DÁIL ÉIREANN

AN COMHCHOISTE UM TURASÓIREACHT, CULTÚR, EALAÍONA, SPÓRT AGUS NA MEÁIN

JOINT COMMITTEE ON TOURISM, CULTURE, ARTS, SPORT AND MEDIA

Dé Céadaoin, 14 Iúil 2021

Wednesday, 14 July 2021

Tháinig an Comhchoiste le chéile ag 3.30 p.m.

The Joint Committee met at 3.30 p.m.

Comhaltaí a bhí i láthair / Members present:

Teachtaí Dála / Deputies	Seanadóirí / Senators
Brendan Griffin,	Malcolm Byrne,
Imelda Munster,	Micheál Carrigy,
Johnny Mythen.	Shane Cassells,
	Fintan Warfield.

Teachta / Deputy Niamh Smyth sa Chathaoir / in the Chair.

Business of Joint Committee

Chairman: I welcome my colleagues. We have a few formalities to deal with before we get into the interesting part of the meeting. I ask that the draft minutes of our public and private committee meetings on Wednesday, 30 June, and our public committee meeting on Wednesday, 7 July, are formally agreed as there are no matters arising. Is that agreed? Agreed.

General Scheme of the Online Safety and Media Regulation Bill: Discussion (Resumed)

Chairman: I welcome our witness, Assistant Garda Commissioner John O'Driscoll, from the organised and serious crime unit of the Garda Síochána, who is attending remotely. The format of the meeting is that I will invite our witness to make an opening statement, which will be followed by questions from members of the committee. As he is probably aware, the committee may publish the opening statement on the website following the meeting.

Before I invite the witness to deliver his opening statement, which will be limited to five minutes, I wish to advise him about parliamentary privilege. Witnesses are reminded of the long-standing parliamentary practice that 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, or otherwise engage in speech that might be regarded as damaging to the good name of that person or entity. Therefore, if their statements are potentially defamatory in respect of an identifiable person or entity, they will be directed to discontinue their remarks.

As the witness today is attending remotely from outside the Leinster House campus, please note there are limitations to parliamentary privilege and, as such, he may not benefit from the same level of immunity from legal proceedings as a witness who is physically present does.

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 her or him identifiable. I remind members of the constitutional requirement that they should be physically present in the confines of Leinster House or the Convention Centre Dublin in order to participate in the public meeting. I cannot permit a member to attend who is not adhering to that constitutional requirement. I ask members to identify themselves when contributing for the benefit of the Debates Office staff who are preparing the Official Report. I remind those participating in the meeting to mute their mobile telephones or, better still, switch them off.

I now call on Assistant Garda Commissioner O'Driscoll to address the committee.

Mr. John O'Driscoll: I thank the Chair.

The primary objective of the Garda Síochána in undertaking the many tasks that fall within its remit is to keep people safe. Throughout its almost 100 years in existence, keeping people safe has involved the Garda Síochána devising strategies to prevent people from being harmed while travelling on road networks as pedestrians, on bicycles, or within vehicles, and through

violence that may be inflicted on them in their homes and on the streets by way of assault, burglary and other such crime that we are all familiar with.

However, as we approach the beginning of our second century in existence, the Garda Síochána is required to be equipped also to keep people safe in the online world where they are connected to others through computer telecommunication systems, such as the Internet. Words and phrases now in common usage within law enforcement such as "malicious domain", "ransomware", "data harvesting malware", "botnet", "cryptojacking" and "the darknet" were until recently not well known. However, cybercrime is progressing at what Interpol describe as "an incredibly fast pace", with new trends constantly emerging. Interpol warns that cybercriminals are becoming more agile, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and co-operating with each other in ways we have not seen before. The crimes concerned know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

It is essential, therefore, that the Garda Síochána and other law enforcement entities keep apace with new technologies to understand the possibilities they create for criminals and how they can be used as tools for fighting cybercrime. In its 2018 report, the Commission of the Future of Policing in Ireland referred to the fact that extortion, fraud, ransomware, child pornography, sexploitation and other cybercrime and Internet-enabled crimes are proliferating fast. In this regard, the commission observed that Ireland is not alone in struggling to deal with the threat.

While we are all vulnerable to being a victim of online-related criminal activity, the Garda Síochána recognises that some are more vulnerable than others, including children and old people. This is reflected in the strategies and initiatives it has undertaken to tackle cyber-related crime. The Garda Síochána endeavours to ensure that all personnel throughout the organisation are aware of and are appropriately trained and equipped to participate in an appropriate manner in tackling online related crime. However, responsibility for ensuring a co-ordinated approach to tacking the criminality involved is assigned to particular sections and units.

In this regard, I mention first the Garda National Protective Services Bureau, GNPSB, which provides advice, guidance and assistance to members of the Garda Síochána investigating sexual crime, online child exploitation, domestic abuse, human trafficking and organised prostitution and plays a particular role in supporting victims of crime. The bureau leads the investigation in more complex cases. The GNPSB liaises with relevant Departments, State bodies and voluntary groups, embracing the essential multi-agency approach to tackling relevant crimes and their causes. The bureau has provided a wide range of advice for use by adults and children for the purpose of protecting children from those who target them online, and with a view to making relevant contact details available to those who fall victim to such crime.

The Garda National Protective Services Bureau keeps peer-to-peer activity relating to file-sharing of illegal material over private networks under constant review. This includes the use of particular software tools. In this regard, it has recently undertaken particular investigations targeting relevant criminality under Operation Ketch. Divisional protective service units have been rolled out nationwide by the Garda Síochána, and roll-out of these units meets a key commitment in A Policing Service for the Future, the four-year implementation plan giving effect to the recommendations of the Commission on the Future Policing.

The local protective services units participate in protecting people who engage in online activity and investigating associated criminality. Ireland's national service for the reporting of

suspected online illegal content is *hotline.ie*. On receipt of reports, *hotline.ie* content analysts examine the content and if the material is considered illegal will issue notice and take down request orders to the appropriate service provider and notify the Garda Síochána with the relevant information. Where that content pertains to children the Garda national protective services bureau has a particular role.

