Tithe an Oireachtais
Houses of the Oireachtas

An Comhchoiste um Dhlí agus Ceart

Tuarascáil maidir leis an nGrinnscrúdú Réamhreachtach ar Scéim Ghinearálta Bhille an Gharda Síochána (Feistí Taifeadta) (Leasú), 2023

Feabhra 2024

Joint Committee on Justice

33/JC/52

Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023

February 2024

Table of Contents

CATHAOIRLEACH'S FOREWORD

In December 2023, the Minister for Justice, Ms. Helen McEntee TD, forwarded the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023 to the Joint Committee on Justice in accordance with Standing Orders for the purpose of pre-legislative scrutiny.

The Committee welcomed the opportunity to conduct pre-legislative scrutiny on this important legislation and noted comments made during its engagements that, in legislating in this area, Ireland has the opportunity to set an example of best practice and ensure that the legislation includes robust safeguards and oversight mechanisms.

While acknowledging that the introduction of facial recognition technology would bring significant benefits for law enforcement agencies, through saving Garda resources and time and assisting in the processing of complex digital evidence, the Committee equally recognises that any introduction of this technology must be balanced against the potential long-lasting and serious impacts it may have on human and fundamental rights.

In undertaking pre-legislative scrutiny, the Committee has sought to scrutinise the proposed legislation and provide recommendations on areas where it believes change or amendments are warranted. Among the areas identified for further examination within the General Scheme include: concerns in relation to the impact of biometric identification technology on human and fundamental rights; concerns with the accuracy of this technology and the potential for racial bias; and comments in relation to provisions on the power to use the Biometric Identification [Head 4] and the Application for Approval of this technology [Head 5].

The Committee has made a number of recommendations and a copy of this report and recommendations will be sent to the Minister for Justice. I would like to express my appreciation to all the witnesses for their contributions and to the Members of the Committee for their work on this subject.

Finally, I hope that this report will help to inform the legislative process and make a valuable contribution to the forthcoming legislation.

James Lawless TD (FF) [Cathaoirleach]
February 2024

COMMITTEE MEMBERSHIP

Joint Committee on Justice

Deputies

James Lawless TD (FF) [Cathaoirleach]

Colm Brophy TD
(FG)

Patrick Costello TD
(GP)

Alan Farrell TD
(FG)

Pa Daly TD
(SF)

Aodhán Ó Ríordáin TD
(LAB)

Mark Ward TD
(SF)

Thomas Pringle TD
(IND)

Niamh Smyth TD
(FF)

Senators

Robbie Gallagher
(FF)

Vincent P. Martin
(GP)

Michael McDowell
(IND)

Lynn Ruane
(IND)

Barry Ward
(FG) [Leaschathaoirleach]

Notes:

1. Deputies nominated by the Dáil Committee of Selection and appointed by Order of the Dáil on 3rd September 2020.
2. Senators nominated by the Seanad Committee of Selection and appointed by Order of the Seanad on 25th September 2020.
3. Deputy Jennifer Carroll MacNeill elected as Leas-Chathaoirleach on 6 October 2020.
4. Deputy James O'Connor discharged and Deputy Niamh Smyth nominated to serve in his stead by the Fifth Report of the Dáil Committee of Selection as agreed by Dáil Éireann on 19th November 2020.
5. Deputy Michael Creed discharged and Deputy Alan Farrell nominated to serve in his stead by the Fifteenth Report of the Dáil Committee of Selection as agreed by Dáil Éireann on 28th June 2022.
6. Deputy Brendan Howlin discharged and Deputy Aodhán Ó Ríordáin nominated to serve in his stead by the Nineteenth Report of the Dáil Committee of Selection as agreed by Dáil Éireann on 8th November 2022.
7. Deputy Jennifer Carroll MacNeill was discharged, pursuant to Standing Order 34, on 21st December 2022.
8. Senator Barry Ward was elected as Leas-Chathaoirleach at the Committee meeting on 15th February 2023.
9. Deputy Colm Brophy nominated to serve on the Committee by the Twenty First Report of the Dáil Committee of Selection as agreed by Dáil Éireann on 7th March 2023.
10. Deputy Martin Kenny discharged and Deputy Mark Ward nominated to serve in his stead by the Twenty-Third Report of the Dáil Committee of Selection as agreed by Dáil Éireann on 26th April 2023.

COMMITTEE RECOMMENDATIONS

The following recommendations were made by the Committee in relation to the topic:

1. The Committee recommends that the rationale for introducing Facial Recognition Technology (FRT) be published in parallel with the progression of this legislation, for the information of all stakeholders.

2. The Committee notes the supply of key use cases to the Committee by the Garda Commissioner during the hearings and recommends that clarity is provided as to the intended use of FRT. The General Scheme is drafted to allow comparisons to databases, however the Garda Commissioner stated to the Committee: “It is not our intention to run images against a database”. The Committee believes that redrafting is needed to provide clarity.

3. The Committee recommends that the legislation must provide further clarity under Heads 2 and 4, on the data sources or reference database that will be used as part of this legislation and that very strict controls should be put in place in relation to the use of additional databases.

4. The Committee also recommends that an Garda Síochána (AGS) and the Department of Justice must urgently clarify some of the following details regarding the database: if it is the intention to provide access to databases; what database they intend to use in respect of retrospective FRT; the source of the database; how a database would be populated if they are to make their own; and the criteria for adding anyone to that database.

5. The Committee recommends that the legislation should provide for a periodic, independent, judge-led review, of all use of biometric identification, based on legislatively defined operational criteria.

6. The Committee recommends that the draft legislation must be compatible with EU law in order to be robust and immune to challenge and to protect victims of crime.

7. The Committee recommends that, to allay the concern by some witnesses and to maintain public confidence regarding the accuracy of FRT and noting that the technology has matured in recent years since some of the earlier testing was performed, the ongoing concern about accuracy must be addressed by the Minister for Justice.

8. The Committee recommends that, to allay the concern by some witnesses regarding potential discrimination in the operation of FRT and to maintain public confidence, the ongoing concern about discrimination or inherent bias must be addressed by the Minister for Justice.

9. The Committee recommends that the legislation should provide for an annual independent audit of the use of biometric identification by AGS under the legislation. This audit should include an analysis of accuracy scores, success rates, and any other legislatively defined operational criteria, including statistically significant differences in performance across race, gender, or other protected characteristics.

10. The Committee recommends that the legislation and/or Code of Practice should provide for necessity and proportionality assessments, to be measured in response to specific legislative operational criteria, including but not limited to, success rates, which shall have legislatively defined criteria, and statistically significant differences in performance across race, gender, or other protected characteristics.

11. The Committee recommends that the legislation should include a mechanism allowing for the immediate revocation of a particular biometric identification technology if it is found that performance metrics are unsatisfactorily low, or if there are significant inconsistencies in performance.

12. The Committee recommends that the legislation should reflect the requirement of AGS to carry out a Data Protection Impact Assessment before introducing any biometric identification system or technology under the Law Enforcement Directive. The legislation should also require AGS to publish each Assessment in the interests of transparency.

13. The Committee recommends that it shall be a requirement under the legislation that any prosecutions arising from the use of FRT shall disclose that fact as part of the standard disclosure to defence in advance of trial.

14. The Committee recommends that the General Scheme should clarify the access to remedy for those whose rights have been breached as a result of FRT use.

15. The Committee recommends that there should be clear and limited criteria set out in relation to access of data by third-parties. Where footage is obtained by Gardaí from third-parties for the purpose of biometric identification, the Code of Practice must be clear as to the legal mechanism or mechanisms that will allow for this processing of personal data.

16. The Committee recommends that the definition of “biometric data” under Head 2 in the draft legislation is redrafted to give greater clarity and to bring it in line with EU law.

17. The Committee recommends that Section 43B(5) of Head 4 be redrafted to bring it in line with EU law and prevent “Live-like” processing.

18. The Committee recommends that the provisions under Head 4 should be amended to restrict Garda personnel from using biometric identification to track, monitor, or follow the movements of an individual over time, unless they believe on reasonable grounds that the person was involved in an offence listed in the Schedule, and such focused tracking is strictly necessary and proportionate to obtain evidence of that offence.

19. The Committee recommends that the proposed Section 43B(1) and Section 43B(2) under Head 4 lack precision and clarity and would benefit from redrafting.

20. The Committee recommends that Section 43B(6) of Head 4 be redrafted to provide a "strictly necessary" requirement in primary legislation, to ensure necessity and proportionality thresholds required by EU law are effectively assured.

21. The Committee recommends that provisions under Head 5 should be amended to provide for an application process based on prior authorisation by an independent administrative authority or by judicial approval, rather than internal Garda approval, whereby an application to use biometric identification shall be made to a District Court judge rather than to a senior member of AGS. A model for this would be the Communications (Retention of Data) (Amendment) Act 2022. It is also recommended that the processing only be done by suitably trained and qualified Gardaí, independent of the investigation, to ensure both sufficient oversight and independence in decision-making and processing.

22. The Committee recommends that the provisions under Head 5 should be amended to provide that any application to use biometric identification must specify a specific and limited set of data sources.

23. The Committee recommends that the provisions under Head 6 should be amended to reflect an application process based on judicial approval.

24. The Committee recommends that the provisions under Head 7 should be amended to provide for a specific time delay between the creation of images or footage and the permitted processing of the images or footage with biometric identification technology under the legislation, to reflect both European law in respect of the ban on live or live-like use of biometric identification and stated national policy.

25. The Committee recommends that the provisions under Head 7 should be amended to provide that any biometric identification may be subject to period sampling by way of blind peer review.

26. The Committee recommends that the provisions under Head 7 should be amended to compel AGS to collect and publish, on an annual basis, aggregate, anonymised statistics on uses of biometric identification under the legislation. Head 7 should provide that such statistics shall include aggregate details of the volume of images or footage scanned, the number of matches made and the number of false or incorrect matches, and a breakdown of uses of biometric identification by offence investigated, and the percentage of prosecutions which relied upon biometric identification.

27. The Committee recommends that Head 7 would regulate the use of any biometric technologies which use web-scraping of images[1], from social media or other publicly accessible locations.

[1] Web-scraping is defined by Cambridge dictionary as 'another name for scraping (= the activity of taking information from a website or computer screen and putting it into an ordered document on a computer)' WEB SCRAPING | English meaning - Cambridge Dictionary

28. The Committee recommends that the provisions under Head 9 should be amended to provide for a disciplinary process arising from deliberate breaches of a Code of Practice.

29. The Committee recognises the very serious nature of the additional list of offences set out in Appendix 2 and calls on the Government to include each of these offences in the Schedule of the Garda Síochána (Recording Devices) (Amendment) Bill 2023. The offences that the Minister asked the Committee to consider are very serious, such as defilement of a child under the age of 17, as well as a number of child pornography offences and offences relating to encouraging a sexual offence to be committed against a child. These offences carry heavy prison sentences and should be included in the Bill when published.

30. The Committee recommends that, under Head 3, a draft Code of Practice should be published alongside the Bill.

31. The Committee recommends that there must be mechanisms under the draft legislation to ensure regular reviews of the Code of Practice.

32. The Committee recommends that sufficient time should be allotted to the development of the Code of Practice and there should be consultations with relevant parties in relation to the development of the Code, including groups that would be disproportionately affected by usage of FRT, e.g. children or those from ethnic minority groups.

CHAPTER 1 - Introduction

This is the report on pre-legislative scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023, which would permit an Garda Síochána (AGS) to utilise Facial Recognition Technology (FRT), in specific circumstances.[2]

Purpose of the Bill

The General Scheme would amend *the Garda Síochána (Recording Devices) Act 2023* and provide a statutory basis to allow for biometric identification to be used by AGS.

It is anticipated that use of FRT would save Garda resources and time, while increasing the speed at which investigations can progress.

The draft legislation would provide that Gardaí can only use FRT retrospectively, to search images which are already legally in the possession of An Garda Síochána.

The Bill sets out the specific crimes for which the use of FRT would be permitted under the Schedule, and also the specific circumstances under which the use of FRT is permitted. These circumstances include:

i. where certain serious offences are suspected, as listed under the Schedule of the General Scheme;
ii. that the use of biometric identification must be necessary and proportionate;
iii. and that its use must be authorised in writing in advance by a Garda chief superintendent, and a record of this authorisation be retained.

The General Scheme will include safeguards around the use of FRT, including that its use must abide by the statutory Code of Practice for the legislation, with the Code

[2] gov.ie - Minister McEntee receives Cabinet approval for draft Facial Recognition Technology Bill (www.gov.ie)

subject to the approval of the Houses of the Oireachtas, while a designated judge of the High Court will also report annually to the Taoiseach on the operation of FRT. [3]

Procedural basis for scrutiny

Pre-legislative consideration was conducted in accordance with Standing Order 174A, which provides that the General Scheme of all Bills shall be given to the Committee empowered to consider Bills published by the member of Government.

[3] gov.ie - Minister McEntee receives Cabinet approval for draft Facial Recognition Technology Bill (www.gov.ie)

Engagement with stakeholders

The Joint Committee on Justice invited submissions from stakeholders on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023.

On 13th February, the Committee held two public engagements with several of these stakeholders, as laid out in the table below:

Table 1: List of public engagements with Stakeholders

Organisation	Witnesses	Date of appearance
Irish Council for Civil Liberties (ICCL)	Ms. Olga Cronin, Senior Policy Officer, Surveillance and Human Rights Mr. Simon McGarr, solicitor Digital Rights Ireland	13th February 2024
Data Protection Commission (DPC)	Mr. David Murphy, Deputy Commissioner Mr. Andrew Carroll, Assistant Commissioner	13th February 2024
An Garda Síochána	Garda Commissioner Drew Harris Mr. Andrew O'Sullivan, Chief Information Officer	13th February 2024
Law Society of Ireland	Mr. Mark Garrett, Director General Ms. Aimée McCumiskey, member of the Criminal Law Committee	13th February 2024
Rape Crisis Network Ireland (RCNI)	Dr. Clíona Saidléar, Executive Director Ms. Donna Parau, Legal Director	13th February 2024

Department of Justice	Ms. Rosaleen Killian PO, Legislation Dr. Frank McNamara, Senior Legal Researcher	13th February 2024

Table 2: List of public engagements with Stakeholders

Witness Name	Title	Date of appearance
Dr. Nessa Lynch	Matheson Lecturer in Law, Technology and Innovation, University College Cork/Research Fellow, Faculty of Law, Victoria University of Wellington, New Zealand	13th February 2024
Dr. Daragh Murray	Senior Lecturer and IHSS Fellow, School of Law, Queen Mary University of London, UKRI Future Leaders Fellow	13th February 2024
Professor David Kaye **Ms. Hinako Sugiyama**	University of California Irvine School of Law Digital Rights Fellow and Lecturer, University of California Irvine School of Law	13th February 2024
Dr. Ciara Bracken-Roche	Assistant Professor of Criminology, Maynooth University School of Law and Criminology	13th February 2024
Dr. Abeba Birhane	Senior Advisory, AI Accountability, Mozilla Foundation & Adjunct Assistant Professor, School of Computer Science and Statistics, Trinity College Dublin	13th February 2024

Department of Justice	Ms. Rosaleen Killian PO, Legislation Mr. Frank McNamara, Senior Legal Researcher	13th February 2024

The primary focus of these meetings were to allow for an engagement between the Members and stakeholders to discuss areas of the General Scheme which may require amending.

In the course of the public hearings, a number of important points were raised and these engagements allowed members to discuss some of these key issues in further detail with witnesses.

This report summarises the key points considered by the Committee when drafting the recommendations set out in this report.

A link to the full transcript of the engagements can be found here.

CHAPTER 2 - Summary of Submissions

The Committee received submissions from the following Stakeholders.

- Data Protection Commission (DPC)
- Professor David Kaye, University of California, Irvine School of Law
- Dr. Nessa Lynch, Matheson Lecturer in Law, Technology and Innovation, University College Cork/Research Fellow, Faculty of Law, Victoria University of Wellington, New Zealand
- Dr. Daragh Murray, Senior Lecturer and IHSS Fellow, School of Law, Queen Mary University of London, UKRI Future Leaders Fellow
- Safe Ireland
- An Garda Síochána
- Dr. Ciara Bracken-Roche, Assistant Professor of Criminology, Maynooth University School of Law and Criminology
- Rape Crisis Network Ireland (RCNI)
- ICCL and Digital Rights Ireland (DRI)
- Law Society of Ireland
- Dr. Abeba Birhane, Senior Advisory, AI Accountability, Mozilla Foundation & Adjunct Assistant Professor, School of Computer Science and Statistics, Trinity College Dublin

The submissions provided several observations on the General Scheme and commentary in relation to specific heads, in particular, outlining the impact of biometric identification technology on human and fundamental rights; outlining concerns with the accuracy of this technology and the potential for racial bias; and on provisions on the power to use the Biometric Identification [Head 4] and the Application for Approval of this technology [Head 5].

