Opening Statement of An Garda Síochána to The Joint Oireachtas Committee on Tourism, Culture, Arts, Sport and Media

Wednesday, 26th June 2024, at 1.30pm

'the State's response to online disinformation and media/digital literacy, including social media and fake news.'

Cathaoirleach, Committee members, Good Afternoon.

Thank you for the invitation to attend here today to discuss this very important issue.

I am Assistant Commissioner Cliona Richardson representing An Garda Síochána and I am joined today by my colleague Detective Chief Superintendent Barry Walsh, who is responsible for our Garda National Cyber Crime Bureau.

While not wishing to encroach on the responsibilities and remits of the other State Agencies here today, An Garda Síochána continues to have concerns regarding the use of both misinformation and disinformation through the use of social media platforms. Many times we have seen the influence of false or misleading information, and the effects it can have on our communities, requiring a policing response.

An Garda Síochána has in the past, had to resort to issuing statements regarding inaccurate information circulating online. Most recent examples include false claims that properties are to be used as accommodation centres and are subsequently targeted in arson attacks. An Garda Síochána has commented publically on the challenges of the circulation of completely inaccurate information about properties and on the potential for serious harm arising from same; including risk to life to occupants, such as construction workers and/or security persons who could be inside any such property. Gardaí are continuing to investigate a number of arson attacks and attempts to damage buildings that were falsely rumoured to be intended for use to house migrants, as well as some buildings that were in-fact intended for use as refugee accommodation.

An Garda Síochána condemns, in the strongest terms, any such criminal activity and will fully investigate same in every circumstance.

Another recent example includes the allegations of a sexual assault on a child by a number of men residing at an accommodation centre in Kildare, which were completely untrue. These false rumours were widely circulated and also shared by a number of agitators. Following the posting of comments on social media, a group of protesters gathered at a hotel housing migrants in Kildare, during which Gardaí were verbally abused while also being targeted with fireworks and other missiles.

Coupled with the above examples, An Garda Síochána continues to receive concerning reports of online abuse from members of the public including politicians, celebrities, journalists and Gardaí which were instigated by disinformation means. These reports generally include posts which are abusive/threatening or harmful to the individual.

Each report is fully investigated by An Garda Síochána for criminal offences. These offences can include offences relating to, but not limited to:

- Harassment, Harmful Communications and Related Offences Act 2020
- Non-Fatal Offences Against the Person Act, 1997

- Prohibition of Incitement To Hatred Act, 1989
- Child Trafficking and Pornography Act, 1998
- Criminal Justice (Theft and Fraud Offences) Act, 2001
- Criminal Justice (Offences Relating to Information Systems) Act 2017
- Criminal Damage Act, 1991

As more and more social media platforms transition towards the use of end-to-end encryption it is becoming increasingly difficult for law enforcement and prosecution agencies to process requests for disclosure on accounts used to post abusive or hatred-inciting disinformation online. The end product of this focus on privacy by social media companies is that the perpetrator of crime is afforded more protection than the victim with a readymade platform to pursue their activity or spread disinformation, with significant access barriers created for them to hide behind.

It is respectfully submitted that any successful response to the spread of disinformation, via social media or any other online communication sources, can only be achieved as part of a combined societal response, which includes Law Enforcement Agencies, Government Agencies and the social media platform providers themselves. Without this joint approach, any response is highly likely to be largely reactive and limited in its effectiveness. At the same time, part of any response must be built on an appropriate reporting and restricting response from the providers and the public who encounter incidents of disinformation that are clearly identifiable as such.

Proactive physical monitoring of social media platforms will not always be a possibility for law enforcement agencies, including An Garda Síochána, given the variety and volume of messages and postings. Ongoing, meaningful, engagement with social media platforms is essential if the policing response to disinformation is to be effective ensuring timely and appropriate proactive reporting and that disinformation content removal processes are in place and observed.

At the same time, it is imperative that An Garda Síochána continues to harness its positive relationship with the public to foster an environment of both engagement and reporting, where users are willing and eager to report incidents of disinformation or abusive content to us for appropriate investigative action.

In some cases, incidents of disinformation, which have been spread via social media and clearly constituting fake or false news with a motivation to confuse, create division or sow seeds of public protest, have acted as a catalyst for physical acts that been criminal in nature. From the perspective of An Garda Síochána, there is an inherent difficulty in addressing such disinformation in advance of that physical manifestation. This is because, these postings may not be illegal in terms of content, despite it clearly being disinformation and, indeed, a call to protest, based on disinformation, may not be illegal in advance; unless it is clearly designed to create hate towards a person or social group, an ethnicity or religious community or a minority group within the community which could amount to a criminal offence.