The Garda national cybercrime bureau, GNCCB, was established as a unit in 1991 and re-established more recently in 2017. Last year it was assigned a detective chief superintendent as its head. It is a national unit tasked with the forensic examination of computer media seized during the course of any criminal investigation. These include murders, cybercrime, online harassment, computer intrusions, child exploitation offences and any criminal investigation in which computers are seized or may contain evidential data. The unit also conducts investigations into cyber-dependent crimes that are significant or complex in nature, network intrusions, data interference and attacks on websites belonging to Departments, institutions and corporate entities.

The GNCCB is responsible for the prevention, detection, investigation and prosecution of cybercrime incidents in the State. Cybercrime generally involves incidents where the Internet, information and communication technology, ICT, systems or digital devices play a significant role in the commission of a criminal offence. The GNCCB works collectively with local and national Garda units along with national and international stakeholders to reduce the threat and impact of cybercrime on individuals and organisations.

The GNCCB is staffed by civilian personnel and Garda members of various ranks up to detective chief superintendent. Personnel assigned to the bureau undergo intensive training in the area of forensic computing and cybercrime investigations, and give expert evidence and testimony in all types of investigations and prosecutions in court. In addition to its forensic and investigative role, the GNCCB acts as a liaison with various partner agencies and law enforcement bodies.

The Garda Síochána has recently increased its dedicated resources in the cyber area and is continuing to grow its capabilities in this regard. In recent months, the GNCCB has established regional hubs throughout Ireland, in places including, Cork, Wexford, Galway and Mullingar.

The Garda national economic crime bureau, GNECB, is a specialist unit that investigates fraud-related crime involving complex issues of criminal law or procedure. The bureau investigates serious and complex cases of commercial fraud, cheque and payment card fraud, counterfeit currency, money laundering and breaches of the Companies Acts. The GNECB has been to the forefront in tackling an increase in online-related crime experienced during the Covid-19 pandemic, including: investment fraud; phishing/vishing/smishing frauds; online shopping fraud; invoice redirect/business email compromise fraud; and fraud involving people allowing others to use their bank accounts, who are referred to as money mules.

Along with launching criminal investigations relating to the many frauds discovered and reported, the GNECB has engaged in an extensive media campaign designed to alert people to the existence of the frauds in question in the hope that they will not engage, online or otherwise, with the criminals involved. The Garda Síochána interacts with the National Cyber Security Centre and contributes to ensuring implementation of a number of commitments with regard to cybersecurity that are included in the programme for Government.

In tackling the wide range of online-associated criminality, the Garda Síochána enforces

provisions within all relevant legislation including: the Criminal Justice (Offences Relating to Information Systems) Act 2017; the Harassment, Harmful Communications and Related Offences Act 2020; the Child Trafficking and Pornography Act 1998, as amended by the Criminal Law (Sexual Offences) Act 2017; the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021; the Prohibition of Incitement to Hatred Act 1989; and organised crime related legislation within the Criminal Justice Act 2006.

On international co-operation, Europol set up the European Cybercrime Centre, EC3, in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus help to protect European citizens, businesses and governments from online crime. Since its establishment, EC3 has made a significant contribution to the fight against cybercrime. Each year, EC3 publishes the Internet Organised Crime Threat Assessment , IOCTA, its flagship strategic report on key findings and emerging threats and developments in cybercrime. The Garda Síochána works closely with the EC3 unit at Europol in targeting cybercrime impacting on Ireland that has a European dimension. We have seconded a staff member to EC3 in Europol in recent months.

The Garda Síochána also utilises the services of the Interpol cybercrime directorate in tackling online related crime. This directorate is working with its almost 200 member countries, private sector partners and cybersecurity communities across the globe in attempting to ensure a robust law enforcement response to cybercrime.

Chairman: I thank Mr. O'Driscoll. That is very comprehensive and insightful in the context of the debate and discussion we are having on the online safety and media regulation Bill. We are very glad to have Mr. O'Driscoll's input into our deliberations on all of this. One can imagine how complex an issue this is for Mr. O'Driscoll and his team.

My colleagues now have the speaking rota. Not all colleagues are online just yet. In the absence of some I will begin with Deputy Mythen. Is Deputy Mythen in a position to take his slot?

Deputy Johnny Mythen: I am sorry, talking about cyber issues and I have just pulled my plug out of the system.

Chairman: I hope it is not a cyberattack.

Deputy Johnny Mythen: I thank Mr. O'Driscoll for his contribution and for the work he has done, especially during the recent ransomware effort, which was a horrendous attack on our health system.

Does Mr. O'Driscoll believe that his unit is up to speed with its counterparts in Europe? What improvements would Mr. O'Driscoll like to see done now and what improvements are required for the future to combat cyberattacks such as that?

Mr. John O'Driscoll: This morning I met with the chief superintendents in each of the bureaus I have mentioned to discuss relevant issues. We have ongoing investigations and we discuss the legislation we have on the Statute Book. As I have referred to, we use a wide range of legislation. The criminals are continuously changing tack so each jurisdiction needs to make sure its legislation is sufficient to tackle the issue involved. In this regard, the Minister for Justice has announced new legislation that is planned, the Garda Síochána (powers) Bill. This will be important legislation from our perspective insofar as we are constantly seizing media equipment that we require to search but we do not necessarily have the sufficient powers to access

what is on those media devices. The proposed legislation will allow us to use a single power of arrest in particular in relation to particular offences. It will allow us to search and to demand access to the content of media equipment. Where people fail to provide passwords, etc., there will be significant offences involved. This legislation is necessary because there is no point in us seizing the media equipment that is so important to the relevant investigation if we cannot access what is on it. If we are prevented from accessing the content then there must be a penalty involved. In Operation Ketch, for example, on four occasions we searched numerous premises where we know that child abuse imagery is being utilised and we seized equipment. The equipment is getting more sophisticated and has greater capacity, and we need the capability to access that data. The Deputy asked about what we need to do our job into the future. We need better equipment. We are in the process of acquiring that in recent months. Decryption equipment has been provided which will help us. This morning, I talked to my team about other equipment which we believe would be useful to us. We are preparing a business plan so that our capacity will match that of the criminal networks involved to be able to tackle them. Constant review of the relevant legislation by the Legislature will probably be necessary. In some regards, much of what we are dealing with here is what one person described as "unknown unknowns". We do not know what is ahead of. There are crimes that we would not have envisaged just a short few years ago which we are now required to tackle. Some of the recent legislation has been especially useful. Continuous monitoring and strengthening of that legislation will be necessary.