1. Impact of FRT on human rights and fundamental rights

- Impact on fundamental rights including privacy, data protection, expression, assembly, movement and equality and non-discrimination.
- Potential of FRT for mass surveillance and 'chilling effect'.
- Legality, necessity, and proportionality of FRT must be considered.

Operation of Facial Recognition Technology [FRT]

Submissions outlined that biometric technology operates through reliance on a database of images and using algorithms to identify specific details in an individual's face and assess the similarity of these details against other faces within the database. This technology can either try to find a one-to-one match in order to identify a particular individual or can produce several matches, ranked by probability, with a particular individual.

The General Scheme proposes to use retrospective facial recognition technology (RFR) only, which would apply FRT to any pre-recorded digital content, e.g. surveillance camera footage, images.

Some submissions stated that FRT has a range of impacts on rights but that, given the safeguards proposed in the General Scheme and the limitations of FRT usage for specific serious offences, this would place Ireland's use of the technology in the 'medium risk' category.

Other stakeholders highlighted that the 'probabilistic' nature of FRT can cause problems and that it may result in individuals, who have no link to an investigation, becoming involved simply because their probability score is high.

The majority of stakeholders highlighted the potential negative impacts of facial recognition technology (FRT) on human and fundamental rights, outlined below.

Impact on Human Rights

Stakeholders outlined how this technology would have an impact on several fundamental rights within democratic society, including, but not limited to:

- Right to privacy and data protection rights; (see Point 3)
- The right to non-discrimination (see Point 2);
- The right to freedom of peaceful assembly, freedom of expression and freedom of movement;
- The right to a fair trial

These rights are protected under several pieces of legislation, including Articles 21, 19(2)(3), 12(1)(3), and 17(1), of the International Covenant on Civil and Political Rights (ICCPR) and similar provisions in the European Convention on Human Rights (ECHR), provisions within the EU Law Enforcement Directive [LED] (Directive 2016/680), relating to police processing of personal data and the European Data Protection Board's Guidelines (EDPB 05/2022) on the use of facial recognition technology in the area of law enforcement.

Concerns with surveillance potential of this technology

Several stakeholders expressed concerns about the surveillance potential associated with this technology, highlighting that it would signal a significant departure from the existing surveillance capacity of the State. Some argued that use of this technology normalises the idea of a surveillance State or allows for indiscriminate surveillance of citizens.

Stakeholders highlighted that the technology could be used to track and monitor a significant amount of data about an individual and their public movements and that, if this were utilised in conjunction with other analytical tools, e.g. mapping tools, this information could be compiled over time to create a 'life profile' or pattern of an individual. For example, an individual's public movements could be tracked to find out where they live, work, their public interactions and relationships, their lifestyle or sexual orientation and their level of political engagement.

Some stakeholders disputed claims that FRT is effective for public order policing, e.g. riots and identifying those involved, arguing that this technology would be unable to identify anyone in footage wearing hats, glasses, face coverings or other accessories that cover their appearance. It was highlighted that the European Data Protection Board (EDPB) guidelines stated the use of FRT in riot situations is unlawful.

Chilling effect of this technology

Some stakeholders spoke of this technology having a 'chilling effect' or lasting effect on these rights, as it would cause individuals to alter their behaviour due to the fear of surveillance. Stakeholders highlighted that the use of surveillance would impact most heavily on those whose political opinions challenge mainstream views and expressed concerns that this could reduce the diversity of political opinion, undermine political engagement and have a negative impact on the ability of citizens to protest and mobilise for political or social change.

Some stakeholders argued that the difference in the surveillance capacities of live facial recognition technologies [LFR] and retrospective facial recognition technologies [RFR] are less pronounced than assumed, as the difference in time between use of LFR and RFR can be miniscule in practice. Some highlighted that the impacts of RFR may be even longer lasting, due to its ability to analyse stored data from any point in the past.

Others spoke of concerns that there could be a 'function creep', which often occurs with surveillance systems, whereby the system is introduced for one purpose but over time its use extends to additional purposes, beyond what was originally intended.

Stakeholders recommended that the legislation should ensure that certain uses of FRT should be strictly forbidden to guarantee fundamental rights. Some suggested that the General Scheme include the prohibition of mass surveillance of protesters in public spaces, banning the use of FRT on footage taken in a publicly accessible place, as suggested by the European Data Protection Board and European Data Protection Supervisor in 2021, or should impose a time limitation on the retention and use of footage taken in a publicly accessible place.

Legality, necessity, and proportionality of this technology must be considered

Stakeholders outlined that there is a three-part test under human rights law, to establish whether restrictions imposed on human rights are lawful or whether they constitute a violation of the right.

- **Legality:** That there must be a legal basis for the introduction of a restriction on human rights; that this restriction must be precise, public, transparent and 'foreseeable' as to its effects; and that the scope of the restriction must be limited to what is strictly necessary.

- **Necessity and proportionality:** Restrictions must target a specific objective and be proportionate to the aim they are pursuing. Applying restrictions must be the least restrictive measure or be the only measure that can be applied effectively to achieve the legitimate aim. In terms of proportionality, the benefits of the restrictions for human rights (e.g. the beneficial impact of FRT for public order policing) must be balanced against the potential harmful effects of this restriction on human rights.

- **Legitimacy:** That the restrictions are necessary and are introduced in pursuit of a legitimate aim, e.g. protecting national security or public order.

Submissions questioned whether the General Scheme fulfils the necessary criteria of legality, necessity and proportionality in relation to the use of FRT and recommended that this should be further examined.

2. Accuracy concerns and potential for discrimination and bias

- Some expressed concern with the accuracy of FRT e.g. results of reviews on the use of FRT by police bodies in other jurisdictions.
- Others highlight results of annual Facial Recognition Technology Evaluation (FRTE) 1:1 Verification, which found over 99% accuracy for some algorithms.
- Concerns around the bias and discriminatory effects of FRT.

Stakeholders outlined concerns with the accuracy of FRT and concerns with the potential bias and discriminatory impacts associated with these systems.

Accuracy

Some stakeholders argued that FRT is a less effective and more intrusive form of technology than other technologies which are used to aid policing and said there is a lack of information available to demonstrate its effectiveness.

Submissions pointed to a survey which reviewed the use of FRT by police in Wales in the period 2016 - 2023 and found that over 508,000 faces were scanned, however, there was an inaccuracy rate of 88% with over 3,000 individuals wrongly identified by the technology. Another survey from the UK Metropolitan Police Service found that over the course of 2023, the Service utilised live FRT 24 times with an estimated 340,672 faces scanned but the average ‘success’ rate at which an individual was correctly identified was only 0.0002%.

It was highlighted that the accuracy rates of this technology can also be influenced by other factors, including the quality of images used, the lighting of the image and whether the individual is wearing a mask or headgear.

Other stakeholders said there is evidence that the accuracy rates of this technology have improved rapidly over time, as the technology itself has evolved and that any analysis on the accuracy of this technology must specify the exact algorithm and version of the algorithm to which it refers. Some argued that it has been shown that

identification by FRT systems performs better than identification done by the human eye, which can be particularly unreliable.

Submissions referred to the bi-annual Facial Recognition Technology Evaluation (FRTE) 1:1 Verification, which is carried out by the U.S. Government's National Institute of Standards and Technology (NIST) and evaluates over 500 algorithms for facial recognition. It was argued that the NIST evaluation had found that while a number of algorithms are somewhat less accurate for demographic traits, that in absolute terms, there is a minute difference in accuracy for the highest rated algorithms.

An example highlighted the results from the algorithm titled "cloudwalk_mt_007", from February 2023, which found identification scores of over 99% accuracy for all categories in which it was tested. This includes its worst false matching ratio at 0.71% for West African women aged 65 to 99 and its worst false non-matching ratio at 0.16% for individuals from Southern Asia.

The results of the NIST found that this technology is most effective when it is used in combination with human intervention. It was highlighted that a mixture of machine and human identification is the best practice approach adopted by other law enforcement agencies and that the Garda National Cyber Crime Bureau (GNCCB) has a strong commitment to

Stakeholders said that An Garda Síochána (AGS) plans to refer to the NIST accuracy ratings when deciding which algorithm it will select to use in the future, following the approach of the Italian national police when they sought to procure this technology.

Discrimination and Bias

Several stakeholders argued that FRT has intrinsic racial and discriminatory bias and that numerous studies have demonstrated that there is a higher rate of misidentification by image classification technology for women, men and those with darker skin, due to the training programmed into these technologies. It was stated that black men and women have the highest rate of being classified as a 'criminal' or

'suspicious person' by these technologies and are more often classified as non-human animals e.g. as chimpanzees and gorillas than lighter skinned people, which is dehumanizing.

Stakeholders also pointed out that FRT could also deepen structural inequalities in marginalised communities as these communities are already over- policed and use of this flawed technology by police could increase the wrongful imprisonment of individuals from these communities. Stakeholders stated that, in the US, 6 black people have been wrongfully arrested on the basis of flawed FRT and that there are likely more individuals that have been wrongfully arrested from FRT misidentification but their cases have not been publicised. It was also pointed out that the database of images that will be used as a comparison by these technologies will likely stem from these marginalised communities and that this should be monitored to avoid perpetrating bias.

3. Data privacy concerns relating to FRT

Several stakeholders raised concerns with the potential impacts of the General Scheme on data privacy and discussed the compliance of the General Scheme with data privacy requirements.

Submissions highlighted that the EU Law Enforcement Directive (LED) regulates the processing of personal data for law enforcement purposes and was transposed into Irish law under Part 5 of the Data Protection Act 2018. It was highlighted that in order for FRT to be used in a proportionate manner by law enforcement, the processing of personal data must comply with standards of clarity and foreseeability in terms of its effects and that it is limited to what is strictly necessary, as required under the LED.

While the General Scheme provides some safeguards around use of this technology, stakeholders said that many issues must still be addressed in the Code of Practice, e.g. the operational use of biometric identification, to ensure that FRT usage by law enforcement is compliant with the requirements of data protection law.

Other potential clashes with data privacy law include the potential discrimination of these technologies, which would breach Article 11.3 of the Law Enforcement Directive [LED], which regulates the processing of personal data for law enforcement purposes and requires that the processing of data laws must be non-discriminatory. Some stakeholders pointed out that the General Scheme should also include specific provisions to guarantee the protection of personal data collected, which may have a negative or traumatic impact on victims or impact on their right to privacy.

Some stakeholders argued that the use of FRT may protect individuals' privacy more than general analysis of CCTV or similar footage by humans, as this technology will target its search of footage for a particular person of interest rather than all individuals who appear in the footage.

Database of Images

Submissions questioned where the database of images, that would be used for biometric identification, would come from, as this is not clarified in the General

Scheme. References were made to the unlawful database of images, created with biometric identification, that was gathered by the Department of Social Protection in relation to the Public Services Card and it was argued that there must be clear strictures around the data that AGS can legally access.

Stakeholders recommended that the General Scheme should stipulate that AGS must only use images that have been legally obtained by outside organisations, or this could compromise a conviction, if it was found that unlawful data was used. It was also recommended that it be stated which national and international organisations can legally provide images to AGS.

4. Need for strengthened safeguards within the General Scheme

- Should be possible to audit all usage and authorisation of FRT.
- Results of biometric identification must be identified by Garda personnel.
- Safeguards must avoid introducing excessive or bureaucratic processes that may delay investigations.

Several submissions highlighted the lack of sufficient safeguards in the General Scheme. Stakeholders argued that having robust safeguards in the legislation is essential to protect individuals from the use of these technologies by AGS, especially more vulnerable groups and to ensure that there is public trust and confidence in AGS to use this technology in a lawful manner.

A number of safeguards were suggested by stakeholders for inclusion in the General Scheme and include some of the following:

- **Verification of biometric identification by Garda personnel:** Several stakeholders underlined that it would be essential for the results from any biometric identification to be verified by a Garda member prior to any action being taken on the basis of automated identification and welcomed the inclusion of this in the General Scheme. The Code of Practice should provide further details on the level of training and expertise that will be expected of Garda personnel involved in the verification process and some stakeholders recommended that this training should entrench a culture of 'ethical data' use within AGS.

  AGS stated that the organisation is strongly committed to the blended model of using both digital and human skills when using biometric identification tools and that they follow the principle that biometric identification tools exist only for decision support. It was highlighted that any decision that will have a significant impact on individuals will be made by a trained and accountable Garda members, who will be responsible for their interpretation of evidence.

- **Audit:** Stakeholders said that all usage of FRT should be documented and it should be possible to audit applications for approval of identification by FRT and the approval granted.

- **External monitoring:** It was recommended that the legislation provide more safeguards on the external monitoring of the use of FRT.

- **Low-quality images:** That it should be forbidden for police to use FRT on unsuitable or low-quality images.

- **Create clear criteria concerning third-party access to the data collected:** That there should be clear and limited criteria set out in relation to access of data by third-parties. Where footage is obtained by Gardaí from 3rd parties for the purpose of biometric identification, the Code of Practice must be clear as to the legal mechanism or mechanisms that will allow for this processing of personal data.

- **Minimum operational thresholds:** That there should be minimum operational thresholds e.g. relating to precision, false positive rates, true positive rates, for policing FRT systems.

- **Safeguards must avoid introducing excessive processes:** Some stakeholders cautioned that the inclusion of safeguards in this legislation must avoid introducing overly bureaucratic or excessive processes, which could delay or jeopardise investigations which used such technology. It was suggested that procedures around authorisation / use of biometric identification should consider the different forms of biometric processing and the level of intrusiveness of each of these.

Code of Practice

Stakeholders noted that the Code of Practice will have an essential role in regulating several key elements of this technology, including the situations in which it will be permissible to use FRT and to provide information and instructions for Garda personnel on its use.

It was highlighted that it can be useful to stipulate such requirements in Codes of Practice rather than in the General Scheme, as these Codes can be a useful tool for regulating emerging technologies because they provide a level of flexibility, as well as the necessary clarity and legal certainty to prevent their arbitrary use.

Several stakeholders welcomed that the Code of Practice must be subject to the approval of the Houses of the Oireachtas under Head 14. Some suggested a provision should be added under this Head so that, in deciding whether to approve the Code, the Houses should confirm whether the proposed Code respects and guarantees fundamental human rights, to affirm these rights will not be compromised under the legislation.

Stakeholders argued that there should be sufficient time allotted to the development of the Code of Practice, given the complexity and scale of issues that it will regulate and given the need for the Code to engage in consultations with relevant parties, including groups that would be disproportionately affected by usage of FRT, e.g. children or those from ethnic minority groups.

Submissions recommended that the Code of Practice should include some of the following elements:

- That the language used in relation to the procedures for deployment of FRT is strong and affirmative, to ensure that the Code contributes to clarity and foreseeability relating to data processing and that the General Scheme fulfils the criteria of the legality test.

- Clear directions on the processing operations for this technology and the circumstances in which the use of biometric identification is considered necessary, proportionate and justified.

- Effective internal oversight mechanisms regulating the deployment of FRT;

- That there are high standards in relation to the procurement, probity, audit and data storage standards of any biometric technology that is acquired and that the accuracy levels of this system must meet accepted standards, such as those published by the NIST;

- Measures to ensure transparency to the public, including public communications campaigns and access to procedures for handling complaints for members of the public;

5. Other concerns with the introduction of FRT as proposed in the General Scheme

Submissions outlined some of the following concerns with the General Scheme as proposed:

- **Use of FRT in other jurisdictions:** Some stakeholders rejected arguments that FRT can be safely introduced in Ireland as it is already used by police in other jurisdictions. For example, it was highlighted that, due to its fundamental risks, some jurisdictions in the US have banned use of FRT by their police forces, including San Francisco, Oakland and Boston.

- **Interaction between legislation and developing AI Act in the EU:** Stakeholders highlighted the ongoing negotiations for the Artificial Intelligence (AI) Act at EU level, which would regulate the use of AI for law enforcement purposes, including the use of FRT. It was underlined that the provisions within the General Scheme must comply with the provisions of the AI Act, once agreed, to ensure there is no inconsistency between the two pieces of legislation.