Removal of material is most commonly achieved via a request to the service provider. Even in circumstances where the post or message is disinformation, it may not actually breach any law. In circumstances where it does breach a Statute, a Garda investigator may seek removal which can be achieved by submitting a written notice or request. Compliance with any such request is entirely a matter for the applicable service provider, and An Garda Síochána has no power of compellability that is immediately available for use.

From a criminal investigation perspective, some limitations can arise when it comes to An Garda Síochána's ability to investigate sources of disinformation or false postings on social media. In order

for An Garda Síochána to initiate a criminal investigation, there must firstly be a criminal offence in this jurisdiction or an element of an offence that is being investigated here so that the member can apply to the court for an order compelling disclosure of relevant evidence. That is not always the case. Such limitations may also apply if the posting originated outside the jurisdiction, and is merely hosted on a platform headquartered within the State. While the posted disinformation may be accessible within the State it may refer to an event, person or organisation outside the State and as such it might not be possible to seek an order to disclose subscriber details in this case without a request to do so from an appropriate authority where the affected event, person or organisation is domiciled.

A recurring difficulty within engagement between An Garda Síochána and social media service providers is the preservation and disclosure process around seeking account and content data from social media platforms used to post disinformation or illegal and abusive content online. While many of the providers have effective online methods for requesting preservation of accounts, serving court issued orders to disclose and receiving the content in response; others do not or the rules imposed are subject to regular change. Most service providers will state that account content data can only be accessed via legal applications within the Jurisdiction where they are headquartered. This necessitates use of the Mutual Legal Assistance process, which can delay access to evidential information for up to 12 months or more.

As mentioned, encryption is becoming an increasing difficulty when it comes to disinformation as many of the social media platforms now operate end-2-end encryption and state that they cannot provide copies or content data for the account. So while it is possible to seek subscriber details, it may only be possible to obtain a copy of the posted disinformation from a third party or by way of downloaded screenshot.

All of the afore-mentioned do present difficulties for An Garda Síochána when it comes to securing removal of posted disinformation, and when required, in investigating offences arising. However, they are not insurmountable and do not deflect from the organisational enthusiasm to ensure such cases are robustly investigated, to work closely with service providers, the global law enforcement community and the public to monitor content, gather intelligence and, in every circumstance where the option is available, to effect the removal of disinformation posted to social media accounts and platforms.

Social media platforms have asserted that they take their responsibility to block or remove disinformation on their respective platforms seriously and that they are taking ongoing steps to combat the spread of disinformation and fake news on their platforms. However, such actions are also predicated on their stated obligation to facilitate the free expression of information and the right to freedom of speech enshrined in the constitutional and rights protections in place in most countries.

That removal response has been subject to some well publicised commentary of late. This has called into question the effectiveness of some platforms' reaction to requests to remove materials and to effectively identify material which very clearly requires removal. At the same time, citing privacy and freedom of expression protections as a rationale for allowing disinformation or the continuation of postings that are clearly offensive, abusive or threaten public well-being and peace, is not, from An Garda Síochána's perspective, realistic nor defensible.

An Garda Síochána considers it incumbent upon social media providers to ensure that material disseminated over their platforms is appropriate for its recipient audience and has been effectively considered for accuracy.

The online environments that are now part of our everyday lives can be exploited by a multitude of sources to commit various crime types. Technology is also evolving, with advances in Artificial Intelligence (AI) and Large Language Models. These advancements in technology have the potential to significantly alter the form that disinformation takes. A simple search on the internet will provide a range of fake videos showing politicians and public personalities skiing, endorsing products or making pronouncements that are entirely false. It is not unrealistic to suggest that AI could be used by motivated people and groups to create similar videos that are then used to falsely reinforce their message or appear to show content that backs up their claim or shows purported opponents or influential public personalities supporting what they claim.

An Garda Síochána's mission statement is 'Keeping People Safe', and this includes the online environment. An Garda Síochána utilises a range of social media platforms in support of this organisational mission. We have a very active engagement programme across all the primary social media platforms. We also utilise public events as a mechanism to highlight the reality that there is misuse of social media to spread disinformation and the need to report in order to enable the safety of all users. Coupled with this, An Garda Síochána continues to work closely with key stakeholders with the goal of keeping people and businesses safe online.