One aspect of legislation that we frequently use relates to organised crime. Besides the legislation that we will use to penalise what is taking place online, the groups involved in this are involved in organised crime. The legislation relating to organised crime from the Criminal Justice Act 2006 and Criminal Justice (Amendment) Act 2009 is especially useful. There are now more frequent charges for those we identify as suspects that relate to organised crime as distinct from the other specific crime that I mentioned earlier. Some crime is newer, such as that relating to what is referred to as Coco's Law. That legislation is especially useful in tackling offences related to cyberbullying. It was enacted in February. Investigations that are currently taking place will probably not yet have reached prosecution stage. That is useful legislation that we are preparing to use and about which training is being delivered to make sure that we implement the offences contained within it where relevant.

Deputy Johnny Mythen: Mr. O'Driscoll mentioned money mules. Does he think there is enough information available to people? Young people often get caught up in this. They see a few quid extra coming in. They do not realise where it is coming from. It is a matter of going down to the bank and putting the money in their account. They do not realise the implications of what they are doing. Is there enough information for young people to avoid that sort of crime?

Mr. John O'Driscoll: Among the people I met this morning and discussed these issues with is Pat Lordan, who is the head of the Garda national economic crime bureau. It has spent much time recently engaging in media campaigns to highlight the importance of not getting involved in criminality of this nature, especially to students. Third level students have been targeted specifically to open accounts to launder money. If one is approached and it appears that a quick buck can be made, there must immediately be significant suspicion that criminality is involved. We are trying to get that message across to students. We recently had a fraud awareness week where we engaged in extensive media campaigns to advise people of the criminality involved. Personnel attached to the Garda national economic crime bureau have gone on "Crimecall" and used other such mechanisms to highlight the criminality involved. There have been a number of recent prosecutions, which are another means by which people will quickly learn the impli-

cations of engaging in criminality of this nature. We particularly warn students about facilitating people to launder money. It can destroy a person's potential to gain employment or to travel abroad. It is clearly ill-advised to engage in the activity although there is a prospect of making money that so many young people of that age desperately need.

Senator Micheál Carrigy: I welcome the assistant commissioner. Has the Garda Síochána supports in place for its own staff to deal with issues such as online crime? Is it sufficiently resourced and does Mr. O'Driscoll feel that the Garda Síochána needs additional resources in future for new regulations that may come in? I noted in correspondence the issue arising relating to GDPR in interactions between gardaí and the media commissioner when that position is put in place. What is Mr. O'Driscoll's view on that? Does he think it needs to be addressed?

Mr. John O'Driscoll: It is always dangerous to ask law enforcement officers if they want more resources. Our demands will be never-ending. That reflects the extent of crime of the nature that we are talking about. Having said that, the Garda Síochána's approach to this has included forming bureaus that did not exist a short few years ago, which are now well-resourced, including the Garda national cybercrime bureau. It was recently provided with more staff. It needs additional staff. We are in the process of employing civilian experts in this area. We are in competition with the private marketplace. The public service and the Garda Síochána in particular are not always in a position to remunerate people to the extent that private industry can. We have a difficulty in acquiring the people we want and then in retaining them. That is a fact of life which we have to deal with. Part of the resolution to that may be bringing people in on a short-term basis, which would not be a typical form of employment in the Garda Síochána or in police services in general but it is the picture we are dealing with.

As I said earlier, the equipment being used by criminals is growing in sophistication so we need to match it. That is expensive. We have drawn on the resources of the International Security Fund recently to fund some of the decryption equipment that has been provided to the Garda national cybercrime bureau. We hope that such funding will be available in future to ensure that we can be equipped in the manner that we need to be equipped.

Demanding work is undertaken by staff, especially those dealing with child abuse imagery. A new policy was recently put in place for staff who are engaged in this sort of activity and investigation to make sure that their welfare is catered for. To be watching that sort of imagery as part of one's job over a protracted period of time is obviously not a task we would wish upon anyone. Thus we are developing our policies in that regard. We obviously cannot acquire all the resources we need to tackle all these issues but by plugging into other agencies and by engaging in the international community we can draw upon the resources of others. This is so critical not just in the cybercrime area but right across the board, be that with drugs and organised crime, economic crime or any other type of crime. We very much engage at an international level with our counterparts in other jurisdictions and, as I referenced, with Europol, Interpol, Eurojust and all those other agencies where resources are available on a European level and a more global basis. We certainly will need more resourcing and will continuously update our requirements in that regard. We hope that with the demands which are right across the board within policing, some of those requirements can be met. The bill for An Garda Síochána this year is just slightly short of €2 billion so there is a huge amount of money involved. It is an ever-demanding requirement but on the other side of the coin we are seizing more money from the criminal networks so hopefully that will help to balance the books to some extent.

Senator Micheál Carrigy: I have one more question, which may reference the general data protection regulation, GDPR, issue. The assistant commissioner has had experience previously

with the main online platforms and dealing with them with regard to abuse. It is something we, as politicians in the national limelight, are unfortunately targeted with on a regular basis. What has the assistant commissioner's experience been of dealing with the various platforms and getting stuff taken down, or getting the use of certain material for evidence in a case, if need be? Is it positive or negative?

Mr. John O'Driscoll: Again, this is an area where international co-operation is important also. I have sat at meetings at an EU level where these issues have been discussed. There is an approach across the EU to our engagement with private industry but at a local and national level we also engage with relevant stakeholders. As time moves on those relationships are improving. We have memorandums of understanding, MOUs, signed with particular private entities in relation to tackling particular forms of crime, particularly the child imagery issues. This is the way forward. We must engage with our stakeholders in a meaningful way. As I said, while we will do that to the extent we can at a national level it does need the international law enforcement community and the institutions of the EU, among others, to ensure all those stakeholders play their part in tackling the criminality involved.

Deputy Brendan Griffin: I thank the assistant commissioner for giving up his time this afternoon and for all the work he and his colleagues do. I take this opportunity to congratulate them on the huge cocaine seizure announced today as well. It is positive news from a law enforcement perspective but also reinforces the huge problem that is there, the huge market that is here as well and the amount of people who continue to use such substances despite knowing everything that goes with that.