- **Risk of cases being appealed through use of flawed technology:** Submissions argued that the flaws present in the General Scheme as proposed could result in secure convictions being appealed on the basis of the use of FRT. Others argued that there should be strict controls around the use of FRT in criminal investigations, to avoid challenges by defendants that its usage infringes their rights to an unacceptable degree.

- **Lack of transparency on the algorithms and practice used by FRT providers:** Stakeholders argued that there is a lack of transparency in respect of the algorithms, models, and training data that are used by some FRT providers. This makes it difficult for the State to evaluate these technologies or for the public to hold providers or authorities to account for failures stemming

from these systems and it was highlighted that the General Scheme contains no access to remedy for those whose rights have been breached as a result of FRT use.

Stakeholders also highlighted that some practices employed by FRT companies have been questioned. They referred to an investigation by several Canadian authorities into the company Clearview AI between 2020 and 2021, which found that Clearview had collected images in an unreasonable manner and that Clearview's practices will often have detrimental impacts for the individuals of whose images it scans. Stakeholders highlighted that several actions and judgements have also been lodged in relation to Clearview AI in Europe.

- **Special protections for children under the legislation:** Stakeholders highlighted that children are a particularly vulnerable group and must be afforded extra protections under this legislation. It was pointed out that the State must adopt a children's rights compliant approach in collecting and analysing children's biometric data and facial images and that such data must only be collected by law enforcement agencies in exceptional circumstances, where there is a considerable risk to public safety. Stakeholders recommended that a children's rights impact analysis of the General Scheme should be undertaken to guarantee the protection of children's rights under the legislation.

Stakeholders made some of the following recommendations for how the legislation should be changed:

- **Moratorium on the introduction of FRT:** Some stakeholders recommended that there should be a moratorium on the introduction of FRT in Ireland, until further research is undertaken into some of the key concerns with this technology, including infringements on human and privacy rights. Others argued that less intrusive technology to assist AGS should be introduced, rather than introducing FRT.

- **Public consultation with groups most impacted:** Submissions recommended that a public consultation should be arranged with marginalized communities and other groups that will be most impacted by FRT, and also with other relevant stakeholder groups including policing and technology experts and civil society organisations, prior to the introduction of this technology. These consultations must be transparent, accessible for those with disabilities or for whom English is not their first language and must demonstrate that the advice from consultations was considered and provide justification for the results stemming from these consultations.

- **Consultation with experts:** It was also recommended that the Department of Justice engage in consultations with academic experts and those from NGOs, who have previously published several articles on the topic of FRT (as detailed further in submissions).

6. Arguments in favour of FRT

Submissions outlined some of the benefits associated with the use of FRT by policing bodies.

While acknowledging the human rights concerns associated with this technology, some stakeholders argued that a human rights approach also requires that the State would investigate and prosecute serious crimes in order to protect the rights of victims. Some argued that the public expects AGS to avail of the most up to date technology, in order to undertake investigations most efficiently, especially where this technology is used in other areas of the public sphere. It was highlighted that studies have shown that there is a level of public support for the use of FRT in relation to serious offences, although stakeholders highlighted that these studies did lack representation of those from minority backgrounds.

Submissions highlighted that use of facial recognition technology would have some of the following advantages for policing:

- **Essential to be able to process complex digital evidence:** Digitalisation has fundamentally changed the nature of crime and it is essential for police forces to be able to collect and process ‘Big Data’ levels of complex digital evidence, in order to prevent crimes and protect public safety. It is also important for law enforcement services to keep pace with digital trends and technology in order to respond to digital crimes.

- **Important for tackling transnational crime:** Criminal gangs use digitalisation to support global organised crime networks and will seek to operate in jurisdictions that are less equipped to prevent these crimes, therefore it is vital that the technological capabilities AGS would be equal to that of other jurisdictions. This would also be important in cases where Ireland may need to co-operate with other law enforcement agencies in transnational criminal investigations.

- **Use of FRT saves resources and time:** Submissions outlined that it is becoming exceedingly difficult for Garda personnel to manually filter through footage, given the sheer level of data that must be processed as evidence in modern investigations.

  It was also highlighted that, of the 8 use cases to which AGS wishes to apply biometric tools (outlined further in its submission), only one of these cases involves the identification of people through FRT. The other use cases envisage FRT being used to filter through significant amounts of evidence, in order to identify useful material for investigations.

- **Current usage of image analysis and recognition technology in child sexual abuse material (CSAM Investigations):** Submissions highlighted that approximately 60% of the cases referred to the Garda National Cyber Crime Bureau (GNCCB), relate to child sexual abuse material (CSAM) and that the GNCBB employs Image Analysis and Recognition Technology tools when handling these cases. The use of Image Analysis and Recognition Technology has some of the following benefits:

1. It was emphasised that recourse to these tools is crucial when investigating CSAM cases and that it would be almost impossible to complete investigations without these tools, given the sheer volume of footage and images involved in these crimes.

2. It was argued that this technology is also more effective in analysing evidence than human operators are.

3. It was stated that use of this technology reduces the invasion of privacy of ordinary citizens that are captured on this footage.

4. Submissions argued that use of these technologies helps to counter the traumatic impact on Garda members who must otherwise manually review this

footage. It was pointed out that several Garda members involved in these cases are on long-term sick leave due to the trauma of viewing the material.

5. Submissions also pointed out that the use of these tools in CSAM investigations is standard practice by law enforcement agencies in developed countries and that use of this technology has not yet been legally challenged, in either national or transnational investigations.

6. It was highlighted that there is a wide level of social support for the use of this technology for investigations relating to CSAM.

7. Comments on specific Heads within the General Scheme

- **Head 2: Amendment to Section 2 of Principal Act– INTERPRETATION**

Stakeholders pointed out the following considerations in relation to Head 2:

- The definition of 'biometric data' under this Head creates a separate definition to that under section 69 of the Data Protection Act 2018, as it only includes facial images, rather than DNA or fingerprint data. This creates an inconsistency between the two terms, with the definition proposed under the General Scheme contradicting existing EU law as a result.

- It was recommended that a data protection impact assessment (DPIA) should be carried out by AGS before any biometric system be introduced, the results of which should be made publicly available in the interests of transparency.

- There must be further clarity around the biometric data that will be legally held by AGS, to prevent against potential misuse of this data.

- That the term 'biometric identification' be more clearly defined, as it appears to allow only for the unique identification of an individual and may preclude other uses of this technology that do not where confirming an individua's identity is not the intent.

- The General Scheme should provide more clarity on the term 'technical processing' and whether this includes processing of physical photographs or facial images created by a camera phone.

- It should be stated more clearly if it is intended that the General Scheme will apply to facial images and not other physical attributes of individuals, e.g. their height.

- That AGS must demonstrate that the probabilistic thresholds defined by the user or developer of any proposed biometric identification system are accurate,

before this system is utilised, to prevent the risk of discrimination against individuals, based on biases within the system.

- **Head 4: New Section 43B – Power to use the Biometric Identification**

Stakeholders made some of the following comments in relation to Head 4 of the General Scheme:

- It was argued that Head 4 grants excessive powers to Gardaí and allows excessive discretion to Gardaí in how to exercise these powers.

- It was argued that Section 43B(1) and Section 43B(2) fail to include any provisions to ensure that use of FRT would be targeted in relation to the individuals that are to be identified or to provide any evidence that a person searched and identified has committed or is suspected of having committed a crime.

- Section 43(B) fails to outline key details in relation to biometric identification, including the specific uses, use contexts and limits of discretion relating to this technology. It was argued that the powers to use FRT should be based on objective criteria, to limit the scope for arbitrary or unjust use of the technology and allow for effective oversight of it.

- It was argued that there is a disparity in the gravity of offences contained in the Schedule of the Bill, with stakeholders arguing that some offences are not serious enough to warrant use of FRT. It was highlighted that including offences of ‘riot’ and ‘violent disorder’ could impact negatively on peaceful protests and the right to freedom of assembly and freedom of expression and could represent a concerning example of ‘mission creep’.

- There is inconsistency in the references to “Garda Personnel” and “Garda Member” under Head 4 and it was recommended that the term “Garda Personnel” be used as the default term.

- Submissions stated that Section 43B(1)(a) should also include detection of offences as a valid purpose for the use of biometric identification, which may be important where reviews of large amounts of footage to detect CSAM may later lead on to an investigation of suspected offences as listed under the Schedules in the General Scheme.

- That the power to locate or follow the movements of an individual gives extensive surveillance powers to Gardaí and there no limitations or safeguards stipulated in the General Scheme in relation to this power, or to guide how it should be exercised.

- That “biometric identification” under Section 43B(2) should be defined so that it may only include systems that meet widely accepted and reliable technical standards, e.g. those evaluated favourably by the NIST or by the European Union Agency for Network and Information Security.

- That Section 43B(3) must specify the exact data sources to be used by AGS for facial identification and include examples of these and that the meaning of “legally” held or accessed images and video should be defined in a manner that is compatible with human rights law.

- That Section 43B(3) fails to provide sufficient criteria around ‘who’ would be included in a search, e.g. criteria around how a Garda would select an image to be searched or the reference database a Garda would use when searching.

- **Head 5: New Section 43C – Application for Approval**

Stakeholders made some of the following comments in relation to Head 5 of the General Scheme:

- Stakeholders argued that the approval for use of biometric technology should be granted by the judiciary, or by an independent and impartial oversight body and not by a Garda member of the rank chief superintendent or higher, as proposed under Head 5. It was argued that permitting internal Garda approval in this area does not allow for enough separation to prevent bias or arbitrary judgements. This provision would also contradict the draft AI Act, which requires judicial approval or the approval of an independent oversight body, when seeking the use of biometric identification.

- Stakeholders suggested that applications to judges should contain several key details relating to the context in which FRT will be used among them the reasons that FRT was selected as a search tool as opposed to other options; justification for the reasons an FRT search is necessary and proportionate for the case in question; and an impact assessment which will explain the benefits and potential harms to human rights, stemming from the use of FRT in the particular situation

- It was argued that the Code of Practice will need to provide additional details to Gardaí on the application process and on how to assess the standards of necessity and proportionality to reach the threshold for use of biometric identification, to ensure consistency of application across the organisation.

- Some argued that it would be difficult for AGS to define ‘the parameters of the search’ in an application for approval, as search terms can change as evidence is assessed. It was argued that including this requirement could cause administrative burdens and delays for the investigation team. Others stated that when defining these parameters, the Code of Practice should stipulate that Gardaí personnel must abide by the principle of data minimization, whereby

personal data must be adequate, relevant, and should not be unnecessary to the purposes for which they are processed.

- Some submissions questioned whether any Garda will be able to access biometric identification software and suggested that there should be limits on who should be able to access this technology or whether it should be limited to trained personnel within a specific Garda unit.

- **Head 6: New Section 43D – Approval**

Stakeholders recommended that the General Scheme should make clearer the criteria against which a Chief Superintendent must assess whether the use of biometric identification is necessary and proportionate.

It was recommended that an evaluation of harm be built into the approval and authorisation process, as this is critical to determine the necessity of the use of FRT in a given case and that Authorising Officers would be trained on how to assess human rights impacts.

It was suggested that a new section be inserted under this Head that would make it obligatory to notify individuals whose data has been processed by FRT of the time, date, and location of the images or video on which facial identification was / will be used, to guarantee that individuals will have the right to an effective remedy, where necessary.

Stakeholders pointed out that provisions under 43D(1) and 43C(2) would permit approvals of applications to be made by individuals of the same, or lower rank than applicants. It was highlighted that issues of rank, hierarchy, and organisational culture could negatively impact on the independence and objective decision-making in relation to applications.

- **Head 7: New Section 43E – Use of the Biometric Identification**

Stakeholders recommended that more clarity should be provided around the range of images or footage that will fall under the scope of this Head for use by biometric identification. It was highlighted that any mass collection of personal data from individuals who are not aware their data is being collected for the purposes of FRT, would have a disproportionate impact on their right to privacy.

It was recommended that this Head would prohibit the use of any biometric technologies which use web-scraping of images, from social media or other publicly accessible locations.

Some submissions suggested that section 43E(2) could be removed, as it suggests that the verification of biometric results should be carried out by a separate member of staff to the primary investigation team. It was argued that this is an unnecessary safeguard, given other safeguards which will be followed and given that it may not be feasible to do this in situations where subject matter experts are essential to the original investigation teams.

It was recommended that more detail should be provided on the 'verification' process under this Head.

- **Schedule of Offences**

Stakeholders welcomed the restriction of the use of FRT to particularly serious offences, as this will ensure that the technology is only deployed in situations where it is necessary and proportionate. It was highlighted that this may depend on the type of investigation, rather than the nature of the offence.

Stakeholders cautioned that careful consideration must be given if it is intended to expand the list beyond serious offences and that attention must be paid to the standards applied in the draft AI Act at EU level.

It was highlighted that this section does not include any terrorist related offences, offences relating to organized crime or the offence of sexual assault.

- **Offences not included in the Schedule**

In relation to the additional offences that are considered for inclusion in the General Scheme, some of the following suggestions were made:

- It was recommended that the Committee would consider the provisions under Recital 19 of the draft AI Act at European level, which stipulates that policing authorities should only use AI tools in relation to criminal offences which would incur a period of detention for a maximum period of at least three years.

- Submissions pointed to the suggested provision that the biometric technology could be applied to drug trafficking offences over the value of €13,000. It was argued this could prove difficult to implement, in situations where biometric identification could be used for a seizure of drugs that is valued below this limit and then questions will arise as to whether the use of technology for this crime would be lawful or not.

- It was highlighted that offences included under Sections 16 and 17 of the Non-Fatal Offences Against the Person Act 1997 would not allow for use of biometric identification for missing persons cases, where abduction is not believed to be a factor.

- Some stakeholders recommended that the Schedule of Offences should include all sexual offences, so that these victims may be reassured that the most up to date technology is being used to gather evidence. It was argued that it can be decided whether this data is necessary and proportionate at a later point when it is decided how the data that is collected should be used.

- Some suggested that certain domestic-violence related offences should be included on this list as, similar to the serious offences already included under the General Scheme, they are all likely to have a serious and lasting effect on their victims, which is reflected in the length of the maximum sentences for these offences. This would include, among others, offences of stalking, harassment, coercive control, and non-fatal strangulation or suffocation.

APPENDICES

APPENDIX 1- ORDERS OF REFERENCE OF THE COMMITTEE

Standing Orders 94, 95 and 96 – scope of activity and powers of Select Committees and functions of Departmental Select Committees

Scope and context of activities of Select Committees.

94.(1) The Dáil may appoint a Select Committee to consider and, if so permitted, to take evidence upon any Bill, Estimate or matter, and to report its opinion for the information and assistance of the Dáil. Such motion shall specifically state the orders of reference of the Committee, define the powers devolved upon it, fix the number of members to serve on it, state the quorum, and may appoint a date upon which the Committee shall report back to the Dáil.

(2) It shall be an instruction to each Select Committee that—

(*a*)it may only consider such matters, engage in such activities, exercise such powers and discharge such functions as are specifically authorised under its orders of reference and under Standing Orders;

(*b*) such matters, activities, powers and functions shall be relevant to, and shall arise only in the context of, the preparation of a report to the Dáil;

(*c*) it shall not consider any matter which is being considered, or of which notice has been given of a proposal to consider, by the Joint Committee on Public Petitions in the exercise of its functions under Standing Order 125(1)[4]; and

[4] Retained pending review of the Joint Committee on Public Petitions

(*d*) it shall refrain from inquiring into in public session or publishing confidential information regarding any matter if so requested, for stated reasons given in writing, by—

(i) a member of the Government or a Minister of State, or

(ii) the principal office-holder of a State body within the responsibility of a Government Department or

(iii) the principal office-holder of a non-State body which is partly funded by the State,

Provided that the Committee may appeal any such request made to the Ceann Comhairle, whose decision shall be final.

(3) It shall be an instruction to all Select Committees to which Bills are referred that they shall ensure that not more than two Select Committees shall meet to consider a Bill on any given day, unless the Dáil, after due notice to the Business Committee by a Chairman of one of the Select Committees concerned, waives this instruction.

Functions of Departmental Select Committees.

95. (1) The Dáil may appoint a Departmental Select Committee to consider and, unless otherwise provided for in these Standing Orders or by order, to report to the Dáil on any matter relating to—

(*a*) legislation, policy, governance, expenditure and administration of—

(i) a Government Department, and

(ii) State bodies within the responsibility of such Department, and

(*b*) the performance of a non-State body in relation to an agreement for the provision of services that it has entered into with any such Government Department or State body.

