. It is okay to do a kind of surface mapping of Whatsapp, but to drill down one needs proper quantitative analysis of what exactly is happening in this field. Good research leads to good policy. Has the Government made any funding available in this space through the Department of Justice and Equality? It seems to me that for small amounts of money - a grant of €10,000 here, a €50,000 grant there - a very solid research platform could be created within the academic field, where there is collaboration between UCC, DIT and so on.

Dr. Maggie Brennan: As far as I am aware no bespoke funding stream is made available either by the Government through the Irish Research Council or by social network companies to research what is going on in the Irish context. As I already mentioned, much of the work carried out by Professor O'Neill was funded by the European Commission. That tends to be where the money comes from. Many of the companies in the industry, such as Facebook, Google and so on, are represented on relevant task forces here and in the UK. The funding tends to go to initiatives in other countries however. They are very selective in respect of what they fund.

Deputy Sean Sherlock: If that is mapped, could the witnesses drop the committee a line on where the research landscape is at the moment?

Ms Alex Cooney: We did get some funding from Tusla in the last year for work in Wicklow specifically. In its strategy for the county it had identified that online safety for children was a key priority so it approached us to provide sessions in schools. It identified the 23 most vulnerable schools across the county. We did sessions with the children and the parents and then reported specifically on the data for Wicklow. The data were very interesting because they differed from our averages.

Deputy Sean Sherlock: Will Ms Cooney provide the committee with a copy of that research?

Ms Alex Cooney: That was our mid-term, but yes.

Deputy Sean Sherlock: If I understand correctly, of the €3.9 million which is available for funding under the EU Connecting Europe Facility, CEF, programme-----

Ms Eileen Leahy: That is a cumulative figure.

Deputy Sean Sherlock: What is the Office of Internet Safety's budget line at the moment? How much is in the kitty?

Ms Eileen Leahy: Our budget line within the Department is for staff.

Deputy Sean Sherlock: It is just for staffing.

Ms Eileen Leahy: It is just for the staffing of the office. Other than that, all the money which comes from the EU is channelled through the four partner bodies which we referenced. We match their funding.

Deputy Sean Sherlock: The bodies are the National Parents Council, the Irish Society for the Prevention of Cruelty to Children, Professional Development Services for Teachers-----

Ms Eileen Leahy: The National Parents Council and *hotline.ie*. In respect of the Deputy's previous question, the National Parents Council run training and online courses for parents. There is probably an issue of awareness around that as well.

Deputy Sean Sherlock: This is the point.

Chairman: I will have to ask the Deputy to conclude now.

Deputy Sean Sherlock: I will make one final point and then I am finished. We have a disparate system but everyone is working with the same aim in mind. There might be a role for this committee in trying to map the system. If we can simply map what is happening throughout the Irish landscape, we can begin to work on solutions and outcomes.

Chairman: I thank the Deputy. I only have one question for our witnesses. It relates to education. Does either the Office of Internet Safety or CyberSafeIreland have a relationship with, for instance, the Irish Primary Principals Network? A moment ago, Ms Curley reference the willingness of primary teachers and whether they felt they had sufficient information and wherewithal to engage in a teaching programme. Aside from training and continuous professional development for those individual teachers who feel they have a deficiency in that very narrow field, where do the principals come in on this issue? Ultimately, they manage the schools and it is their responsibility to ensure that the curriculum and any additional elements are being implemented within the four walls of their schools. I would have thought that it might be an avenue for discussion with both primary and secondary school teaching networks.

The other avenue, which should be considered automatically, is the unions, because virtually every practitioner in the field of education is unionised. From my few months as Chairman of this committee, I know that the trade union movement is heavily involved in the committee's area. It does some really good work. It would certainly be of benefit to try to tap into those organisations and bodies because they appear, at least from my brief, superficial reading, to have something to bring to the table.

I compliment Deputy Sherlock. He is right in that it is necessary for somebody to map the entirety of what the child services and child protection community is doing in the State. While duplication is not unusual, in this instance I would imagine that all the bodies, including An Garda Síochána, Tusla and others, are attempting to do the exact same thing on the cyber side. There may be distinct roles in certain aspects on the criminality side, the preventative side and the education side, but ultimately determining who is doing what and why, and how we can better support them, perhaps through the appointment of a digital commissioner or a single point of authority within the entirety of the sector and all Departments, is of critical importance. My question was whether Ms Leahy, Ms Cooney or Dr. Brennan had a view on building relationships with principals and unions.

Ms Eileen Leahy: From the office perspective, the link is through Webwise and back through it to the Department and the National Parents Council. We would not have a direct contact with the principals' network.

Ms Alex Cooney: We have not had direct contact with the network. We have tried to meet with it but have not done so yet. Hopefully, we will. We deal with principals all the time. It is the principal who will make the booking and have the initial discussion.

Ms Cliona Curley: We would like to see digital safety champions in schools. It could be one teacher, the principal or the home school liaison officer who would have that level of confidence or the tech savviness to be that champion. It would be critical if we are to roll out the programme to have the support of the IPPN, Irish Primary Principals Network, the unions, as well as the Department of Education and Skills. That is how one gets it in every school. We need to reach every child.

Chairman: It could be like the Green-Schools project which is extremely successful across the State. Children at primary level are really engaged and interested in it. A promotional campaign like that would be beneficial. Most of my family, in some way or other, are in the teaching profession at various levels. The majority of them have been involved in the Green-Schools project. A similar type of digital or cybersecurity school project would be worth it.

Ms Alex Cooney: A whole-school approach would be good.

Ms Siobhán McCabe: Webwise organises nationwide ambassadors in schools for the safer Internet day effort in February each year. It recruits school pupils for this role who have a specific focus.

Dr. Maggie Brennan: On the point of digital champions for schools, it is important to focus on prevention in the context of awareness raising efforts and educational intervention. Another important role for any digital champion in a school would be to offer a first line of response where issues come up for children online. This would mean there is a distinct safeguarding and child protection component to this. When issues such as compromised images going viral, bullying within classes, etc, arise in schools, there needs to be both an element of response, as well as a preventive component. This is recognised within the UK policy in this area. The mandate for online safety, education and response in schools was established in the 2016 statutory safeguarding guidance for schools in the UK. It recognises it as a safeguarding issue, as well as one that requires preventive intervention.

Deputy Anne Rabbitte: I agree when an issue emerges, there has to be somebody equipped to respond. It is important it involves both primary and post-primary pupils because those going online are getting younger. Earlier, An Garda Síochána spoke about rolling out a programme with transition year pupils which is to be commended. They can engage with the first-year pupils as they come into the school. It creates awareness and responsibility, as well as bringing out a level of maturity of understanding. That is how we can empower from a bottom-up approach. Do the witnesses agree with that?

Ms Alex Cooney: It is important it is covered both at secondary and primary level. The children going online are getting younger. Our focus is on reaching them before they embark on an online life. We are involved at secondary level and transition year. Our chairperson, Avril Ronan, is involved with Trend Micro's programme that trains up transition year students to deliver to first years. There are some good examples out there.

We have produced an infographic which highlights the need for digital champions, the need for preventive intervention mechanisms, collaboration and leadership. I will share it with the committee.

Chairman: On behalf of the committee, I thank the witnesses for their presentations. Their input, contribution and time are very much appreciated. It will go a long way in informing us on how to put together a report on the issue of cybersecurity for children and young adults.

The joint committee went into private session at 12.15 p.m. and adjourned at 12.25 p.m. until 9.30 a.m. on Wednesday, 8 November 2017.