Policing Facial Recognition Technologies
Expert briefing note
10 May, 2023

The current landscape of facial recognition technologies is very uncertain. As the risks, biases and harms attached to this specific type of AI have become apparent, large tech companies including Microsoft, IBM and Amazon have backed away from selling it to police. Axon, one of the largest manufacturers of police body cameras in the world, has refused to sell it. The use of this technology without proper democratic care can also be very destabilising politically. In the Netherlands, use of AI to detect fraud was brought to an immediate halt by the courts. In this context, it is apparent that the hopes and trusts some have in the promise for policing AI don't line up with the reality of its functions, including its risks and harms.

In light of recent media coverage pointing to officials' support of ever expanding uses by An Garda Siochana of facial recognition technologies (collectively, policing FRT), experts will brief officials on FRT in the **Oireachtas AV Room on Wednesday, 17 May, 2023 from noon until 1pm.**

In anticipation of that meeting we detail here our concerns, alongside the democratic and technical requirements necessary for use. These requirements would apply, in particular, to the government's stated intention for the Gardai to use real-time *or* retrospective biometric facial recognition either through a last-minute amendment to the Garda Síochána (Recording Devices) Bill *or* to stand alone legislation.

A. EXPERTS' ONGOING CONCERNS

Policing technology must meet rule of law and democratic requirements. We have concerns regarding a lack of due diligence, conflicts with forthcoming EU law, and the lack of engagement with current evidence and ongoing calls for bans. Proposed use cases promote mass surveillance

which do not meet the test of strict necessity in a democratic society or respect the presumption of innocence in criminal matters.

Due diligence

In expressing their commitment to the use of policing FRT, officials in Ireland have omitted a number of important first steps and acknowledgement of existing positions which require attention for the sake of due diligence. These include in particular:

- As of April 2023, the Office of the Data Protection Commissioner (DPC) advised members of this group that the State has not yet met its statutory obligation to formally consult with the DPC;
- The Minister for Justice has not published, as agreed, a Cabinet report on the matter; and
- In their pre-legislative report (p8) on the Recording Devices Bill, the Joint Committee on Justice specifically recommended that FRT not be used by members of An Garda Síochána.

Conflict with EU law

The government's stated intention for the Gardai to use real-time biometric facial recognition may come into direct conflict with the forthcoming AI Act. Article 5 of the current version prohibits the use of real-time biometric identification systems in publicly accessible spaces, with no exceptions. It also prohibits analysis of recorded footage of publicly accessible spaces through 'post' remote biometric identifications systems without pre-approved judicial authorisation.

Current evidence of policing FRT bias and harms

The evidence is not outdated. There is current, significant and robust scientific evidence demonstrating accuracy and bias concerns. See in particular:

- 2022 research into racial bias
- 2018 research into development, and
- 2022 audits of deployment practices.

Bias exists particularly for darker skinned people. Innocent people have been arrested by police relying on this flawed technology. Literature recently cited by the government in relation to FRT and static portraits have no application to their proposed use cases.

Ongoing expert and official calls for bans

While some EU states use policing FRT, this fact alone is not reason for Ireland to follow the example. Calls for bans from expert authorities and officials are an increasing norm:

- The European Data Protection Board and European Data Protection Supervisor have called for a ban on the use of FRT in public spaces,
- The UN has called for a moratorium on the sale and use of artificial intelligence systems like policing FRT that pose significant risks to human rights, and
- In Ireland, the Joint Committee on Justice specifically recommends that FRT not be used (see p8) by members of An Garda Síochána.

In other jurisdictions officials have begun to acknowledge such calls and ban use of FRT for law enforcement. There are significant concerns from civil society organisations around the world.

Mass surveillance

That people are able to record the police with their phones is a democratic accountability measure. It does not presume that the Gardai should be capable of mass surveillance of the Irish public. Equipping body worn cameras with FRT turns the original purpose of body worn cameras on its head: Holding police accountable to the public. Instead, this use would turn gardai into roaming surveillance units, in defiance of the presumption of innocence required for criminal matters. It would permit pervasive monitoring of the public without their knowledge or consent in defiance of the legal requirement of strict necessity.