(2) A Select Committee appointed pursuant to this Standing Order shall also consider such other matters which—

(a) stand referred to the Committee by virtue of these Standing Orders or statute law, or

(b) shall be referred to the Committee by order of the Dáil.

(3) The principal purpose of Committee consideration of matters of policy, governance, expenditure and administration under paragraph (1) shall be—

(*a*) for the accountability of the relevant Minister or Minister of State, and

(b) to assess the performance of the relevant Government Department or of a State body within the responsibility of the relevant Department, in delivering public services while achieving intended outcomes, including value for money.

(4) A Select Committee appointed pursuant to this Standing Order shall not consider any matter relating to accounts audited by, or reports of, the Comptroller and Auditor General unless the Committee of Public Accounts—

(a) consents to such consideration, or

(b) has reported on such accounts or reports.

(5) A Select Committee appointed pursuant to this Standing Order may be joined with a Select Committee appointed by Seanad Éireann to be and act as a Joint Committee for the purposes of paragraph (1) and such other purposes as may be specified in these Standing Orders or by order of the Dáil: provided that the Joint Committee shall not consider—

(a) the Committee Stage of a Bill,

(b) Estimates for Public Services, or

(c) a proposal contained in a motion for the approval of an international agreement involving a charge upon public funds referred to the Committee by order of the Dáil.

(6) Any report that the Joint Committee proposes to make shall, on adoption by the Joint Committee, be made to both Houses of the Oireachtas.

(7) The Chairman of the Select Committee appointed pursuant to this Standing Order shall also be Chairman of the Joint Committee.

(8) Where a Select Committee proposes to consider—

(a) EU draft legislative acts standing referred to the Select Committee under Standing Order 133, including the compliance of such acts with the principle of subsidiarity,

(b) other proposals for EU legislation and related policy issues, including programmes and guidelines prepared by the European Commission as a basis of possible legislative action,

(c) non-legislative documents published by any EU institution in relation to EU policy matters, or

(d) matters listed for consideration on the agenda for meetings of the relevant Council (of Ministers) of the European Union and the outcome of such meetings, the following may be notified accordingly and shall have the right to attend and take part in such consideration without having a right to move motions or amendments or the right to vote:

(i) members of the European Parliament elected from constituencies in Ireland,

(ii) members of the Irish delegation to the Parliamentary Assembly of the Council of Europe, and

(iii) at the invitation of the Committee, other members of the European Parliament.

(9) A Select Committee appointed pursuant to this Standing Order may, in respect of any Ombudsman charged with oversight of public services within the policy remit of the relevant Department consider—

(*a*) such motions relating to the appointment of an Ombudsman as may be referred to the Committee, and

(*b*) such Ombudsman reports laid before either or both Houses of the Oireachtas as the Committee may select: Provided that the provisions of Standing Order 130 apply where the Select Committee has not considered the Ombudsman report, or a portion or portions thereof, within two months (excluding Christmas, Easter or summer recess periods) of the report being laid before either or both Houses of the Oireachtas.[5]

5 Retained pending review of the Joint Committee on Public Petitions.

Powers of Select Committees.

96. Unless the Dáil shall otherwise order, a Committee appointed pursuant to these Standing Orders shall have the following powers:

(1) power to invite and receive oral and written evidence and to print and publish from time to time—

(a) minutes of such evidence as was heard in public, and

(b) such evidence in writing as the Committee thinks fit;

(2) power to appoint sub-Committees and to refer to such sub-Committees any matter comprehended by its orders of reference and to delegate any of its powers to such sub-Committees, including power to report directly to the Dáil;

(3) power to draft recommendations for legislative change and for new legislation;

(4) in relation to any statutory instrument, including those laid or laid in draft before either or both Houses of the Oireachtas, power to—

(*a*) require any Government Department or other instrument-making authority concerned to—

(i) submit a memorandum to the Select Committee explaining the statutory
Instrument, or

(ii) attend a meeting of the Select Committee to explain any such statutory instrument: Provided that the authority concerned may decline to attend for reasons given in writing to the Select Committee, which may report thereon to the Dáil,

and

(*b*) recommend, where it considers that such action is warranted, that the instrument should be annulled or amended;

(5) power to require that a member of the Government or Minister of State shall attend before the Select Committee to discuss—

(a) policy, or

(*b*) proposed primary or secondary legislation (prior to such legislation being published),

for which he or she is officially responsible: Provided that a member of the Government or Minister of State may decline to attend for stated reasons given in writing to the Select Committee, which may report thereon to the Dáil: and provided further that a member of the Government or Minister of State may request to attend a meeting of the Select Committee to enable him or her to discuss such policy or proposed legislation;

(6) power to require that a member of the Government or Minister of State shall attend before the Select Committee and provide, in private session if so requested by the attendee, oral briefings in advance of meetings of the relevant EC Council (of Ministers) of the European Union to enable the Select Committee to make known its views: Provided that the Committee may also require such attendance following such meetings;

(7) power to require that the Chairperson designate of a body or agency under the aegis of a Department shall, prior to his or her appointment, attend before the Select Committee to discuss his or her strategic priorities for the role;

(8) power to require that a member of the Government or Minister of State who is officially

responsible for the implementation of an Act shall attend before a Select Committee in relation to the consideration of a report under Standing Order 197;

(9) subject to any constraints otherwise prescribed by law, power to require that principal office-holders of a—

(*a*) State body within the responsibility of a Government Department or

(*b*) non-State body which is partly funded by the State,

shall attend meetings of the Select Committee, as appropriate, to discuss issues for which they are officially responsible: Provided that such an office-holder may decline to attend for stated reasons given in writing to the Select Committee, which may report thereon to the Dáil;

and

(10) power to—

(*a*) engage the services of persons with specialist or technical knowledge, to assist it or any of its sub-Committees in considering particular matters; and

(b) undertake travel;

Provided that the powers under this paragraph are subject to such recommendations as may be made by the Working Group of Committee Chairmen under Standing Order 120(4)(*a*).'

APPENDIX 2 - LIST OF STAKEHOLDERS AND SUBMISSIONS

The Committee received submissions from the following stakeholders:

- Data Protection Commission (DPC)
- Professor David Kaye, University of California, Irvine School of Law
- Dr. Nessa Lynch, Matheson Lecturer in Law, Technology and Innovation, University College Cork/Research Fellow, Faculty of Law, Victoria University of Wellington, New Zealand
- Dr. Daragh Murray, Senior Lecturer and IHSS Fellow, School of Law, Queen Mary University of London, UKRI Future Leaders Fellow
- Safe Ireland
- An Garda Síochána
- Dr. Ciara Bracken-Roche, Assistant Professor of Criminology, Maynooth University School of Law and Criminology
- Rape Crisis Network Ireland (RCNI)
- ICCL and Digital Rights Ireland (DRI)
- Law Society of Ireland
- Dr. Abeba Birhane, Senior Advisory, AI Accountability, Mozilla Foundation & Adjunct Assistant Professor, School of Computer Science and Statistics, Trinity College Dublin

[Submissions are available in the online version of the Committee's Report, which will be accessible at https://www.oireachtas.ie/en/committees/33/justice/].

An Coimisiún um Chosaint Sonraí
Data Protection Commission

GSRDA_01 (1)

Submission by the Data Protection Commission to the Joint Committee on Justice on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill

Contents

Executive Summary

1. The Data Protection Commission (DPC) welcomes the opportunity to contribute to the Joint Committee's deliberations on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill by way of this written submission. As the statutory supervisory authority in the State for the data protection legislative frameworks, the DPC is tasked with monitoring the application of data protection law and upholding the rights and freedoms of individuals in relation to the processing of their personal data.

2. This submission addresses the issues arising from a data protection perspective in the processing of personal data necessary for the carrying out of biometric identification as set out in the General Scheme of the Bill, and details the expectations of the DPC with regard to the legislation, and for the operational deployment of biometric identification by An Garda Síochána, in a manner that complies with data protection law.

3. This submission sets outs an overview of the applicable legal frameworks regulating the processing of personal data in the context of the General Scheme, as well as particular data protection considerations arising from the technology utilised for biometric identification, including in relation to facial recognition technology (FRT). These legal and technological observations are considered in the specific context of the Heads of the Bill, with a particular focus on the code of practice. The submission also sets out in detail the data protection obligations of An Garda Síochána, as the competent law enforcement authority, prior to the implementation of any biometric identification systems.

4. The Submission makes reference to Guidelines 05/2022 of the European Data Protection Board on the use of facial recognition technology in the area of law enforcement[1] (the Guidelines). The DPC is a constituent member of the European Data Protection Board (EDPB) and the Guidelines express the Board's position on the data protection implications of biometric identification by way of facial recognition in law enforcement.

[1] Please see: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

Introduction

5. The DPC is grateful to the Joint Committee for the opportunity to comment on the General Scheme of this proposed legislation. The DPC recognises the important public policy objectives of the General Scheme, namely to empower An Garda Síochána to deploy FRT in limited and specific circumstances. It is crucial to the long-term viability of the proposed legislation that it is compatible with data protection law and that it clearly defines the circumstances in which the deployment of FRT shall be lawful. It is in this spirit that the DPC wishes to share its observations on the General Scheme for the consideration of the Joint Committee.

6. The DPC is Ireland's independent supervisory authority responsible for upholding the fundamental right of individuals in the European Union (EU) to have their personal data protected. In addition to its role in monitoring and enforcing the General Data Protection Regulation (GDPR), it also has important functions and powers related to other regulatory frameworks, including the EU Directive known as the Law Enforcement Directive (LED). The LED regulates the processing of personal data for law enforcement purposes. The purposes for such data processing includes the prevention, detection, investigation and prosecution of criminal offences, or the execution of criminal penalties.

7. The LED differs from the GDPR in that it is a directive that was transposed into Irish law by way of the Data Protection Act 2018. In particular, the LED can differ from the GDPR where an individual's data protection rights are concerned, and can afford organisations greater restrictions to be placed on individual data protection rights to avoid prejudice or obstruction in potential legal proceedings and to protect freedoms and national security. Accordingly, it is the LED and not the GDPR that will be the applicable data protection regulatory framework for any proposed deployment of FRT by An Garda Síochána.

8. In light of the above, the DPC's submission will set out the requirements of the LED both for any legislation that will provide for the deployment of FRT by law enforcement authorities and for those authorities themselves as a regulated entity – or competent authority – under same. The DPC's submission will also provide concrete examples of the requirements that will need to be addressed in the code of practice to be developed by An Garda Síochána prior to the commencement of usage of FRT.

Data Protection Legislative Frameworks

9. As noted above, the processing of personal data by organisations for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, is regulated by the LED, as transposed into Irish law under Part 5 of the Data Protection Act 2018.

10. The LED sets out specific requirements, at a high level, for legislation intended to provide for the processing of personal data by competent law enforcement authorities. Recital 33 LED states that any such legislative measure "*should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights*. *Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.*" This is given legal effect by Article 8(2) LED which requires that "*Member State law regulating processing within the scope of this Directive shall specify at least the objectives of processing, the personal data to be processed and the purposes of the processing*."

11. The DPC notes, therefore, that the lawfulness of the processing of personal data in this context is contingent upon the Bill providing clarity and foreseeability in terms of its effect. The code of practice referred to in Head 3 of the General Scheme will be a key measure in providing sufficient additional detail regarding the operational use of biometric identification, and contributing to the clarity and foreseeability of the application of this technology in practice. The DPC welcomes that Section 47 of the Principal Act (Garda Síochána (Recording Devices) Act 2023) requires that the DPC will be consulted on the code of practice in due course by the Commissioner of An Garda Síochána. Further, detailed expectations for the code of practice are set out later in this submission.

Biometric Identification, Facial Recognition Technology, and Data Protection Law (Head 2)

12. The use of biometric identification, by way of the application of FRT, for the purposes of the prevention, investigation, detection or prosecution of criminal offences has specific data protection implications, which are addressed in this section of the submission.

13. Head 2 of the General Scheme provides that "biometric data" has the same meaning attached to it as Section 69 of the Data Protection Act 2018, but that it does not include DNA, fingerprints or any other data than facial images. For the purposes of the LED, and Part 5 of the Data Protection Act 2018, "biometric data" is one of the identified "special categories of personal data". Therefore, any particular requirements that pertain to the processing of special categories of personal data will apply to biometric identification under the Bill.

14. Article 10 LED provides that special categories of personal data may be processed for law enforcement purposes only, "where strictly necessary". This means that where An Garda Síochána proposes to process biometric data for the purposes of biometric identification, the strict necessity requirement means that it must be demonstrable that the purpose of the processing cannot be achieved by less intrusive means. The DPC notes that Head 4 of the General Scheme provides that, "*Biometric Identification referred to in subsection (1) will be presumed to be necessary and proportionate if its use is in accordance with the applicable code of practice under Section 47*." For the operation of the provisions of the Bill to meet the requirements of Article 10 LED, it will be necessary for the code of practice to clearly set out the circumstances in which the application of biometric identification will be deemed strictly necessary.

15. Biometric identification as defined in Head 2 of the General Scheme means, "*identifying or attempting to identify, natural persons, through the comparison of a person's biometric data with the biometric data which is legally held by An Garda Síochána*." The DPC understands that this comparison is to be carried out by way of the application of FRT, which will require the automated processing of the personal data of affected data subjects. Automated processing in this context is subject to certain conditions under the LED and Part 5 of the Data Protection Act 2018, as set out below.

16. Article 11(1) LED provides that:

"Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller."

17. The DPC notes, in relation to Article 11(1) LED that Head 7 of the General Scheme requires that, "*the results from the any use of the biometric identification must be verified by a member of Garda personnel prior to that result being forwarded to the investigation team*". The DPC considers this to be a key safeguard to protect the rights and freedoms of individuals subject to the automated processing of their personal data. The code of practice should provide further specific detail as to the role of Garda personnel in this regard, including the level of training and expertise in the application of the technology, to ensure the accuracy of the verification of the result of biometric identification.

18. As noted in the above-referenced EDPB Guidelines, facial recognition for the purposes of biometric identification is a probabilistic technology, based upon the estimated match between biometric templates derived from facial images. The comparison of two or more images deduces a higher or lower probability that the person in question is in fact the person to be authenticated or identified. In addition to verification of the result of biometric identification, it will be necessary for An Garda Síochána to demonstrate that the probabilistic thresholds defined by the user or developer of any proposed biometric identification system before it is deployed are sufficiently accurate, and do not give rise to a risk of discrimination against natural persons based on inherent biases.

19. Further to this point, the Guidelines point out that the probabilistic nature of this technology means that it does not provide for definitive results but relies on the probability that two or more facial images correspond to the same person. The probabilistic determination of this result may be reduced depending on factors including the quality of input images, low camera resolution, motion blurring, to name a few. Section 71(d) of the Data Protection Act 2018, and Article 4(1)(d) LED, require that personal data processed for law enforcement purposes shall be accurate. The verification of any results of biometric identification by An Garda Síochána should therefore explicitly address the accuracy of any derived personal data, i.e. the identification of an individual. The Guidelines note that human intervention may only be

considered as a safeguard if the person intervening may critically challenge the results of FRT. Accordingly, the code of practice should address this verification process in significant and substantive detail.

20. The Guidelines set out that most use cases for the deployment of FRT contain intrinsic high risks to affected data subjects on the basis of, inter alia, the probabilistic and automated nature of processing, the novelty of the technology, and the serious nature of the consequences for data subjects of unlawful, inaccurate or insecure processing of their biometric data. For that reason, the DPC considers that the carrying out of a data protection impact assessment (DPIA) by An Garda Síochána shall be a requirement prior to the introduction of any biometric identification system. Furthermore, the Guidelines recommend that the supervisory authority (i.e. the DPC) be consulted as part of the DPIA process, and that the results of this process be published in the interests of transparency and public trust.

21. The DPC notes that Section 47(3)(a) of the Principal Act requires the Commissioner of An Garda Síochána to carry out an assessment of the impact of the proposed code of practice on the human rights of individuals affected by it. This provision is welcomed, notwithstanding the separate requirements in data protection law for the carrying out of a DPIA referred to in the previous paragraph.

Power to use Biometric Identification (Heads 3 and 4)

22. Heads 3 and 4 of the General Scheme address the powers of An Garda Síochána to use biometric identification. The DPC notes the centrality of the code of practice to the lawfulness of the use of biometric identification and thus the processing of personal data for that purpose in the proposed Section 43A(3), and also the reliance upon the code of practice to ground the necessity and proportionality of the use of biometric identification.