I welcome the remarks about the welfare of the assistant commissioner's team which is tasked with the most difficult job of having to go through some of this really atrocious online content, which is a priority. These team members really are some of the unsung heroes of law enforcement. They work behind the scenes but they deserve all the support they can possibly get because exposure to that level of depravity on such a regular basis can, I am sure, have a really profound impact on a person.

Touching on a point raised by Senator Carrigy, have the tech companies been co-operative with the Garda in relation to prosecutions and its investigations? I ask because I want to delve further into that and see whether there are impediments there from the tech companies that require remedying to ensure easier prosecution.

The other area I want to ask about as well is the issue of minors who are perpetrating online crime and abuse and how we deal with that. It is an area of difficulty for law enforcement in general, be that with street crime or anti-social behaviour. As such, the assistant commissioner might speak to the approach to online crime as well.

Mr. John O'Driscoll: Taking the last matter the Deputy mentioned, that is, minors who are perpetrators of crime, the Garda national protective services bureau, GNPSB, works closely with the Department of Education. That Department has educational campaigns in place on trying to keep people safe online. These are delivered within schools to the various age groups. Influencing parents is an important part of the process and we work closely with the Department in that regard and have been jointly involved in initiatives that attempt to keep people safe and to improve behaviours online. That is essential and will continue. We have divisional protective services units throughout the country now. Our Garda national crime prevention office is also engaged in the distribution of material dealing with personal safety online, particularly targeted at parents and referring to cyberbullying. I am looking at one document that talks

specifically about cyberbullying and gives key advice for parents, such as blocking senders, not replying and reporting problems. All these issues are dealt with in information bulletins issued by the Garda Crime Prevention National Centre of Excellence which is next door to me in Harcourt Square. Minors are particularly vulnerable in this area. Additional policing methods of protecting young people when young people were on the streets was easier than protecting them online but we all must adapt to this online world and try to police as best we can.

The Deputy will have to remind me of the first issue he mentioned.

Deputy Brendan Griffin: I asked about the tech companies and their level of co-operation or otherwise. Other than that it was just comments on the welfare of Garda investigators and on today's seizures.

Mr. John O'Driscoll: Again, I referenced the tech companies and our engagement with them to some extent. The relationships are developed and much improved. Aside from engaging with them to the extent that we want to get their assistance we also have a formal engagement with them where they are required to provide evidence when we deem that information in their possession might be useful as evidence. For that purpose, we will use the relevant legislation, search warrants and other such devices, in order to acquire the evidence so that it is available in a manner that is suitable for prosecution of a crime. While institutions, companies or whatever may be willing to provide evidence, we have to use that formal route in any event and it gives better legal coverage to all concerned when we go about business through the use of the relevant legislation in that manner. We get the assistance of those companies in many of those investigations, where that formal route is used in order to acquire the evidence involved.

On the welfare issue, as I said, we have a new policy document issued by our chief medical officer. It was some time in the making to ensure it was robust and appropriate for this type of crime. It is the sort of service that needs to be available to members of An Garda Síochána in a whole range of areas, where they engage in traumatic events. In this case, the welfare issues of those specifically involved in dealing with issues online is addressed.

Also, approximately two years ago, we issued details to all of our members of a 24-hour phone number where welfare issues arise in particular investigations. Members of An Garda Síochána engage in all sorts of activities where trauma can be involved. This can be fatal traffic accidents which, regrettably, we have had too many of in recent weeks. It can be a situation similar to that I attended many years ago following the tsunami. In such a scenario one has to deal with many dead people. It can also be dealing with people, such as those who were found dead in a container in Wexford a number of years ago. There are fires, traffic accidents and many different types of events where trauma is involved, which can have an impact on members of An Garda Síochána. We endeavour through our chief medical officer and welfare services to provide the sort of backup to personnel that is required. Again, this is something that needs to be monitored on a continuous basis to ensure those services are working and are protecting personnel to the extent that is appropriate.

Chairman: I thank the assistant commissioner and Deputy Griffin for his question. I invite Senator Warfield to join the debate. He has five minutes and I thank him for his patience.

Senator Fintan Warfield: I thank the Chairman and I thank the assistant commissioner. I have heard some negative stories from people who report online harassment to An Garda Síochána. I note from the assistant commissioner's statement that An Garda Síochána endeavours to ensure personnel throughout the organisation are aware of, and are appropriately trained and

equipped to deal in an appropriate manner with tackling, online-related crime. Is there a knowledge gap in An Garda Síochána when it comes to online safety?

My second question is to ask the assistant commissioner to outline the process adopted when a person is subjected to a torrent of online abuse from numerous possibly anonymous accounts where one abusive comment may be made but collectively there are hundreds of other accounts. What steps does An Garda Síochána take to try to help a person in that case?

I am interested in hearing if the assistant commissioner has anything to say about the prevalence of cyberstalking or harassment online. Restraining orders only go as far as to restrain a person from the family home and most of these cases would come under harassment under the Non-Fatal Offences Against the Person Act 1997. Anecdotally, I hear that most young people would be of the belief that cyberstalking or cyberharassment is still rampant. Has the assistant commission anything to say on that issue?

Mr. John O'Driscoll: The extent of cyberstalking is difficult to estimate. Like many forms of crime, we only know of those reported to us. Part of what we are doing is trying to encourage more people to come forward and report crimes of that nature so we can get a full understanding of the extent that it is taking place. There have been successful investigations of such activity where, on their conclusion, there has been a prosecution and, in some cases, a conviction.

Clearly, much of the investigation involved in criminality of the nature described by the Senator is new to members of An Garda Síochána. Ensuring that our members are equipped and have full knowledge of all of the legislation available to them and, indeed, the existence of offences is a challenge for us. Delivering training has been a particular challenge for An Garda Síochána and for the Garda College in Templemore during the Covid-19 pandemic when the college closed. We are delivering training to our members throughout the country. The Garda national protective services bureau is particularly involved in developing training in the area of some of the criminality involved here and some of the training is being adapted to be delivered online to members rather than in a classroom scenario.

We have started to recruit again recently and I am aware there was one class of recruits who joined us in May and who spent the first number of weeks being trained online before travelling to Templemore to receive some training in a classroom scenario.

