Joint Oireachtas Committee on Justice Opening Statement

13 February 2024

Garda Commissioner Drew Harris

I wish to thank the Committee for inviting me and my colleague Garda Chief Information Officer Andrew O'Sullivan here today.

Every major criminal investigation now involves processing digital evidence. This evidence often take the form of images or footage obtained from seized devices or CCTV. Two separate judgments from the Court of Appeal recently confirm that Gardaí have a duty to process available footage to identify or exclude suspects. In dismissing the respective appeal cases of Freddie Thompson and Philip Dunbar, the Court's rulings were instructive in terms of the balance between a suspect's right to privacy and the human rights of the victim.

Digitalisation in society has led to an explosion in the volume of digital footage as evidence. The footage from the 23 November riots runs to 22,000 hours. Individual murder investigations can have upwards of 50,000 hours of footage. Seized devices can have over a million images of child sexual abuse.

The key to these cases may just be in a few frames out of millions. A child's school uniform crest can help to identify the victim. The importance of brief footage in a murder investigation that places Freddie Thompson in a particular make and colour of vehicle at a relevant time and place.

Digital evidence that Gardaí have a duty to process is now at Big Data scale in terms of its massive volume, complexity of formats and the rate at which it is generated. Digital crime and evidence can only be investigated with digital tools. Manual processing by Garda personnel sitting at screens is becoming unfeasible and ineffective. In the case of child sexual abuse material, which is the rape of children and every form of sexual depravity that can be visited on a defenceless victim, there is the traumatic impact on Garda members viewing the material. A number of members of An Garda Síochána are on long term sick leave due to the trauma of viewing these images, which can never be unseen.

In order to be effective at fulfilling our mandate to protect victims, investigate crime and vindicate the human rights of citizens in a digital society, An Garda Síochána must have access to modern digital image analysis and recognition tools.

There is understandable public concern and some confusion about AI technology. I wish to clarify that digitalisation in An Garda Síochána means that electronic tools act only as a support for decisions taken by Gardaí. There is no question of autonomous machine decision making, ever. All decisions that can impact on a person are only taken by identifiable and accountable personnel. This decision support approach is already used. People make the final decision on driver penalty notices issued initiated by Go Safe vans, the 600,000 vetting applications processed annually, the use of technology to flag uninsured vehicles and the existing use of biometric processing in

online abuse cases. We have outlined the wider set of use cases where we need to apply image analysis and recognition technology. It is worth noting that only one of these use cases involves actually attempting to identify people. Most of them involve searching or sifting massive amounts of evidence for material that is relevant. The successful use of decision support tools by Garda witnesses has never been successfully challenged in criminal trials.

An Garda Síochána has invested significantly in digital policing, including the in house expert professionals required to build and manage the underlying technology and data. This had directly contributed to the effectiveness of major investigations as well as establishing our reputation for high quality data, as confirmed by the CSO in October 2023.

The reliability of biometric decision support tools is demonstrated by the success of the Garda National Cyber Crime Bureau in detecting and prosecuting online abuse cases, often as part of transnational investigations. The 99%+ accuracy of modern biometric identification systems is clearly demonstrated by the bi-annual review by the U.S. National Institute for Standards and Technology (NIST). We intend to follow the practice of European law enforcement partners in using the NIST ratings to select the best available technology.

There must be safeguards but these should be proportionate to the risks involved in the specific use cases.

In summary, extending the already accurate, reliable and safe usage of image analysis and biometric identification technology beyond abuse cases to other serious criminal investigations is essential for An Garda Síochána to keep people safe in a rapidly changing digital society, to counter emerging threats and to meet our obligations to work with European law enforcement partners to counter Transnational Organised Crime.