23. The proposed Section 43B(3) provides that biometric identification will only utilise images and video that have already been gathered and are legally held or legally accessible by An Garda Síochána. In this context, it will be necessary for the code of practice to provide clear detail as to the sources or categories of personal data that may be in scope for processing for biometric identification purposes in order to meet the requirements for clarity and foreseeability of the effects of the Bill outlined above.

24. Clarity as to the sources of images and footage that An Garda Síochána may utilise for biometric identification is of critical importance in order to ensure that the technology is not deployed in a disproportionate and excessive manner. For example, the DPC would be concerned that in the absence of specific safeguards to prevent such usage, large public databases of facial images, such as those held by the Department of Social Protection (public service cards), the Road Safety Authority (driver licensing), of Department of Foreign Affairs (passports) might fall within the scope of biometric identification. This would represent a significant change in the purpose of such databases in the direction of surveillance of large sections of the population, in a wholly disproportionate manner. The DPC considers that the application of biometric identification to bulk population databases in a non-targeted manner would represent a serious and disproportionate intrusion upon the rights and freedoms of affected persons.

25. Section 71(1)(b) of the Data Protection Act 2018 requires that personal data shall be collected for one or more specified, explicit and legitimate purposes and shall not be processed in a manner that is incompatible with such purposes. It will be necessary therefore for An Garda Síochána, at the time of obtaining images or footage for the specific purpose of biometric identification, to be able to justify so doing on the basis of strict necessity and proportionality. Where images and footage, obtained by An Garda Síochána for a different original purpose, are utilised for the purpose of biometric identification it will similarly be necessary to demonstrate that processing is strictly necessary and proportionate on a case-by-case basis.

26. Where images and footage are to be obtained by An Garda Síochána from third parties for the purposes of biometric identification, the code of practice must be clear as to the legal mechanism or mechanisms that will allow for this processing of personal data.

27. Section 41 of the Data Protection Act 2018 provides that the processing of personal data, including special categories of personal data, for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes of (a) preventing a threat to national security, defence, or public security, and (b) preventing, detecting, investigating or prosecuting criminal offences, and (c) for purposes of legal advice and legal proceedings.

28. These provisions could allow for the lawful obtaining of images or footage by An Garda Síochána from a third party for biometric identification purposes, where those images or

footage were originally processed for a different purpose (e.g. CCTV footage obtained for security purposes in a private car park). However, in the Decision of the Data Protection Commission in the matter of the Department of Health of 16 June 2023, the DPC notes that while, "*section 41 of the 2018 Act permits the re-purposing of personal data where it is "necessary and proportionate" for the purposes of legal advice, claims and proceedings, Article 6(4) GDPR takes supremacy over Irish law, and the compatibility test must apply equally when controllers seek to rely on section 41*."[2]

29. This in essence requires that the provision of images and footage by a third party to An Garda Síochána for the purpose of biometric identification must not be incompatible with the purpose for which it was originally processed. Article 6(4) GDPR states that the assessment of compatibility should consider, inter alia, any link between the purposes for which the personal data was obtained and the purposes of intended further processing; the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed (highly relevant to the present context); the possible consequences of the intended further processing for data subjects; and the existence of appropriate safeguards.

30. Noting in particular the intrinsic high risk to data subjects in the use of FRT for biometric identification purposes, the obtaining of images and footage by An Garda Síochána from third parties for the purposes of biometric identification must be on the basis of strict necessity and proportionality, and must not be excessive or indiscriminate.

31. With regard to the scope of images and footage that may be utilised by An Garda Síochána for the purposes of biometric identification, the Guidelines note that:

> "*Article 6 LED regards the necessity to distinguish between different categories of data subjects. This distinction has to be made where applicable and as far as possible. It has to show effect in the way the data are processed. From the examples given in Article 6 LED it can be inferred that, as a rule, the processing of personal data has to meet the criteria of necessity and proportionality also with regard to the category of data subjects. It can further be inferred that with regard to data subjects for whom there is no evidence capable of suggesting that their conduct might have a link, even an*

[2] Please see: https://www.dataprotection.ie/sites/default/files/uploads/2023-07/20230710_Full%20decision%20IN-21-3-2%20Dept%20of%20Health.pdf

indirect or remote one, with the legitimate aim according to the LED, there is most likely no justification of an interference."

32. The use of FRT for biometric identification purposes on large image databases, or CCTV obtained in the public space, is likely to involve the large-scale processing of the personal data of third parties with no link to the investigative purpose for which the processing is taking place. For the purposes of data protection law, the processing of the personal data of each category of affected data subjects must be justified on the basis of strict necessity and proportionality. In the case of the widespread and indiscriminate processing of the personal data of unrelated third parties, the assessment of necessity and proportionality underpinning the approval of biometric identification must take into consideration the interference with the fundamental rights of all affected data subjects.

33. Head 4, in the proposed Section 43B(2) outlines two distinct purposes for the use of biometric identification namely 1) to locate a person or to follow their movements, and 2) to identify a person. It will be necessary that these two purposes are clearly and separately defined in the code of practice, in particular in terms of the assessment of the necessity of the utilisation of biometric identification in each case.

34. In the case of the first identified purpose, this is a very broad description which will require significant clarification in the code of practice with regard to the categorisation of the types of data subjects who may be in scope, as well as the search parameters for the application of the technology with regard to the time period and geographical area for which the person's movements may be tracked. The following of the movements of a person by way of the use of automated FRT represents a significant and high risk interference with their fundamental rights, and should only be utilised on the basis of strict necessity and proportionality, and only for as long as strictly necessary to progress the relevant investigation.

Approval of the use of Biometric Identification (Heads 5 and 6)

35. Heads 5 and 6 set out the procedural steps for the approval of the use of biometric identification by a member of An Garda Síochána. Head 5 provides that an application to use biometric identification shall be made in writing and shall include:

    a) the purpose of the request and parameters of the search
    b) any other detail that may be specific in the associated code of practice under Section 47

36. It is clear from these provisions that the code of practice will need to provide substantive detail on the application process, and provide clarity to Garda personnel on the circumstances that may give rise to the authorisation of biometric identification on the basis of strict necessity. Additionally, in terms of defining the parameters of a search, including the comparator images and videos, Garda personnel should be required by the code of practice to adhere to the principle of data minimisation, which requires that personal data shall be adequate, relevant, and not excessive in relation to the purposes for which they are processed (Section 71(1)(c) Data Protection Act 2018).

37. We note that the approval of the use of biometric identification shall be made to a member of An Garda Síochána not below the rank of Chief Superintendent, and that this member shall be independent of the investigation to which the application relates. The approving officer must also form a belief on reasonable grounds that the use of biometric identification is necessary and proportionate, and connected to an investigation in relation to a scheduled offence or to the protection of the security of the State.

38. The DPC welcomes that approval of the use of biometric identification must be made by a senior member of An Garda Síochána, independent of the investigation concerned. Again, the code of practice should provide clarity for Garda personnel as to the carrying out of the assessment of necessity and proportionality required to approve the use of biometric identification in order to ensure consistency of application across the organisation. Further safeguards, such as staff training in the implementation of the code of practice and the use of biometric identification in general should be implemented.

39. The DPC also welcomes, under Head 6, the requirement for An Garda Síochána to create and maintain a written list of applications for the utilisation of biometric identification. This is in line with An Garda Síochána's obligations in relation to accountability under the LED and Data Protection Act 2018. This includes general adherence to the principle of accountability under Article 4(4) LED, as well as the obligation to maintain logs of specific processing operations under Article 25 LED.

Use of Biometric Identification and derived information (Heads 7 and 8)

40. Head 7 provides that biometric identification may be utilised to conduct searches on:

a) any images or footage that An Garda Síochána legally retains;

b) any images or footage that An Garda Síochána can legally access

The preceding section of this submission on Heads 3 and 4 (paragraphs 22 to 34) expands on the need for greater clarity as to the scope of images and footage that may be used for biometric identification purposes as well the need for the justification of any utilisation on the basis of strict necessity and proportionality on a case-by-case basis, and with regard to the specific categories of affected data subjects. In this regard, the DPC considers that the proposed new Section 43(1)(b) does not, as presently worded, provide sufficient clarity as to the potential range of images and footage that would be accessible by An Garda Síochána for the purposes of biometric identification. The DPC suggests that this provision should offer further clarification as to the envisaged sources of images and footage, which could be further developed in the code of practice. The DPC is concerned that Section 43(1)(b) could open the door to a scenario in which FRT could be used, for example, to conduct searches of databases of facial images held by public bodies for incompatible purposes as outlined in the preceding paragraphs.

41. In order to meet the legal clarity and foreseeability requirements for legislative measures underpinning the processing of personal data for law enforcement purposes, the DPC considers that the General Scheme and code of practice, as appropriate, will need to provide much greater clarity on the sources of images or footage that may be in scope for biometric identification. A key distinction in the processing of personal data for the purposes of biometric identification will be between the images that will be processed to generate specific biometric templates of individuals, and the processing of other images or footage for probabilistic comparison with the templates of, for example, suspects or missing persons. Greater clarity is also required as to the circumstances that will give rise to the justified processing of personal data for the generation of a biometric template of an identified or identifiable person for the purposes of biometric identification by way of comparison with other images or footage.

42. Head 7 also requires the verification of the results of biometric identification by a member of Garda personnel prior to any result being forwarded to an investigation team. This element of human intervention in an automated processing operation is a key safeguard, the efficacy of which will depend on the expertise and training of the member of Garda personnel concerned, and their ability to critically challenge the comparative parameters and

functionality of the technology itself. Garda policy and procedure in this area, including the code of practice, should explicitly address these points.

43. Head 8 provides that the processing of personal data obtained from biometric identification by a member of Garda personnel shall be lawful for a purpose referred in the proposed Section 43B(1) and in accordance with the code of practice. This further highlights the centrality of the code of practice to the lawfulness of the processing of personal data in this context.

Code of Practice

44. The DPC notes, and welcomes, the requirement under Section 47 of the Principal Act for prior consultation on the code of practice. This submission at several points notes the centrality of the code to the lawfulness of the processing of personal data for the purposes of biometric identification under the General Scheme. Given that the General Scheme does not set out in detail the situations in which deployment of FRT will be permissible, it will fall to the code to set out comprehensive information and instructions for Garda personnel on numerous complex issues. In particular, the code will need to include the following elements:

    a) A clear articulation of the legal basis for processing, reflecting its statutory footing under the Principal Act. The code must ensure that the circumstances in which An Garda Síochána is allowed to deploy FRT are clear to the public and provide sufficient clarity and legal certainty to prevent arbitrary use of these technologies.
    b) Strong affirmative language governing the procedures for deployment of FRT (e.g. An Garda Síochána "shall" or "must" rather than "may" or "should"). The lawfulness of data processing in this context is dependent upon the code contributing to the clarity and foreseeability of the end-to-end effect of data processing operations and any room for deviation from standard operating procedures will undermine this.
    c) Effective internal oversight mechanisms governing the deployment of FRT, and identification and definition of the roles and responsibilities of relevant staff (e.g. authorising officers, technical process owners, system oversight responsibility, etc.). In addition, all usage of FRT should be documented and auditable, in order to discourage any potential misuse of FRT by staff for personal reasons.
    d) Clear descriptions of the processing operations that are envisaged, and in particular the circumstances that will give rise to the justification of the use of biometric identification on the basis of necessity and proportionality.

e) Measures to ensure transparency to the public. This should, as appropriate, include public communications campaigns, online privacy statements, deployment of notices and signage, access to complaint handling procedures by affected members of the public, and provision for making available the contact details of the relevant Data Protection Officer.

f) Clear descriptions of the safeguards to be put in place to protect the fundamental rights of individuals including, but not limited to, measures to ensure the integrity and confidentiality of personal data undergoing processing, and staff training for use of the technology.

g) Measures to prevent the use of FRT on the basis that it is a convenient, effective or popular alternative to conventional police work. The code must ensure that the requesting officer is obliged to set out why less-intrusive alternative methods are not effective in the circumstances as required under Article 10(1) LED. There should be no discretion on a requesting officer to opt for FRT over other workable methods based on mere preference or because it spares additional work that is not unreasonable in the circumstances.

h) Measures to lower the risk of confirmation bias where a suspect is identified using FRT. Given the potentially severe consequences for individuals who are wrongly identified by FRT, facial matches generated by FRT should be treated as investigative leads only, which must be backed up by independent evidence.

i) Clear review periods for any authorisations or implementations of technological solutions. Reviews should encompass an assessment of efficacy of the safeguards to protect the fundamental rights of affected individuals. They will also need to address the ongoing circumstances giving rise to deployment on the basis of necessity.

45. None of this is to suggest that these requirements should be set out in the General Scheme itself. The DPC considers that statutory codes of practice, as provided for in the Principal Act, can be an effective tool for regulating emerging technologies, as they can provide a degree of flexibility alongside the necessary clarity and legal certainty to prevent their arbitrary use. The DPC does wish to highlight, however, that the drafting of the FRT code will likely be a significant body of work, which will require lengthy consultation with the parties identified in the General Scheme. Given the scale and complexity of the issues that remain to be resolved, it is important that the code of practice is not regarded as a mere afterthought or formality, and that the process of creating the code is not rushed.

46. The DPC notes, and welcomes, that Head 14 requires that the draft of the Order in relation to the code of practice shall be laid before the Houses of the Oireachtas, providing an additional level of legislative scrutiny and oversight.

Schedule of offences

47. The DPC notes the schedule of offences for which the General Scheme will permit the use of FRT. It is welcome that the General Scheme limits the use of FRT to particularly serious offences, as this will help to ensure that FRT is only used in scenarios where it is strictly necessary and proportionate.

48. The DPC understands that the Joint Committee has been asked to consider an additional list of serious offences for possible inclusion in this schedule. In this regard, the DPC would suggest, in considering these additional offences, that the Joint Committee has regard to Recital 19 of the draft AI Act[3] which states that law enforcement authorities should only use AI tools in relation to criminal offences that "*are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined in the law of that Member State*."[4]

49. The use of AI for law enforcement purposes (such as in the utilisation of FRT for biometric identification) will be regulated by the forthcoming EU AI Act. The framing of the General Scheme should have regard to the draft AI Act to ensure, as far as possible given the developmental nature of the EU Act, that there is no inconsistency or conflict between these legislative instruments.

Conclusion

50. The DPC acknowledges that FRT has the potential to significantly benefit the work of An Garda Síochána by speeding up investigations and freeing up police resources. However, as the use of FRT presents serious risks to the individual's right to data protection, it is imperative that the General Scheme and code of practice provide the necessary restrictions, limitations and

[3] Please see https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
[4] It should be noted that while the final text of the AI Act is not available at the time of writing, the guidance contained in this Recital stems from Council Framework Decision 2002/584/JHA and therefore reflects longstanding principles of EU law.

safeguards to ensure that any deployment of FRT by An Garda Síochána is necessary and proportionate and respects the requirements of data protection law.

51. Data protection law is not a blocker on the proportionate use of FRT in a law enforcement context, but it requires that the underlying processing of personal data meets the standards of clarity and foreseeability from the perspective of the general public, and is limited to what is strictly necessary as required under the LED. More generally, it should be noted that the regulation of FRT is a complex and rapidly-evolving area, and it will be important to ensure that the General Scheme anticipates future legislative developments at a national and European level.

52. While the General Scheme will provide a legal basis for deployment of FRT by An Garda Síochána and contains a number of welcome safeguards, it leaves many of the most complex issues to be addressed in a subsequent code of practice. As such, the DPC regards the General Scheme as a welcome first step in the process of empowering An Garda Síochána to deploy FRT in a manner that respects data protection law, but significant work remains to be done in order to ensure that usage of FRT respects the requirements of data protection law.

53. Further clarity in particular is required around the extent of images or footage that may fall within the scope of Head 7 of the General Scheme. As the above-referenced EDPB guidelines set out, a scenario involving "mass-scale collection of personal data from individuals not aware of their data being collected" for the purposes of running facial comparisons is likely to represent a disproportionate interference with the rights to respect for private and family life and to data protection under Articles 7 and 8 of the Charter of Fundamental Rights. Accordingly, and in addition to the general requirement for further clarity in the code of practice, it may be appropriate for the General Scheme to rule out the use of any FRT tool that uses web-scraping of images - e.g. from social media and other publicly-accessible resources - to create a proprietary database that law enforcement authorities can access to identify previously-unknown individuals.

54. The DPC thanks the Joint Committee on Justice for the opportunity to make a submission on the General Scheme and would be happy to discuss further any of the observations made in this submission.