Undoubtedly, it will take some time for all of our members to become fully *au fait* with the full plethora of new legislation in this area but through the creation of the bureaus in recent years, namely, the Garda national protective services bureau and the Garda national cybercrime bureau, in particular, we now have centres of excellence where, when members of An Garda Síochána throughout the divisions and the country come across criminality, the investigation aspect of which they are ensure, they can link into the national bureaus which will assist them in undertaking the investigations. Indeed, in the case of the Garda national protective services bureau, we have more recently established units of this bureau in each division. These units are trained by personnel from within this bureau in the investigation of criminality, some of which falls under the headings that we mentioned. There is a unit of that nature in each division and training is being delivered in that area.

There is no doubt that these are complex investigations and can take some time to bring to a successful conclusion. Through the interaction with victims and with their assistance, we have the capacity to achieve convictions. That is occurring on an ongoing basis.

Chairman: Does Senator Carrigy wish to come back in?

Senator Micheál Carrigy: I wish to return to a couple of matters. Deputy Griffin referred to one of them, namely, the fact that in recent times we have seen journalists being abused online and, as politicians, we are trolled and abused. There is the issue of false accounts. The online platforms have many procedures in place, but they are not dealing with the large number of false accounts. As I said, they are trolling many of us involved in political life and, recently, journalists have been abused and have received threats online. What is Mr. O'Driscoll's view on what these media companies should do to address this?

Mr. O'Driscoll mentioned working with the Department of Education. This is something we discussed at a previous meeting. We asked representatives of Facebook, Twitter and so forth to fund a campaign with the Department of Education. As Mr. O'Driscoll said, some work is done there, but it is not rolled out across all schools. Individual schools have to ask for that programme and the number of schools that have asked for it is significantly low. As I have stated previously, a safety programme should be rolled out across all schools in the country to show children the abuses and so forth that exist. It would be good to hear Mr. O'Driscoll's views on that.

Mr. John O'Driscoll: Certainly, every child should have the opportunity of receiving information and help in tackling the criminality involved. Whatever way that has to be delivered, we must ensure we leave nobody behind. The Garda Síochána, being in every district and division in the country, will do its part to engage with the Department of Education, with schools at local level and with young people in whatever manner it can to ensure it delivers its message and the guidance it can offer.

The Senator mentioned the example of the targeting of journalists. I am aware of a number of successful investigations that have resulted in prosecutions in that area. In any case where criminality of that nature is discovered we certainly will engage with the relevant companies and will do all we can to ensure that they play their part in preventing the crime, in the first instance, and the continuation of it where it has commenced, while at the same time focusing to a large extent on the investigation and attempting to gather the evidence that will be sufficient to institute a prosecution. A lot of the criminality involved recently is new to all concerned. It is a fact that everybody is now online whereas a few years ago fewer people would have been online. Each year that the number grows, the potential for all of us to become victims is growing and obviously the extent of the criminality of this nature occurring is growing. Into the future, it is going to take the resources of all of us, including the resources of the Garda Síochána, relevant Departments and other State agencies, to bring about a situation where it is safer to be online.

Chairman: I wish to tease out further something that has been touched on by my colleagues. Many witnesses, organisations and groups have appeared before the committee over the last couple of months for our pre-legislative scrutiny on this topic, including the element of reporting, the steps taken by An Garda Síochána and how tangible these tech giants are in terms of accountability. We heard repeatedly from Facebook, TikTok and the social media giants about their community standards in terms of what is acceptable online behaviour or harmful content and what is not. To my mind, and I would say for many of my colleagues, there is no benchmark for what should and should not be acceptable.

We also heard accounts of families who had seen their children receive online abuse, taken a screenshot of that abuse and reported it to the companies. Of course, that was a futile exercise,

with some recounting that it was days before that content might be removed. You have touched on this already. In a scenario where a child is in primary school and the parent sees harmful content, the parent gathers as much information as he or she can and goes to the local Garda station and reports it, do you find that this can be expedited quickly through the tech giants to get to the source of the information or are there challenges put in your way in terms of sourcing the identity or shutting down that account to get rid of the harmful content? I am thinking specifically of children. In a practical sense, when a parent goes to local gardaí with as much evidence as he or she can gather on harmful content, what are the steps or how long does it take for the tech giants to respond in a meaningful way?

Mr. John O'Driscoll: Each investigation, obviously, has to be taken in isolation. They vary greatly. Some may result in success in bringing about an end to the activity much quicker than others, but the expertise of the national units is available to members of An Garda Síochána at a local level and the intervention with the private companies involved can be facilitated through the expertise at national level. However, we can only bring about a scenario that is permitted by law. We can only force companies to do that which we are lawfully entitled to demand of them. This is an area where the legislation needs to be monitored on an ongoing basis to make sure it is robust enough to achieve the aims we all desire in preventing the activity involved.

Chairman: Can I stop you there?

Mr. John O'Driscoll: Yes.

Chairman: I do not mean to be rude, but I am trying to get this clear in my head. What I am asking is not a reflection on An Garda Síochána. I am trying to elicit the agreeableness and the forthcomingness of the tech giants when the Garda has an issue and approaches them. I have been told that one will never get contact with Facebook, TikTok or Twitter immediately on the telephone to address something like that, that one almost has to get clearance from their operations in the United States and that it can take a number of weeks before it comes back again. In other words, it becomes a very elongated process which is exasperating, particularly for the victims involved. It is no reflection on the work of the Garda Síochána, but more a reflection on the challenges and obstacles that are put in its way in terms of these tech giants being forthcoming with the information and being as helpful as possible to address this when it happens.

Mr. John O'Driscoll: I understand you are not criticising us, Chairman, to the extent that we can only do whatever the law permits us to do.

Chairman: Exactly.

Mr. John O'Driscoll: Obviously, at the same time we have to ensure that those who are investigating take every step within their remit to bring about a situation where the contact is made in an appropriate way with the company involved and the requests that are appropriate in terms of taking down information from their servers are done as expeditiously as possible. Unfortunately, it has to be done by us within a legal framework and, as the Chairman said, that can take time. In some investigations, that will take longer than others. We endeavour to commence the process as expeditiously as possible so that we do not contribute to any delay. Investigations vary in their complexity and resolution is reached more quickly in some cases than in others. We hope that as we become better and more experienced in dealing with these complex investigations, the desired result will be achieved more speedily as time progresses.

Chairman: I am trying to establish how helpful the social media companies are. The Garda

can only do so much. It needs willingness from the tech giants to give it the information that is required to enable it to follow through on its investigation. That is what I am trying to nail down. How willing to help are those companies? What can we, as legislators, do to progress that? The anecdotal information is that the willingness to help is not there among the tech giants.