B. DEMOCRATIC REQUIREMENTS

While experts have provided recent evidence of bias and harm, the Irish State has in turn not met its evidentiary obligations for requirements in relation to privacy, data protection, consultation, and demographic impacts.

Privacy requirements

Privacy is a fundamental right that should be firmly supported by our officials. Our rights are enshrined in law and can only be limited in manners that are strictly necessary in a democratic society compared to less intrusive measures. To meet this standard, the State will need to demonstrate scientifically verifiable evidence:

- In the form of Ireland-specific data to inform the legal test of 'necessary in a democratic society';
- Of whether it has identified less intrusive alternative measures and proven that FRT is strictly necessary compared to these measures using scientifically verifiable evidence;
- That the chosen policing FRT use cases do not disproportionately limit the privacy and other human rights of affected persons, including those who are misidentified or impacted by unwarranted intrusions; and
- That they have pre-established minimum thresholds to be met for the FRT system's accuracy (precision, false positive rate, true positive rate) to inform the legal test of strict necessity for personal data processing.

Data protection requirements

The State has an unfortunate record on personal data protection such that it is not clear if it is capable of meeting its requirements for policing FRT. Significant legal problems have resulted from the State's approach to policing technologies including data retention and CCTV schemes. The State Public Services Card was also found to be illegal by the DPC in many aspects in relation to its data sharing practices, while the DPC's investigation of the Department of Social Protection's facial recognition practices is ongoing. Therefore, before committing to FRT use, at a minimum the State will need to demonstrate that:

- FRT databases will not be collected through private facial recognition databases;
- Procurement contracts and data-sharing agreements with other parties are published;
- Clear measures enabling data subjects to exercise their rights including the rights to rectification, erasure, and object with clear justifications if exemptions apply; and

- Clear, objective, and limited criteria are established concerning third-party access to the data collected or retained, including what data can be shared, with whom it can be shared, and for what specific purpose it can be shared.

Consultation requirements

The State will need to meet democratic consultation requirements designated for risky surveillance technologies like policing FRT. If they choose to proceed with policing FRT, in particular they will need to provide:

- Published evidence of the State's transparent, proactive consultations with civil society and independent experts on the particular types of policing FRT they intend to use;
- Published evidence of clear, proactive processes for the public, especially marginalised communities indicated in the literature as being at increased risk of bias, to influence how FRT is implemented; and
- Published outcomes explaining their reasons if expert advice is not followed and/or community views are disregarded.

Demographic requirements

It is insufficient to provide research trials and training datasets from bodies that are in favour of using policing FRT (for e.g., members of An Garda Siochana). Rather, given the clear evidence of demographic impacts against marginalised groups, it is incumbent on the State to carry out and publish evidence of:

- An equality impact assessment;
- The demographic makeup of the populations where FRT will be deployed;
- For each individual deployment of FRT use case, the demographic data for arrests, stop and searches, and other outcomes resulting from the use of FRT;
- The demographic makeup of the training dataset to ensure the dataset is representative of the population where it is to be used; and
- The evaluation of their FRT use case performance across demographic groups, in different conditions that match FRT's operational use, to ensure FRT performs well and similarly across the population.

C. TECHNICAL REQUIREMENTS

The State's ability to meet its democratic requirements is also contingent on its capacity to enable independent technical evaluation of the technology and appropriate training for its officers. This may not be possible if An Garda Siochana enter a partnership with a private institution whose technology is not transparent. We explain here the meaning of FRT and the independent tech evaluation and safeguards required, including minimal technical capacity requirements of An Garda Siochana.

What is FRT

While the State has not identified explicitly its intended uses for policing FRT, but mentioned some use cases that we assert would not be lawful, we provide here a quick primer on the meaning of terminology:

- **Facial recognition technology (FRT)**. A system that tries to match a human face from a digital image (biometric data) such as a video frame, typically against a database of faces.
- **Biometric data**. Legally defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (hand or footprint) data. **A person's face** is a unique identifier. It is a form of biometric data permanently and irrevocably linked to a person's identity.
- **Real-time FRT**. FRT that is used in 'real time' or live scenarios for biometric identification.
- **Retrospective FRT**. Images available following real time identification, i.e. applying an FRT system to footage previously collected.