Written Submission on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023

17 January 2024

I. Introduction

1. In this comment, we will highlight some of the key issues concerning the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill's compatibility with the International Covenant on Civil and Political Rights (ICCPR), which Ireland is legally bound to uphold through its ratification in 1973. We will focus on the rights to freedom of peaceful assembly, expression, movement, and privacy as guaranteed by ICCPR Articles 21, 19(2)(3), 12(1)(3), and 17(1), respectively. A state's duties under the ICCPR regarding these Articles align closely with similarly binding provisions in the European Convention on Human Rights.[1]

2. We understand that the Bill grants the Garda Síochána the power to use facial identification on *any* past images or video that they have legally accessed for the purpose of (1) crime investigation and prevention and (2) national security, so long as it is not used on live feeds. While in some situations such technology may aid law enforcement and contribute to national security as the drafters of the Bill intend, facial identification, which extracts unique identifiers from individuals without their knowledge, poses a formidable challenge to a wide variety of fundamental human rights, including the right to privacy, in different contexts and situations.[2]

3. The actual and potential uses of facial identification on video or images of protests, or of generally publicly accessible places, would pose a severe burden on the exercise of the freedoms of peaceful assembly, expression, and movement. These very rights are foundational to democratic societies, as the European Court of Human Rights and the United Nations Human Rights Committee repeatedly make clear.[3] The risks of being identified or falsely flagged by facial identification, which is regularly

[1] *See* Article 11 (guaranteeing the right to freedom of peaceful assembly), Article 10 (guaranteeing the right to freedom of expression), and Article 8 (guaranteeing the right to privacy) of the European Convention on Human Rights, and Article 2 (guaranteeing the right to freedom of movement) of Protocol No. 4 to the European Convention on Human Rights.

[2] *See*, for example, Volker Türk, UN High Commissioner for Human Rights, *Artificial intelligence must be grounded in human rights, says High Commissioner* (12 July 2023) ("Facial recognition systems, for example, can turn into mass surveillance of our public spaces, destroying any concept of privacy"); the Office of the United Nations High Commissioner for Human Rights (OHCHR), *Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age* (24 June 2020) (hereinafter "2020 OHCHR Report,"), A/HRC/44/24, para. 31. *See also* the Guarantor for the protection of personal data, *Facial recognition: Sari Real Time does not comply with privacy legislation, the Guarantor for the protection of personal data* (16 April 2021); UK Court of Appeal, *R v. the Chief Constable of South Wales Police* (8 November 2020); and Columbia Global Freedom of Expression, *A Civil Court in São Paulo's judgment on the case of São Paulo Subway Facial Recognition Cameras* (These decisions recognize privacy restrictions caused by the mere use of facial identification, regardless of whether individuals are matched on a watch list.)

[3] European Court of Human Rights, *Kudrevičius and Others v. Lithuania*[GC], para. 91 ("the right to freedom of assembly is […] one of the foundations of [democratic] society."); and Human Rights Committee, *General comment No. 37 (2020) on the right of peaceful assembly (article 21),* (17 September 2020), para.1 ("[the right to peaceful

experienced by members of marginalized populations,[4] create a chilling effect on individuals' ability to freely participate in public protest and move freely in publicly accessible places. Echoing the views of other experts, we believe that international human rights law requires that the most stringent safeguards be applied to the use of facial identification on data recorded in publicly accessible places.[5] This applies regardless of real-time or retrospective use, given the far more extensive data to which the facial recognition system might be applied.[6] Considering the far-reaching and enduring chilling effect associated, human rights law may even warrant the prohibition of such use, as recommended by the European Data Protection Board and European Data Protection Supervisor as well as civil society organizations. [7]

4. The contents of this comment are partly informed by Professor Kaye's tenure as the United Nations Special Rapporteur on Freedom of Opinion and Expression from 2014 to 2020. A 2019 report as Special Rapporteur examined how various advanced surveillance technologies, including facial recognition technologies, impact the right to freedom of expression and of peaceful assembly.[8] Professor Kaye teaches international and human rights law at the University of California, Irvine School of Law; Ms. Hinako Sugiyama serves as Digital Rights Fellow at the University and currently co-teaches the Law School's International Justice Clinic; and Ms. Tomris Ahmad Shah is an advanced law student in the Clinic.

---

assembly] also constitutes the very foundation of a system of participatory governance based on democracy, human rights, the rule of law and pluralism.")

[4] Grother, P., Ngan, M. and Hanaoka, K., *Face Recognition Vendor Test Part 3: Demographic Effects*, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology (December 2019). *See also*, 2020 OHCHR Report *supra* note 2, para. 32.

[5] Clément Nyaletsossi Voule, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association (17 May 2019), A/HRC/41/41, para. 57 ("Surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted [...] under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision."); Human Rights Committee, *General comment No. 37 (2020) on the right of peaceful assembly (article 21)*, CCPR/C/GC/37 (17 September 2020), para. 62 ("for the use of facial identification on a protest, "[i]ndependent and transparent scrutiny and oversight must be exercised over the decision to collect the personal information and data of those engaged in peaceful assemblies and over its sharing or retention, with a view to ensuring the compatibility of such actions with the Covenant); 2020 OHCHR Report *supra* note 2, para. 26; and EU Parliament, *EU AI Act: first regulation on artificial intelligence* (19 December 2023).

[6] EDRi, *European Commission adoption consultation: Artificial Intelligence Act* (3 August 2021), page 12 (see "The "post" RBI loophole"); EDRi, *Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces* (Comparing the use of real-time facial identification and saying "In fact, the extra time entailed by "post" processing uses, which is often claimed to mitigate the risks, has in fact been shown to exacerbate them.")

[7] European Data Protection Board and European Data Protection Supervisor, *EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence* (18 June 2021) ("the EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces."); and EDRi, *Prohibit all Remote Biometric Identification (RBI) in publicly accessible spaces*.

[8] David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression: *Surveillance and human rights* (28 May 2019), A/HRC/41/35.

II. Comments on Individual Heads of the Garda Síochána (Recording Devices) (Amendment) Bill 2023

5. To avoid redundancy, we will start by summarizing the requirements under Article 21, 19(2)(3), 12(1)(3), and Article 17(1) of the ICCPR. We will then refer to these rules in the head-by-head comment.

6. ICCPR Articles 21, 19(2)(3), 12(1)(3), 17(1) guarantee the rights to freedom of peaceful assembly, expression, movement, and privacy, respectively. These provisions share a similar set of standards that require a state to meet the so-called "three-part test" in order to justify the lawfulness of any interference with the rights the ICCPR guarantees.[9] Namely, a state imposing any limitation on those rights must demonstrate that the limitation is (i) provided by law and (ii) necessary and proportionate to protect (iii) a legitimate objective. These are cumulative standards; a limitation may not be justified simply on grounds of "crime prevention or investigation" or "for national security." As further detailed below, the Bill, if the material issues highlighted below are not rectified, would raise serious concerns about the legality and necessity/proportionality requirements.

- **Legality**: For a restriction to be "provided by law," it must be precise, public, and transparent to enable individuals to self-regulate their conduct while limiting the discretion of the state.[10] Furthermore, the state must implement robust safeguards sufficient to eliminate the risk of abuse of power and the chilling effect on individuals' exercise of those rights caused by the state's conduct, such as the use of facial identification.[11] Although the Bill includes some safeguards, we must highlight certain critical deficiencies, as outlined below.

- **Necessity and Proportionality**: Restrictions must target a specific objective and be proportionate to the aim pursued. The necessity test requires the method deployed to be the least restrictive or only means of achieving a legitimate aim pursued.[12] The proportionality test requires the existence of a benefit that is balanced by the degree of infringement of fundamental human rights, and in the law enforcement context, the indispensability of the evidence to the investigation or prevention of the crime, the unavailability of other methods, and the limitation of the scope of

[9] While in its text Article 17 prohibits "arbitrary or unlawful" interference in the right to privacy, the long-standing practice of the Human Rights Committee, as well as the instruments of the UN Human Rights Commission, supports the interpretation that Article 17 requires any interference with the right to privacy to be (i) prescribed by the law and (iii) necessary and proportionate (ii) to achieve a legitimate aim. *See* Report of the Office of the United Nations High Commissioner for Human Rights: *The right to privacy in the digital* age (30 June 2014), A/HRC/27/37 (hereinafter "2014 OHCHR Report"), paras. 21-23.
[10] Human Rights Committee, *General Comment 34: Article 19: Freedom of Opinion and Expression*, CCPR/C/GC/34, para. 25, 12 September 2011.
[11] *Supra* note 5 *General comment No. 37 (2020) on the right of peaceful assembly (article 21)*, paras. 62, 94; 2014 OHCHR Report *supra* note 9, paras. 28-30.
[12] *Supra* note 10 para. 34.

data to be collected and used is at the minimum.[13] The restriction must not "eliminate the right entirely."[14]

- **Legitimacy**: Restrictions may only be imposed to protect legitimate aims. Article 21, 19(3), and 12(3) enumerate such legitimate aims, namely (a) respecting the rights or reputations of others, and (b) protecting national security, public order (*ordre public*), or public health or morals. A State must show in specific and individualized fashion the precise nature of the threat at issue.[15]

7. Please see below for our head-by-head comment of the Bill.

Head	Comment
PART ONE: Preliminary and General	
1-2	No comments.
PART TWO: The Insertion of the following Part 6A into the 2023 Act after Part 6	
3	No comments.
4 Power to use the Biometric Identification	***Section 43B(1):*** *A member shall not utilise biometric identification unless for one of the following principal purposes (a) the prevention, investigation, detection or prosecution of one or more of the criminal offences listed in the Schedule;(b)the protection of the security of the State.* **Recommendation: N/A** **Reasons:** These purposes may pass the legitimacy test on the condition that the Garda Síochána show the precise nature of the threat at issue in a specific and individualized fashion. However, even if the legitimacy test is met, the use of facial identification technology must undergo separate examinations through the legality and necessity and proportionality tests. In this regard, there are several shortcomings in this Bill as outlined below. Regarding which crimes to include in the Schedule, careful democratic discussions should be conducted, especially considering the balance with the fundamental human rights that may be affected. ***Section 43B(2):*** *Without prejudice to the generality of subsection (1), a member of Garda personnel may use biometric identification: (a) to locate a person or to follow the movements of a person in order to progress an investigation into one or more of the offences specified in the schedule or a matter relating to the protection of the security of the State;(b) to identify a person in order to progress an investigation into one or more of the offences specified in the schedule or a matter*

[13] *See* Electronic Frontier Foundation and a coalition of NGOs, *Necessary & Proportionate on the application of human rights to communication surveillance* (May 2014).
[14] David Kaye, *The impact of spyware on fundamental rights*, Testimony to the PEGA Committee of the European Parliament, (27 October 2022). *See* Human Rights Committee, *General Comment No. 31 [80]* (26 May 2004), CCPR/C/21/Rev.1/Add. 13, para. 6 ("in no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right.")
[15] *Supra* note 10 para. 35.

	relating to the protection of the security of the State. **Recommendation:** Define "biometric identification" to encompass only those systems that meet, at a minimum, the widely accepted and reliable technical standards, such as those outlined by the United States' National Institute of Standards and Technology (NIST) or bodies in Europe such as the European Union Agency for Network and Information Security.[16] **Reasons:** This qualification is crucial to address the bias embedded in biometric identification systems that produces disproportionate results in the accuracy of identification for specific demographics such as individuals with dark skin tones, women, and people with disabilities, as repeatedly highlighted by studies and observations from authoritative sources.[17] Such biases further lead to a disproportionate chilling effect on these groups of people. Recalling that it is obligatory for states to ensure fundamental human rights "without distinction of any kind, such as race, colour, sex, [...] or other status" (Article 2(1) of ICCPR), the Bill should restrict the facial identification technologies used by Garda Síochána to those that minimize the risk of biases by adhering to a trusted technical standard. ***Section 43B(3):*** *Biometric identification referred to in subsection (1) will only utilise images and video that has already been gathered and are legally held or legally accessed by An Garda Síochána.* **Recommendation 1:** Specify the exact data sources to be particularly utilized by the Garda Síochána for facial identification, incorporating examples such as passport databases, National Driver License Service (NDLS) records, and most importantly, past police-recorded images and video taken during protests, or more broadly, in a publicly accessible place, if such use is anticipated. **Reasons:** Without specifying which data sources will be used to run facial identification, individuals will not be able to comprehend the potential negative consequences associated with their conduct, such as, for instance, participation in protests. As a consequence, people cannot regulate their conduct accordingly. This may mean, for example, covering their faces during protests to mitigate the risk of identification by Garda Síochána's potential use of facial identification in the future. This, in turn, will cause the Bill to fail in serving as a "law" providing a basis for the use of facial identification, thereby failing the legality test. **Recommendation 2:** Exclude data recorded in a publicly accessible place or during a peaceful protest from the data sources on which facial identification may be run. **Otherwise,** at the very least, establish a defined time frame between the moment images or video are captured and until when facial identification can be employed for data recorded during a protest or, more broadly, in a publicly accessible space. **Reasons:** The indefinite retention and use of images or video for facial identification purposes compels individuals to confront an overwhelming apprehension, such as

[16] *See*, for example, National Institute of Standards and Technology (NIST), *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* (22 August 2016).
[17] *Supra* note 4.

	the fear of being identified at *any time* in the future, to participate in protests or express themselves in a publicly accessible place, considering the potential sharing of videos with the police. Such a deep and long-lasting effect will so severely burden the right to peaceful assembly and expression that it could eliminate the ability to exercise these rights entirely.[18] To ensure the Bill meets the proportionality test, we recommend banning the use of facial identification on images or videos of a publicly accessible place, as proposed by the European Data Protection Board and European Data Protection Supervisor in 2021, and continuously called for by civil society.[19] Or, at the very least, for images taken during protest or in publicly accessible places, a strict time limitation should be imposed for their retention and use. **Recommendation 3:** Qualify the meaning of "legally" held or accessed images and video in a manner that is compatible with human rights law. **Reasons:** Due to the vagueness of the term "legally," databases that the Garda Síochána considers "legally" held or accessed may contain data legally shared by a third party with the Garda Síochána but collected by a third party in a manner that is incompatible with human rights. For example, examples of such data include information collected from individuals without their fully informed and voluntary consent. A notable example would be companies that scrape online data to create a database that is banned by the EU Artificial Intelligence Act.[20] Qualifying the meaning in a manner that is consistent with human rights law is necessary to ensure that any access to data for facial identification purposes complies with human rights norms. ***Section 43B(6):*** *Biometric identification referred to in subsection (1) will be presumed to be necessary and proportionate if its use is in accordance with the applicable code of practice under section 47.* **Recommendations**: Delete this clause. **Reasons:** No matter how meticulously procedural rules are prepared and followed, unexpected situations may arise for which arbitrary application of the law may be enabled. The compliance with the code of practice itself, thus, does not necessarily mean that a specific use of facial identification meets the necessary and proportionate standard. To guarantee the right to seek effective remedy (ICCPR Article 2 (3)) for individuals affected by the use of facial identification that was not necessary or proportionate, individuals should be given the opportunity to claim that the use of facial identification in that specific case was not necessary or proportionate, regardless of compliance with the code of practice.[21]
5 Application for Approval	***Section 43(C)(2):*** *An application under subsection (1) may be made to a member of Garda Síochána not below the rank of chief superintendent.*

[18] *Supra* note 6.
[19] *Supra* note 7.
[20] EU Parliament, *EU AI Act: first regulation on artificial intelligence* (19 December 2023).
[21] 2020 OHCHR Report *supra* note 2, para. 37 ("any use of recording an facial recognition technology should be open to judicial challenges.")