Mr. John O'Driscoll: We will not get information from companies unless we have the legal demand to achieve it. That does not apply only to dealing with Internet-related material. In circumstances with which I would be more familiar, going back a number of years, we would, for example, look for information from the banks on money laundering related to drug trafficking. The banks wanted us to come in with orders under section 63 of the Criminal Justice Act 1994 and would then immediately hand over the material. If we went knocking on the door and suggesting the banks had material that could prove money laundering or information about it, the banks could not give it. They needed to get the court order but would then immediately provide the information to us. That, of course, can only be achieved if the appropriate legislation is in place. The less complex the legislation which makes it crystal clear that companies are to provide the information, the fewer difficulties there will be in acquiring it. We have to go through those legal processes, make the legal demands of companies to provide us with the information and-----

Chairman: There are challenges in terms of the constraints on the Garda under the legislation in place at the moment. The legislation does not provide for the flexibility the Garda needs to act in a more immediate way and force the tech giants to give it the information it needs.

Mr. John O'Driscoll: The less complex the legislation is, the easier it will be for us to make the demands. Inhibiting factors in terms of requiring the evidence at a speed we desire will be removed if there is less complexity to the legal process involved.

Chairman: I thank the assistant commissioner. That brings us neatly to the end of today's session. I thank the assistant commissioner most sincerely for his time and the preparation he put into his comprehensive presentation. His contributions very much assist us in the pre-legislative scrutiny work we are doing around this cyber and online regulation Bill.

Sitting suspended at 4.34 p.m. and resumed at 4.47 p.m.

Chairman: This meeting has been convened in the context of the committee's continued pre-legislative scrutiny of the online safety and media regulation Bill 2020. I welcome Mr. Ciaran Moore, helpline manager with Samaritans Ireland, and his colleague, Ms Louise Hamra, policy manager for Samaritans Ireland. Both witnesses will be joining the meeting remotely via Microsoft Teams. The format of the meeting is such that I will invite our witnesses to make their opening statement which will then be followed by questions from members of the committee. I remind members that they should raise a hand if they wish to speak. We will not be using a speaking rota. As our guests are probably aware, the committee will publish their opening statement on its website following the meeting.

Before I invite the witnesses to deliver their opening statement, which is limited to three minutes, I will advise them of the following with regard to parliamentary privilege. Witnesses are reminded of the long-standing parliamentary practice that they should not criticise or make charges against any person or entity by name or in such a way as to make her, him or it identifiable, or otherwise engage in speech that might be regarded as damaging to the good name of the person or entity. Therefore, if their statements are potentially defamatory in respect of an

identifiable person or entity, they will be directed to discontinue their remarks. It is imperative that they comply with any such direction. As the witnesses are attending remotely from outside the Leinster House campus, I ask them to note that there are some limitations to parliamentary privilege and, as such, they may not benefit from the same level of immunity from legal proceedings as a witness who is physically present does.

With all of that housekeeping out of the way, I welcome our guests. This is the way we do things now, that is to say, virtually. We used to have people in the committee rooms. Having said that, we make the most of it. I thank the representatives for joining us today. Their submission in respect of our pre-legislative scrutiny is very welcome. Without further ado, I ask Mr. Moore to take the floor to make his opening statement.

Mr. Ciaran Moore: I thank the Chair and the members of the committee for inviting Samaritans Ireland to discuss the general scheme of the Bill and the relationship between online harms and the impact they can have on an individual's mental health and well-being. As the Chair has mentioned, I am joined today by Ms Louise Hamra, our policy officer. Samaritans is the only all-island, 24-hour emotional support helpline. We have more than 2,000 volunteers in 21 branches, responding to approximately 1,500 calls for help every day. We believe that every life lost to suicide is a tragedy and we work tirelessly to reach more people and make suicide prevention a priority. As part of our vision that fewer people die by suicide, Samaritans Ireland has undertaken extensive research around best practices online and developed clear guidance on staying safe in the online environment. These guidelines were co-designed by young people with lived experiences of self-harm and suicidal feelings and those with experience of supporting others at risk.

The Internet can be an invaluable resource for individuals experiencing self-harm and suicidal feelings. However, it can also provide access to content that can be distressing and triggering. In our written submission to the committee, we specifically examined the context in which suicide and self-harm exist within an online environment and the best ways to minimise these online harms without silencing or stigmatising those with lived experiences. We would like to recommend that the following matters are considered and incorporated within the proposed legislation.

First, suicide and self-harm are complex and multifaceted, as are the recovery journeys, and what can be a trigger for one user could be helpful to another. Understanding the potential risks and benefits to users is critical when determining what content should be removed. We recommend the development of guidelines and policies to encourage safe posting and to also ensure that regulations around the removal of content are drafted in ways which will not further stigmatise those with self-harm or suicidal thoughts and experiences, or both.

Second, the prevalence and placement of harmful online content should be explicitly identified as a key risk of harm. Measures should be included in the Bill requiring service providers to identify instances of inappropriate display or inappropriate prevalence of content with a risk of harm. The introduction of ethical algorithms would allow for the minimisation of prolific consumption of difficult content. The adoption of such policies could reduce so called doom scrolling and encourage help seeking without inhibiting individuals' rights to view public content.

Third, platforms should also consider how they can provide support and signposting to people who have already viewed distressing content online, and how to communicate sensitively with users whose content needs to be removed or edited. Companies must take measures to

protect and promote the well-being of all persons who moderate self-harm and suicide content and should be held accountable, both for their moderation policies and for the support procedures in place for moderators.

Samaritans Ireland welcomes legislation for online safety and would encourage amending the Bill to specifically provide for the establishment of an adequately resourced online safety commissioner as part of the new media commission. This measure would ensure the complexities around delineating harmful and helpful content relating to suicide and self-harm are appropriately managed with codes of practice being developed in consultation with experts. I thank members for their time. We are open to any questions.

Deputy Imelda Munster: I welcome Mr. Moore. I am well aware of Samaritans Ireland and the excellent work it does; it has a branch in my town of Drogheda. I also know that Samaritans Ireland gives guidance to journalists and broadcasters around talking about suicide. Am I right in saying that?