The use of FRT in real-time and retrospective scenarios *both* represent a major interference with people's fundamental rights. The European Parliamentary Research Service states in its report at p55 that the risk of persistent tracking and its associated adverse impact on rights and democracy, in respect of retrospective use of FRT, are "at least equivalent" with those of real-time FRT. It says:

> "As the images potentially available for 'post' remote biometric identification of natural persons are actually more numerous than those available at any point in time for real-time identification, they should also make it possible to draw a much more complete picture of the activities of any individual, thus representing a major interference with their fundamental rights.

Independent technical evaluation requirements

Independent tech evaluation and safeguards will be required of the State for policing FRT, irrespective of whether the technology is public or proprietary. These include:

- Deployment of independent audits;
- Giving independent auditors access to training dataset and models to in order to audit them;
- Outlining safeguards precluding the use of FRT with unsuitable low-quality images;
- Carrying out performance tests (i.e. precision, false positive rate, true positive rate) across demographic groups; and
- Documenting non-operational research trials of FRT with informed consent from participants before the operational use of FRT for policing.

If the State is precluded from deploying these evaluations and safeguards because a chosen technology is proprietary, then the police should not use that particular technology.

Technical training requirements for officers

The State has not, to date, provided evidence of sufficient training for officers in respect of existing technologies. For example, the DPC previously found Gardaí operating a CCTV scheme were "unaware of the full range of technical features of their own CCTV system" (see p67). It is unclear to experts how the State meets these requirements for policing FRT. We ask:

- What plans the State has for training for the particular type of FRT mandated for An Garda Síochána officers using the technology; and
- For the State's publication of clear standards for technical training on using FRT, data protection training, and training on risks including differential treatment, function creep, and

unwarranted intrusions as developed transparently and in consultation with experts and impacted communities.

In conclusion, we support the need to resource the guards, to embrace the digital transformation, and to invest in new technologies. However, we do not support the uptake of policing FRTs. The risks to legality, fundamental freedoms, marginalised groups, and democratic structures are too great.

Signed,

Dr Elizabeth Farries, Director, UCD Centre for Digital Policy

Olga Cronin, Senior Policy Officer, Irish Council for Civil Liberties

Dr Ciara Bracken-Roche, Assistant Professor, Maynooth University School of Law and Criminology

Professor Barry O'Sullivan, FAAAI, FAAIA, FEurAI, MRIA; Director, Insight SFI Research Centre for Data Analytics, School of Computer Science & IT, University College Cork; Director, SFI Centre for Research Training in AI; Past President, European Artificial Intelligence Association; Vice Chair, European Commission High-Level Expert Group on AI (2018-2020)

Abeba Birhane, Senior Fellow in Trustworthy AI at Mozilla Foundation and Adjunct Assistant Professor at TCD.

Dr TJ McIntyre, Associate Professor, UCD Sutherland School of Law and Chairperson, Digital Rights Ireland

Professor Michael Madden, Established Professor of Computer Science, Head of School of Computer Science and Head of Machine Learning Research Group, University of Galway

Further reading

- 02 June 2022 Open letter to Irish Times - FRT concerns from 7 Universities and 13 NGOs
- 20 June 2022 Expert letter to Oireachtas Cabinet Members
- 18 April 2023 Opinion Editorial in the Irish Times
- 13 April 2023 Expert Letter to Data Protection Commissioner (Contact digitalpolicy@ucd.ie for a copy)

For Inquiries

Dr Elizabeth Farries Director, UCD Centre for Digital Policy elizabeth.farries@ucd.ie	Olga Cronin Senior Policy Officer, ICCL olga.cronin@iccl.ie
Dr Ciara Bracken-Roche Assistant Professor, Maynooth University School of Law and Criminology ciara.brackenroche@mu.ie	Professor Barry O'Sullivan, FAAAI, FAAIA, FEurAI, MRIA; Director, Insight SFI Research Centre for Data Analytics b.osullivan@cs.ucc.ie | 086 8035550

Dr TJ McIntyre, Associate Professor, UCD Sutherland School of Law and Chairperson, Digital Rights Ireland tjmcintyre@ucd.ie (available after 15 May)	Professor Michael Madden School of Computer Science, University of Galway michael.madden@UniversityOfGalway.ie, +353-86-7952802