	Recommendations: Replace the authority of "a member of Garda Síochána not below the rank of chief superintendent" with a "competent court" for the use of facial identification on images or video captured in publicly accessible place, or, at the very least, those taken during protests. **Reasons:** Multiple human rights bodies and experts, as well as the EU Artificial Intelligence Act, which was agreed upon by EU co-legislative bodies, support *judicial* pre-authorization for the use of facial identification, especially on data recorded in a publicly accessible place.[22] This is an indispensable element as safeguards are required under the "legality" test. Internal approvals granted solely by Garda Síochána, even if not below the rank of chief superintendent, fall short in terms of independence and impartiality to effectively prevent arbitrary judgment.[23] Thus, if the Houses of the Oireachtas chooses to allow the use of facial identification on records of publicly accessible places, we recommend that the Bill mandate judicial authorization to subject the use of facial identification on records of publicly accessible space to the strictest rule of law.
6 Approval	***Section 43D(1):*** *The chief superintendent of the Garda Síochána to whom an application is made under subsection (1) of section 43C, may approve the application if: (a) he or she is independent of the investigation to which the application relates; (b) he or she believes on reasonable grounds that the use of biometric identification is necessary and proportionate; and(c) he or she believes on reasonable grounds that the use of biometric identification is connected to an investigation of an offense specified in the schedule or a matter relating to the protection of the security of the State.* **Recommendation:** Replace Section 43D(1) (b) ("he or she believes on reasonable grounds that the use of biometric identification is necessary and proportionate") with the following: "he or she must ensure that the biometric identification is necessary and proportionate by determining that based on the evidence: a. the use of facial identification to be the least restrictive or only means of achieving a legitimate aim pursued; b. the existence of a benefit that is balanced by the degree of infringement on fundamental human rights, such as the right to freedom of peaceful assembly, freedom of expression, and privacy; requiring, in the context of criminal investigation, the high, demonstrable probability that a serious crime has or will be committed, the indispensability of the data to the investigation or prevention of the crime, the unavailability of other methods to obtain the evidence; and c. the limitation of the scope of data to be collected and used is at the minimum.

[22] *Supra* note 5.

[23] A case in the United States highlights the importance of the independence and impartiality of the approving body overseeing police use of facial identification. A Black Lives Matter activist, known for organizing over 50 Black Lives Matter protests faced an attempted arrest by the New York Police Department through police's use of facial recognition technology retrospectively. The NYPD identified and tracked down the protestor, besieging his apartment for five hours deploying dozens of officers, a helicopter, riot police, and police dogs, over an incident where the protestor, through a megaphone, vocally expressed dissent without physical force. Amnesty International, *Ban the Scan New York City* (2022).

	Reasons: The existing language is abstract and lenient, failing the necessity and proportionality test under Articles 21, 19(3), 12(3), and 17(1).[24] The proposed amendment is necessary to ensure that the use of facial identification adheres to human rights standards. ***Section 43D(2):*** *An approval granted under subsection (1) may be subject to conditions as the approving member of the Garda Síochána considers appropriate, having regard to the information contained in the application.* **Recommendation:** Qualify that the conditions placed by the approving member of the Garda Síochána may only be in addition to the requirements of subsection (1) and may not curtail on those requirements. **Reasons:** By ensuring that conditions are complementary to, rather than contradictory or restrictive of the stipulated requirements in subsection (1), this recommendation aims to prevent potential loopholes or dilution of the necessary and proportionality standards. ***Addition of New Section 43D(4):*** *Notification to individuals should be made prior to use of facial identification, or, if this contradicts with the investigation's interest, it can be made as soon as possible after the use.* **Recommendation:** Add Section 43(D)(4). **Reasons:** To ensure the right to effective remedies for individuals whose faces are subject to facial identification (Article 2(3)), the Bill should mandate the notification of individuals whose images or videos will be processed or have been processed through facial recognition. In doing so, it should ensure that affected persons are notified of the date, time, location of the images or video on which facial identification will be used, was used, or may be used, and have access to effective remedies in cases of abuse.[25]

[24] *See supra* note 13.
[25] 2020 OHCHR Report *supra* note 2, para. 36 ("All persons [on whom facial identification run] should have the right to access and to request the rectification and expungement of such information that is stored without a legitimate purpose and a legal basis, except when this would frustrate criminal investigation or prosecutions for which these data are needed"); and Concluding Observations on Ukraine (9 February 2022), CCPR/C/UKR/CO/8, para. 42.

7 Use of the Biometric Identification	**43E(2):** *The results from any use of the biometric identification must be verified by a member of Garda personnel prior to that result being forwarded to the investigation team.* ***Recommendation:*** Add the following after the above sentence: "Verified" means, at least, (i) there is no mis-identification of subjects; and (ii) all procedures required for the use of facial identification were followed. **Reasons:** A state is obliged to "ensure" fundamental rights "with no distinction of any kind, such as race [...]" and gender (Article 2(1)). Yet errors such as false positives remain prevalent in facial identification, detrimentally burdening individuals' exercise of their right to peaceful assembly, particularly those with dark skin tones and women due to lower accuracy rates for identification of these demographics.[26] This addition aims to provide a necessary clarity to the verification process, ensuring that it encompasses the absence of misidentification and circumvention of applicable procedural restraints.
8	No comments.
9 Offences	***Addition of Section 43G(4):*** *In cases of the use of facial identification on data recorded during peaceful assemblies, or more broadly, recorded in a public place, a failure to observe any provision of an order (other than an order under section 1(2)) of this Act), or a code of practice, by any member of Garda personnel during the performance of their functions under this Act shall render any evidence obtained inadmissible.* **Recommendation: If the use of facial identification on images or videos of protests or publicly accessible places will not be banned**, add Section 43G(4) following Section 43G(3). **Reasons:** Considering the insurmountable burdens it would impose on the rights to freedom of peaceful assembly, expression, and movement, as well as the right to privacy, if facial identification is used on data from a publicly accessible place without necessary restraints, it is critical to eliminate any motivation for Garda personnel to circumvent the rules applicable to such use of facial identification. This is an important element of safeguards in the duty to "ensure" fundamental human rights.[27]
PART THREE	
10-13	No comments.
14 Amending section 47	***47(4A):*** *Where the Minister proposes to make an order under this section relating to Part 6A:(a) a draft of the order shall be laid before each of the Houses of Oireachtas and (b) the order shall not be made until a resolution approving the draft has been passed by each House of the Oireachtas and (c)an order under this*

[26] *Supra* note 4.
[27] *See* Human Rights Committee, *General Comment No. 20: Article 7 (Prohibition of torture, or other cruel, inhumane or degrading treatment or punishment* (10 March 1992), para. 12.

	subsection shall set out the text of the code of practice to which the order relates and (d)the code of practice shall come into operation on the date specified on the order. **Recommendation:** Add the following after the above sentence: *To decide whether to approve a code of practice, the Houses shall confirm whether a proposed code of practice respects and ensures fundamental human rights, including, among others, the right to freedom of peaceful assembly, expression, and movement, as well as the right to privacy.* **Reasons:** We welcome section 47(4A) that subjects the adoption of a code of practice to democratic control at the Houses of Oireachtas. Nonetheless, to ensure that the code respects and never makes loopholes or compromises human rights, the Bill should clarify the recommended minimum approval criteria.
15	No Comments.
16 Amending section 49	***Section 49(5):*** *The Taoiseach shall ensure that a copy of a report under subsection (3)(b) is laid before each House of the Oireachtas not later than 6 months after it is made, together with a statement of whether any matter has been excluded under subsection (6).* **Recommendation:** Add the following after the above sentence: *For reports related to facial identification, the copy should also be made available to the public.* **Reasons:** We welcome section 49, which extends the oversight of a judge to the use of facial identification and the review of the oversight report by the House of the Oireachtas. Nonetheless, public disclosure of the report ensures the public's understanding of the facial identification's usage and its implications, enabling robust public oversight. It serves as an additional but critical safeguard against abuse of facial identification and its associated chilling effect as requested by the "legality" test.[28]

[28] *See* OHCHR, *Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age* (3 August 2018), A/HRC/39/29, para. 40 ("Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review). *See also* 2014 OHCHR Report *supra* note 9, para. 37 and 38.

Submission to the Justice Committee on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023

Dr Nessa Lynch – 18th January 2024

1. Introduction and Overview

Thank you for the invitation to make a written submission to the Joint Oireachtas Committee on the proposals for legislation to empower the use of facial recognition technology by An Garda Síochána. As I explain below, although currently resident in New Zealand, I am moving back to Ireland in March and so am available for further consultation in this process.

In my submission, I first set out my background and the research and analysis which has informed my comments. I make some overarching comments about facial recognition technology, and then move to commentary on the use-case proposed in the draft legislation. I then consider oversight and assurance mechanisms. My insights are primarily based on the New Zealand experience (which is a comparably sized jurisdiction, also with a single police service, and a comparable legal system and values).

2. My Background and Expertise in Biometrics & Policing

I am a graduate of University College Cork (BCL, LLM) and the University of Otago, New Zealand (PhD). For 12 years, I was an academic at Victoria University of Wellington, New Zealand specialising in criminal law, youth justice and emerging technology and law, particularly in DNA, biometrics and facial recognition technology. I have led influential research on facial recognition technology in New Zealand and globally, particularly in policing. I spent time on secondment at the New Zealand Ministry of Justice and was a member of the New Zealand Law Commission's Expert Advisory Group on the review of DNA legislation which reported in December 2020. I was a special advisor to New Zealand Police on facial recognition technology in 2021, and a foundation member and then Chair of the New Zealand Government's Data Ethics Advisory Group which provides advice on ethical use of data in the public sector in New Zealand. I was the independent advisor on the New Zealand Cross-Government Biometrics Group in 2020-2021. I have consulted regularly for a range of government and non-governmental agencies on biometrics and surveillance technologies.

From March 2022 to February 2024 – I was the Academic Director at New Zealand Police with responsibility for oversight of training at the Royal New Zealand Police College. I was the New Zealand representative on the Australia New Zealand Policing Advisory Authority's Artificial Intelligence group which developed principles for the use of artificial intelligence in policing.

From February 2024, I will be taking a leave of absence from New Zealand Police to take up a position as the Matheson Lecturer in Law, Technology, and Innovation at University College Cork.

The material in this submission draws on a number of published reports and academic publications and I acknowledge the input and knowledge of my co-authors.[1]

[1] Lynch N, Campbell L, Purshouse J, Betkier M. Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework (Law Foundation, 2020), Lynch, N. & Chen, A. Facial Recognition Technology – Considerations for Use in Policing (New Zealand Police, 2021). Available at https://www.police.govt.nz/sites/default/files/publications/facial-recognition-technology-considerations-for-use-policing.pdf, Lynch, N., Gordon, F., & Campbell, L. (2023). Facial Recognition Technology: The Particular Impacts on Children. In J. Purshouse, & A. Roberts (Eds.), *Privacy and the*

My opinions expressed in this submission are not reflective of my employers and are made in a personal capacity.

3. Overarching Comments

- **Facial Recognition Technology is a wide-ranging technology with a spectrum of impact on collective and individual human rights.**

Facial recognition technology (FRT) is in use in a range of applications in the general and the policing context.

It is very important to distinguish the range of use-cases and the spectrum of impact on collective and individual rights.

Common use-cases for FRT range from highly intrusive and high-risk use cases such as live automated FRT and emotion recognition technology to more benign and socially acceptable use cases such as online passport applications, automated passport control at the airport, and "tagging" on social media applications.

The proposals in the draft legislation appear mainly centred around retrospective use in relation to specified serious criminal offences, with assurance mechanisms. Along with the requirement to comply with new European Union standards, this would place the proposed use-case in the medium risk category of our risk framework (Lynch & Chen 2021 -see Appendix 1).

- **The state has a duty to protect human rights, and this includes the duty to investigate and prosecute serious crime and vindicate the rights and interests of victims of crime**

FRT is a technology which has a potential negative impact on collective and individual human rights, particularly privacy, the right to be free from discrimination, the right to freedom of expression and peaceful assembly, and various fair trial rights. There is considerable scholarly and advocacy literature on these potential impacts.

A human rights compliant approach also requires the state to investigate and resolve serious crimes and harms, to provide resolutions for victims, and to promote the safety of the public.

- **Lawful and ethical innovation in technology supports public trust and confidence in policing**

The public is likely to expect that An Garda Síochána considers available technology, particularly where these technologies are in reasonably common use in the public sphere. This is particularly relevant in the investigation of child abuse imagery, where retrospective FRT is in common usage by law enforcement agencies globally. Studies have demonstrated public support for FRT use in relation to serious offences, but there is a lack of minority group representation in these studies.[2]

Criminal Process. Routledge; Lynch, N & Campbell L. (2023), Principled Regulation of Facial Recognition Technology – A View from Australia And New Zealand. In Zalnieriute, M & Matulionyte, R (eds) *Cambridge Handbook on Facial Recognition in the Modern State,* Cambridge.

[2] A Smith (2019) "More than half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly" (5 September 2019) Pew Research Center, Brookings; Ada Lovelace Institute (2019) *Beyond face value: public attitudes to facial recognition technology*. Available at https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/; and Roy Morgan (2017) "Australians not concerned about use of mass facial recognition technology".

Social licence and public opinion can be important in assessing appropriateness of use, but this does not override fundamental human rights.

- **Accuracy of FRT is increasing, but the potential for bias and inaccuracy remains**

Earlier analysis of the use of FRT in a policing context identified the potential for bias due to low levels of accuracy. Reports highlight reduced accuracy levels on people with darker skin tones, and instances of misidentification triggering automated enforcement action.

The evidence is that accuracy rates are improving rapidly as the technology evolves, but this is an aspect which must be monitored closely. Accuracy rates can be significantly diminished by the context – e.g., low or variable lighting, and whether the person is wearing a mask or headgear.

It is important to remember that identification evidence by the human eye is notoriously unreliable, and FRT systems consistently perform better than humans. Nonetheless, appropriate controls must be in place (such as multiple reviews) before any enforcement action should be taken on the basis of a match. This is necessary to ensure public trust and confidence that An Garda Síochána is using the technology in a lawful and justified manner.

It is important to understand that existing lawfully acquired images which will form the comparison images are likely to be primarily drawn from over-policed communities such as ethnic and social minorities and people with disabilities or mental health conditions, and impact must be carefully monitored to avoid perpetrating bias.

- **Privacy in the public space is an evolving area of law and practice**

The use cases comprehended by the draft legislation are likely to involve analysis of images collected in the public space – such as the street, public buildings, or indeed public spaces in the online context. The analysis of imagery and footage collected in the private space is a different question and will generally involve authorisation by way of search warrant.

The common-law approach to public spaces is that there is no, or lesser expectation of privacy compared to one's private residence. While this conceptualisation was more suited to analog methods of surveillance in the public space, such as film photography, digital capabilities such as FRT have a much greater potential impact on privacy and require a different approach.

The new EU Artificial Intelligence Act is indicative of a growing recognition of privacy rights in public spaces.

- **Particular groups, such as children, must have special consideration and protection.**

All people have human rights, but the human rights framework has particular protections for children. Children are recognised as being particularly vulnerable in the investigation of criminal offending, and require special protection that upholds their best interests.

The state is required to take a children's rights compliant approach to the collection, retention and analysis of children's biometric data including facial images. The children's human rights framework requires an emphasis on reintegrative and non-stigmatising resolutions where children are in conflict with the law. This would preclude collection and retention of children's facial images by law enforcement save for exceptional circumstances where public safety is at risk.

Yet, the children's human rights framework does recognise the need to protect public safety and there may be instances where it is necessary and proportionate to use the technology to analyse images of young suspects. These should be exceptional instances, involving a significant risk to public safety.

Consideration should be given in the draft legislation as to whether this power will apply to children, and a children's rights impact analysis should be undertaken.

4. Specific Comments on Retrospective FRT In the Policing Context

As discussed above, FRT encompasses a broad range of use-cases, with a spectrum of impact on collective and individual rights and interests.

The General Scheme indicates that the intention of the proposed legislation is to confine usage to retrospective analysis. However, it is not clear whether this is retrospective search for known people in footage rather than comparing suspect images against images already held in a database. While neither are as intrusive as live automated FRT, the latter has more impacts on human rights, particularly where larger and broader sources of comparison imagery are used.

The proposals in the draft legislation appear mainly centred around retrospective use in relation to specified serious criminal offences, with assurance mechanisms. Along with the requirement to comply with new European Union standards, this would place the use-case in the medium risk category (see Appendix 1).

Our review for New Zealand Police made the following reflections on retrospective FRT use:

- It is important to distinguish speed and scale versus new capabilities. Retrospective use can be categorised more easily as speeding up what is already possible, rather than live automated FRT which is an entirely new capability.
- It is a regular feature of criminal investigations that a police officer or civilian investigator will spend time reviewing still or video images containing people of interest and make manual comparisons against already held images to identify suspects. In many cases this involves considerable amounts of people hours, particularly in complex investigations. The human eye may miss persons of interest, particularly where suspects have attempted to fully or partially hide their face.
- Retrospective FRT analysis of lawfully acquired still images or video footage involves automated searching against a probe image or images. The technology can quickly identify suspect people, drastically cutting the time to identify persons. There is a public interest in reducing the time taken to identify suspects in serious cases, and in efficiency in complex investigations.
- Some have made the point that FRT usage in this context may be privacy protecting, as the search of the images or footage is targeted at persons of interest rather than other people who appear in the public space at the time and whose privacy may be impacted by larger scale analysis or repeated viewings of footage or images by humans.