Mr. Ciaran Moore: We have been publishing media guidelines, which have been adopted by the Broadcasting Authority of Ireland, BAI, for a number of years and we do training with different journalists through the National Union of Journalists, NUJ.

Deputy Imelda Munster: Could Mr. Moore talk about the differences between regulating or managing this type of content in the traditional media versus online?

Mr. Ciaran Moore: It is a relevant question because this is something we started to deal with about four years ago when we started to look at online content. For a number of decades, we had been providing guidance to broadcasters, journalists and editors in newspapers on how they would treat a story that would break. We pointed out what types of things were helpful to say in a story and what types of things should be avoided. Also, in dramas we would consult with the likes of "Eastenders", "Coronation Street" or "Fair City" if they covered these type of issues in a story.

The main difference between traditional media and broadcasting online is who one is talking to. We can talk to the journalists and broadcasters and that decides what is broadcast whereas anybody can publish something online. One of the things we are concerned about is that many of the people who publish things do not intend to cause harm. They could be vulnerable themselves or talking about their experiences and it could be part of their therapeutic process. Yet, other people receive this content and it can cause harm. The scale of the material is different, who is publishing it and who one has to talk to in order to try to manage the environment is different and the dangers are different. Harm could be caused to some of the people who are talking by stigmatising them and removing their content. We put quite a lot of work into adapting our media guidelines and we are concerned that there has to be adaption in the way the regulation works from one sphere into the other.

Senator Fintan Warfield: I thank Mr. Moore and Ms Hamra for joining us. I would like to pick up the conversation about ethical algorithms. There is a quote from "The Social Dilemma" to the effect that the algorithm is convincing someone somewhere that the earth is flat. I am guessing the witnesses agree that we need more transparency around the algorithms. Can they talk about why the algorithms concern them in terms of suicide and suicide prevention?

Mr. Moore made a brief reference to the well-being of staff who moderate platforms and whether platforms should be accountable for the well-being of their staff and the supports they

get. Could the witnesses expand on that?

Mr. Ciaran Moore: On the ethical algorithms, we are aware of a lot of work that has been done around the transparency of same. The Digital Services Act and some of the European legislation also contemplated this area. One of the areas we are particularly concerned about is that a lot of the algorithms present content to increase engagement and younger people may not have the same awareness that they are going down a rabbit hole of particular types of material. We know that in the UK there have been a number of cases of younger people who have died by suicide, and on examining their social media use, it has been heavily dominated by this type of material. We have also undertaken research with the University of Bristol, which has looked at how people who have had suicidal ideation use the Internet. We see that they initially use it in quite a targeted way to seek support or to look for something but in the period of distress they see a huge amount of content. Much of that content tells them that if they watch this, they can also see something else. It is important to interrupt these patterns. A great deal of our research around ways to engage with people who are suicidal is about interrupting these circles of thought they have. The online environment is dangerous because we are still looking for the most engaging content to be presented to people.

The issue of content moderators is related. The people who will identify patterns of complaints will be the content moderators. If parents are complaining that their child is seeing an awful lot of something, it is the content moderators who should be empowered to escalate that. Samaritans Ireland has approximately 60 years of experience in looking after our volunteers. We care for them and we have formal debrief procedures, informal peer support procedures and rotations so that they are not doing the same patterns all of the time. That is partly for the mental health of our volunteers but it is also because they are better able to support others if they are not burned out and if they are in a better place.

In the past, we have brought some of this experience to bear. We have been funded by the National Office for Suicide Prevention, NOSP, to work with other front-line staff with some of these techniques. It is important that this is part of the experience of content moderators and that the regulation of this industry recognises that there is a specific health and safety risk around the mental health issue for the content moderators. It should be regulated in that manner. In the same way one would regulate an industry with toxic chemicals or health safety passes, this regulation should include this particular risk and it should be legislated for. We have guidance on that issue, which Ms Hamra might talk about, as well as talking about the algorithms.

Ms Louise Hamra: In the briefing that was circulated we referenced that we have ten guiding principles that were designed in collaboration with academics and industry. They essentially outline the ten best principles that should be adopted to make the Internet a safer place. Regarding the moderators, our tenth principle is specifically concerned with looking after the well-being of people who come into contact, especially over an extended time, with this difficult content that involves aspects such as self-harm and suicide. We are very aware of the profound impact that experience can have on these people and on their ability to appropriately moderate content. It could mean that, in turn, things could fall through the net and content might become available on the Internet which would have been moderated if the moderators themselves had been in a better head space and able to limit the prevalence of such content.

The algorithms are also referred to in our principles. Mr. Moore mentioned that it even comes down to search terms. We are lucky in the sense that some of the platforms have instigated measures whereby typing in certain keywords, such as “suicide” or any other problematic and potentially dangerous terms, will cause our or another helpline to immediately pop up.

Anyone searching that content, therefore, will know immediately that help is available to them. Therefore, this is not only about minimising the amount of harmful content, but also about maximising knowledge regarding the supports which are available to people in this context and making those supports readily accessible at those times when people may be experiencing periods of difficult mental health.

Chairman: I thank Ms Hamra and Senator Warfield. I call Deputy Mythen.

Deputy Johnny Mythen: As politicians, sometimes we receive the same types of phone calls as the witnesses' organisation because people turn to us when they are in these situations as well. I have experienced it, but I was never trained in this regard, unfortunately. It is a serious situation and I thank the witnesses and their organisation for the work being done. It saves lives every day of the week and it is really important.

I have a few questions. How important is it that individual complaint mechanisms should be included in this Bill? I ask this because I attended a webinar yesterday in which Mr. Peter Tyndall, the Ombudsman, Dr. Karen McAuley, the head of policy-making for the Ombudsman for Children, and Ms Noeleen Blackwell, the chief executive officer of the Dublin Rape Crisis Centre, all participated. It was chaired by Ms Jillian van Turnhout. All those people insisted on the importance of an individual complaints mechanism, but it is not currently included in the Bill. The point made was that making individual complaints possible might allow systematic occurrences in this regard to be observed. The data could be extracted in that context and it would be very valuable to the bodies working in this area. I ask the witnesses to comment on that aspect.

The witnesses also outlined how important signposting is for people who have viewed harmful content online. Can more detail be given regarding how that process should work and what such a mechanism would look like? In addition, what mental health and well-being supports do the witnesses think should be in place for the workers who must respond to reports of online abuse? Often, the people on these platforms are just normal people like ourselves, but then they must deal with these difficult situations as well.

Chairman: I thank Deputy Mythen. I call Mr. Moore.

Mr. Ciaran Moore: I thank Deputy Mythen for his questions. I will deal with the first and third of those questions, and then I will hand the query regarding signposting over to Ms Hamra. She is our policy officer and will be aware of our stance on this matter.

We have had discussions with some of the other people who have looked at the independent complaints mechanism. One key point is that the various kinds of content are very different. For example, if we are talking about child abuse and-or image-based sexual abuse, those are illegal contents and the problem is that such content is not being taken down quickly enough. The content that we deal with, however, is not illegal content that presents harm to specific users. However, one of the things that concerns us regarding a potential complaints mechanism is how such complaints would be acted on and how content would be taken down. I state that because often people posting material about self-harm, for example, or survivors talking about their own suicide attempts, are themselves very vulnerable. We support the proposal, therefore, that there should be a mechanism to manage content online and we think there are different types of such content. However, we also think that any such complaints mechanism must take account of the impact of how it will work and who will take down the material.

The other aspect, and we have talked to several groups about this issue, concerns the scope of such a mechanism and who would be covered by it. It is one thing to say that we can engage with getting material down off Facebook, but some of the content we see tends to be driven into very specific forums. Therefore, it tends to be less visible and perhaps present in less regulated spaces. In that regard, we would be a little concerned about whether it would be possible to get everywhere on the Internet to undertake this type of endeavour and also about the resulting impact. We are supportive of the broad thrust of the arguments being made by the Children's Rights Alliance and other groups, but a great deal of detail is involved when we get to the level of considering differences between legal and illegal content and different websites.

Turning to mental health supports, we believe some basic good practices that we have in place with our volunteers are important. At the core of those is the ability to debrief. I refer to a formal debrief at the end of a duty period. If someone is particularly concerned about something, he or she can then say that and someone will be on hand to talk that through with the person concerned. It is an element of peer support. We understand that a great deal of this work is highly confidential, but we deliver a fully anonymous and confidential helpline. To be able to do that, it is necessary to provide somewhere to allow people to talk about what they have experienced within that confidential sphere. It would not be right for people in that situation to go home and tell others about what had happened to them, but those experiences will sit with the people concerned until they have been able to deal with them.

Some aspects of this type of situation concern the work structure. Training aspects are definitely involved and we give training to a whole range of people who take calls. For example, we talk to the people who take calls for the Dublin Fire Brigade. During the recent lockdown, we also engaged with several other groups that found it difficult and with staff who found it difficult to work from home while receiving these difficult calls. I refer to groups that in the past might have provided more general supports, but that are now interacting with suicidal callers. Much of the training in this regard involves learning how to deal with specific content, learning what the role itself involves and what it is okay to say in that regard. That is where the issue of transferring on something arises.

People are often looking at content of this nature and are shocked by it. It is important that the environment in which those people work is supportive and that they are empowered to take space for themselves for the good of their own mental health and to escalate issues they have identified. I state that because it is often these people who see the problems and we are asking them to clean up the Internet for us. If they are working in an environment where they do not feel that they can report a problem, then that problem will remain and sit with those people. I will hand over to Ms Hamra to address the issue of signposting.

Ms Louise Hamra: I might also extend the point to include looking after the moderators. The moderators in a team are likely to take the brunt of viewing this difficult content. However, anyone else who might come into contact with that content should also receive the same type of well-being supports. It should be ensured that there are check-ins and specialist training in this regard, for example. The number of people who must see and moderate this type of problematic content in a work setting should be kept as small as possible.

Regarding signposting, I mentioned that some platforms have already adopted a mechanism whereby searching for certain keywords will automatically bring up our 116 123 helpline number for immediate support. It is important that websites should also be signposting contact details for other emergency services and other supports, and especially more targeted supports which may be available 24-7. Users should also be encouraged to contact trusted family mem-

bers and friends. The key point is that people are encouraged to reach out to someone, even if they do not feel the situation has reached the extent where the emergency services may be required. People in these types of situations should be supported and encouraged to say something to someone.

Chairman: I thank Ms Hamra. I think all my colleagues have had an opportunity now. I thank Mr. Moore and Ms Hamra for being with us today, making their presentations and comprehensively answering our questions. I wish to ask them a little about their explicit call for the measure to include or address the inappropriate display or prevalence of content with a risk of harm. Could Mr. Moore extrapolate on that a little further?

Mr. Ciaran Moore: We had focused on the section in the general scheme of the Bill in which reference is made to online harms and content that is there with the intention to promote suicide and self-harm. We felt this was the wrong approach. For a start, these are not illegal harms, so the question of intent should not really arise because that is an idea in criminal law. More significantly, however, the content quite often could be posted with good intentions. It is a question of how it is used and how the harm is created. We have a lot of experience of this and of testimonials and signage in specific places. We engage with communities on putting up appropriate signage and so on. We know that people quite often want to engage with content relating to suicide and want to put up helpful content, but they might say the wrong thing or put it in the wrong way. What we have is a set of guidelines on how to assess the harm and identify the impact on people. Quite often that impact is a question of how frequently people see the content. We believe it is not necessarily the case that one piece of content or one post in itself is always wrong but rather that there should be restrictions on how it is spread around in order that potentially harmful posts or content can be identified. That way, it stays within a friend circle and cannot be passed on further and a testimonial to a dead teenager or dead child can be there and be valued by that local community. We know there are pages which collect these testimonials. We would say, "Look at how impactful you would be if you were to consider this." We think that that secondary use of some of the content is important to avoid.

Chairman: That brings us to the conclusion of our meeting. I thank both witnesses for being with us, for their comprehensive presentation and for their willingness to share their thoughts and views. The next meeting of the joint committee will be held on Wednesday, 21 July, at 10 a.m. - a bit of an early start compared with our usual midday slot - when we will continue our pre-legislative scrutiny of the online safety and media regulation Bill with representatives from Safety Over Stigma. That will be followed by a session with the Office of the eSafety Commissioner of Australia. Then we will have a private session at the end of that meeting via Microsoft Teams.

The joint committee adjourned at 5.13 p.m. until 10 a.m. on Wednesday, 21 July 2021.