The breadth of availability of comparison images is important in assessing impact:

- The proposed legislation confines use to lawfully retained images held by An Garda Síochána. It is not clear from the General Scheme whether this is confined to images of convicted persons held by An Garda Síochána or whether it could extend to other types of images

collected in the context of regulatory processes or voluntarily provided images (in the context of provision by victims of crime, or potential suspects).

- The available categories of images should be clarified or cross-referenced in legislation or in the code of practice, as the wider the power the more serious the privacy impacts.
- In particular, images collected from victims of offences or crime scenes should be excluded. A useful analogy is DNA, where it is more generally accepted that those convicted (or in some cases arrested) for serious offending should have their DNA searched against a database.

5. Categories of Offences

The offences listed in the General Scheme are those which involve a high degree of harm to persons and property, and thus use of FRT is more likely to be proportionate, and to adhere to the new European Union regulations.

It is sometimes argued that objectively less serious offending (for instance, more minor property offending) can meet a proportionate threshold for use of FRT where that alleged offending is repeated. These arguments are often made in the context of retail crime or household burglary. Globally, privately owned camera networks which provide imagery from retail crime directly to law enforcement are becoming more common, and some can involve use of retrospective or live automated FRT. Careful consideration would have to be given to expanding available offence types, even in volume crime, particularly given the recent adoption of European Union standards. (see my comments below about direct access to third party camera networks with analytical capabilities).

Use in child abuse imagery cases is common practice in comparable jurisdictions and can be used effectively to identify suspects and also to identify child victims. There is a high degree of social licence for this type of application.

6. Oversight, Assurance and Governance

The draft legislation has robust oversight and governance including a high level of sign-off required within An Garda Síochána. There is also an element of judicial oversight of usage patterns.

Intrusive surveillance technology should be only utilised where necessary and proportionate, and this is specified in the draft.

The Code of Practice or other regulatory or policy mechanism should fill in the operational gaps that are not able to be addressed or foreshadowed in legislation:

- It is likely that An Garda Síochána will procure a proprietary technology application for the proposed use-cases rather than developing in-house. It is vital that high standards of procurement, probity, audit, and data storage standards are followed, and that accuracy levels are in line with accepted standards (such as NIST). Non-compliant aspects of the system should be turned off by the vendor.
- Audit procedures for access to the system should be robust, and samples of access audited regularly to ensure that access is legislatively and ethically compliant.

- A match by the technology system should be subject to human oversight by an appropriately trained person (this appears to be intended to be specified in the legislation).
- Access to third-party camera systems is another issue which should be addressed in legislation or policy. This refers to a situation where a member of the public or an organisation offers access to, or data/analytics drawn from third party camera networks to police. Such networks of privately owned CCTV are increasingly prevalent, and use of analytics is less well controlled. It is important that the same standard be applied.

My report co-authored with Dr Andrew Chen for NZ Police (2021) made a number of other risk and assurance related points on police use of FRT which are relevant here:

- It will be important to embed a culture of ethical data use in An Garda Síochána, through recruit training, guidelines provided at time of issuance of a device or access to a system, and general organisational attitudes. Legislation is not likely to cover every situation, as technology is rapidly evolving, and individual system users and officers must have appropriate training to apply discretion safely and ethically.
- Significant risks lie in individual officers using "shadow IT" on personal devices, where open-source FRT tools are widely available. An organisation's audit procedures can only cover official systems, and ethical frameworks are vital.

Finally, the development of the Code of Practice should have representation/consultation with groups that could be disproportionality affected by the usage, including children, ethnic and social minorities and others who are over-represented in the criminal justice system.

Appendix 1 (from Lynch & Chen, 2021)

Facial Recognition Technology in Policing: Risk Framework

	Low Risk	Medium Risk	High Risk	Unacceptable
Attributes	• Opt-in • Clear consent • Alternative path available • Low-impact at individual level	• Trained staff in-the-loop making decisions • Information sharing between agencies • Private sector suppliers of data • Independently authorised	• Wide data sources (e.g. OSINT) • Third-party data sources without Police standards • Overseas transfers of data • High-impact at individual level • Inaccurate or biased systems • Combining multiple technologies	• Highly automated (human out-of-the-loop) • Unconstrained use without governance or audit trails
Example Applications	• One-to-one verification (with other factors available) • Authentication and Access • Anonymised counting with data minimisation	• One-to-many verification • Retrospective analysis • Anonymised demographic analysis of groups • Isolated live FRT in controlled environments	• One-to-many identification • Live response • FRT on footage from public spaces • Emotion analysis of groups	• Live person tracking using automated FRT • Profile building • Emotion analysis of individuals

7. Closing Remarks

This submission has traversed the General Scheme at a high level. I would be very willing to make further submissions on this legislation when more details are published in due course. I can also provide further detail on any of the points made in this submission.

Written Submission to the Joint Committee on Justice
Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023
Dr. Daragh Murray
18 January 2024

Introduction

1. Thank you for the opportunity to provide a written submission to the Joint Committee on Justice in relation to the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023.
2. I am currently a Senior Lecturer in Law and Fellow of the Institute of Humanities and Social Sciences at Queen Mary University of London, where I lead a UK Research and Innovation Future Leaders Fellowship Project looking at the relationship between advanced technologies and human rights.[1] My research is grounded in international human rights law, and a significant part of my work focuses on the use of facial recognition technology (FRT),[2] and the impact of police surveillance.[3] In 2019 I co-authored an 'Independent Report on the London Metropolitan Police's Trial of Live Facial Recognition Technology',[4] and I have contributed to the UK Surveillance Camera Commissioner's guidance on facial recognition.[5]
3. To frame this submission I will briefly set out the surveillance capability made possible by live and retrospective facial recognition, introduce the potential 'chilling effects' of surveillance, highlight the impact that these chilling effects may have on human rights protections, and discuss the utility and harm associated with FRT. I will then provide substantive comment under Heads 4, 5, and 6. The final section sets out key recommendations.

Key Takeaways

4. Police facial recognition should be subject to a moratorium until further research can examine its effectiveness to policing and potential harm to human rights.
5. Head 4 is overly broad and grants excessive discretion to An Garda Síochána. The powers to use FRT should be based on objective criteria, both to limit the scope for discretion/arbitrariness, and to ensure that FRT can be subject to effective oversight.
6. An assessment of harm to human rights should be built into the approval process.
7. Safeguards are absent from this Bill. The approval process should be independent of An Garda Síochána and consideration should be given to the establishment of an independent and impartial oversight body.

The surveillance capability made possible by facial recognition

8. Live facial recognition (LFR) involves the application of facial recognition technology to video feeds in real time. If a match against the reference database (the 'watchlist') is returned an alert is generated allowing officers to engage the identified individual in real time. Retrospective facial recognition (RFR) involves the after-the-fact application of facial recognition technology to any pre-recorded – i.e. not 'live' – digital content. This may include, for example, surveillance camera footage, body cam footage, an image from social media, or a photo or video taken by a member of the public on a smartphone. At its most simple, RFR may be applied to CCTV

[1] This submission was supported by UK Research and Innovation Grant Number MRT042133/2.
[2] Daragh Murray, 'Police use of Retrospective Facial Recognition Technology: A Step Change in Surveillance Capability Necessitating an Evolution of the Human Rights Law Framework' (2023) The Modern Law Review.
[3] Daragh Murray & others, 'The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe' (2023) Journal of Human Rights Practice; Amy Stevens & Others, 'I Started Seeing Shadows Everywhere': The Diverse Chilling Effects of Surveillance in Zimbabwe'(2023) Big Data & Society.
[4] Pete Fussey & Daragh Murray, 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology', Human Rights, Big Data & Technology Project, July 2019.
[5] Surveillance Camera Commissioner, 'Facing the Camera: Good practice and guidance for the police use of overt surveillance camera systems incorporating facial recognition technology to locate persons on a watchlist' (2019).

footage of a single incident to identify those present.[6] However, the prevalence of surveillance cameras, coupled with the availability of cheap data storage, means that footage from across an entire city may be stored, for a potentially significant period of time. The application of RFR to stored footage allows police officers to 'look into the past' and locate an individual at any point in time, or to identify who was at a particular location at a specific time.

9. It is often assumed that, from a human rights perspective, LFR is more invasive than RFR. This assumption, however, fails to acknowledge the extensive surveillance capabilities made possible by both forms of facial recognition. Three points are relevant in this regard:
    a. While LFR can facilitate engagement with an identified individual in real time, the application of RFR to stored footage can also be 'highly intrusive.[7] RFR can be used, for example, to identify participants at a protest, to track an individual's movements and activities, or to map their public relationships/interactions. The impact on the rights to privacy, freedom of expression, and freedom of assembly is likely to be the same, or similar, irrespective of whether surveillance occurs in real time or retroactively.
    b. Although RFR involves recorded material, it may actually be deployed in near real time, in a manner proximate to LFR. For example, surveillance camera footage may be stored to a database, and facial recognition technology applied to this stored material. The time lag between the recording of the footage and the application of a RFR algorithm may be negligible, and RFR could be used to generate an alert capable of influencing events in real time. In such a scenario, the distinction between LFR and RFR is minimal.
    c. Additional analytical tools (including AI/machine learning tools) may be applied to stored video footage. As noted, a city's surveillance camera feeds may be recorded to a centralised database, to which RFR is applied. This can then be subject to further analysis. For instance, a record could be created of an individual's movements, and an alert generated if they visit a particular location or meet a certain person. When overlaid with other sources, such as an annotated map, an individual's movements can also be used to infer further information, such as where they live, where they work, their relationship status, where and how they socialise, their lifestyle, their sexual orientation, or their political opinion and level of political engagement. An individual's movements can also be analysed over time to generate a pattern of life profile, and any 'unusual' activity flagged. This may be repeated for a nearly infinite number of individuals: the only real limitations are processing power and storage capacity.[8]
10. Both live and retrospective facial recognition represent highly intrusive surveillance capabilities, of themselves. Importantly, however, they also facilitate additional surveillance by making possible the application of analytical tools. While these tools may be useful for the investigation of crime, they represent a step change in police surveillance capability. Both initial and more advanced uses of facial recognition have the potential not only to significantly shift the balance of power between the State and its citizens, but also to undermine democratic life through the emergence of surveillance-related chilling effects.

The chilling effects of surveillance

11. Chilling effects are phenomena that arise when individuals modify their behaviour due to the fear of surveillance. The impacts of chilling effects can be diverse and may, for example, influence what websites a person visits, what books they check out of the library, who they

[6] The main difference in this scenario – compared to officers reviewing the footage – is the speed of review, and the size of the reference database that a facial recognition algorithm can refer to, which will inevitably far exceed that a police officer's memory.
[7] *Glukhin v. Russia*, Judgment, ECtHR, App. No. 11519/20, 4 July 2023, para. 90.
[8] This capability is not merely hypothetical. China has used its facial recognition enabled surveillance camera network to flag 'suspicious' activity, or create a 'virtual fence' preventing individuals from leaving a particular area, or accessing particular sites. See, e.g. Chris Buckley & Paul Mozur, 'How China Uses High-Tech Surveillance to Subdue Minorities', *The New York Times,* 22 May 2019.

meet, what organisations they join, and whether they partake in political activities.[9] Documented impacts include self-censorship and an unwillingness to engage in political discussion,[10] a reluctance to engage with organisations believed to be subject to surveillance,[11] and interference with political or activist groups' ability to organise and mobilise.[12]

12. Facial recognition's potential to induce chilling effects has been explicitly recognised. The European Union Agency for Fundamental Rights noted that: '[t]he use of facial recognition technology can also have a negative impact on the freedom of assembly, if people fear that facial recognition technology is being used to identify them ("chilling effect").'[13] In *Glukhin* v *Russia* – the first and only European Court of Human Rights case to-date to address the use of facial recognition technology – the Court noted that 'the use of highly intrusive facial recognition technology to identify and arrest participants of peaceful protest actions could have a chilling effect in regard of the rights to freedom of expression and assembly.'[14]

Human rights considerations linked to facial recognition technology

13. Any surveillance-related chilling effects will bring numerous human rights protections into play. Worth highlighting here are the rights to privacy, expression, and assembly, given their role in facilitating the development of individuals' personality, and their centrality to democratic functioning. The right to privacy protects all aspects of an individual's personality, including the right to personal autonomy and personal development.[15] Similarly, the right to freedom of expression is recognised as constituting 'one of the essential foundations of a democratic society, and one of the basic conditions for its progress and for each individuals' self-fulfilment'.[16] It is widely regarded as fundamental to the effective functioning of participatory democracy.[17] The right to freedom of assembly is recognised as 'the collective exercise of freedom of expression',[18] and as 'a fundamental right in a democratic society and, like the right to freedom of expression, is one of the foundations of such a society.'[19] Importantly, the protection of personal opinions is recognised as one of the objectives of the right to freedom of assembly.[20]
14. Any interference with these rights caused by a surveillance-related chilling effect has the potential to be severe. The free development of an individual's personality, and free participation in political activities, are rightly regarded as central to democracy society.
15. Two points relevant to surveillance-related chilling effects are worth highlighting:
    a. Chilling effects are most likely to be felt at the margins of society, or by those in opposition to the status quo.[21] That is, they are most likely to limit the political engagement of precisely those individuals who challenge mainstream opinion, introduce alternative political possibilities, and push for change.
    b. Due to their nature, chilling effects may be almost imperceptible in the short term but they may exert a profound influence in the long term. The concern is that, over time,

[9] Amy Steven & others, 'I Started Seeing Shadows Everywhere': The Diverse Chilling Effects of Surveillance in Zimbabwe' (2023) Big Data & Society.
[10] Arshad Imitaz Ali, 'Citizens under Suspicion: Responsive Research with Community under Surveillance' (2016) 41 Anthropology & Education Quarterly.
[11] Amory Starr and others, 'The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis' (2008) 31 Qualitative Sociology; Val Aston, 'State Surveillance of Protest and the Rights to Privacy and Freedom of Assembly: A Comparison of Judicial and Protester Perspectives' (2017) 8 European Journal of Law & Technology, p. 10.
[12] Daragh Murray & others, 'The Chilling Effects of Surveillance and Human Rights: Insights from Qualitative Research in Uganda and Zimbabwe' (2023) Journal of Human Rights Practice.
[13] European Union Agency for Fundamental Rights, 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (21 November 2019), p. 4.
[14] *Glukhin v. Russia*, Judgment, ECtHR, App. No. 11519/20, 4 July 2023, para. 88.
[15] *A, B and C* v *Ireland*, Grand Chamber, ECtHR, App. No. 25579/05, 16 December 2010, para. 212.
[16] *Axel Springer* AG v *Germany,* Grand Chamber, ECtHR, App. No. 39954/08, 7 February 2012, para. 78.
[17] *Centro Europa 7 S.R.L and Di Stefano* v *Italy* , Grand Chamber, ECtHR, App. No 38433/09, 7 June 2012, para 129.
[18] *United Communist Party of Turkey and Others* v *Turkey,* Judgment, ECtHR, App. No. 19392/92, 30 January 1998, para. 43.
[19] *Kudrevicius and Others* v *Lithuania*, Grand Chamber, ECtHR, App. No 37553/05, 15 October 2015, para. 91.
[20] *Navalnyy* v *Russia,* Grand Chamber, ECtHR, App. No 29580/12 and others, 15 November 2018, para. 101.
[21] Daragh Murray & Pete Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' (2019) 52 Israel Law Review 1, 43-47

chilling effects encourage social conformity,[22] and a coalescence around the status quo.[23] There is a concrete risk that they may reduce the breadth of political opinion and undermine political engagement.

16. The advent of digital technology, and the emergence of facial recognition, represent a step change in the State's surveillance capability. This is the first time in human history that the State can monitor a significant proportion of the population and infer information about their day-to-day activities. In this context, chilling effects are likely to be pronounced.
17. The rights referred to above are not absolute rights. That is, they may be limited in certain circumstances. Human rights law establishes a three-part test to evaluate the legitimacy of such limitations, in order to determine whether they constitute a violation of the right in question, or not. This test will be briefly set out here, as it provides a frame of reference for some of the discussion under the Heads.
18. To be legitimate, any interference with the above mentioned rights must be: in accordance with the law, in pursuit of a legitimate aim, and necessary in a democratic society.
    a. To be 'in accordance with the law' there (a) must be a legal basis for a rights interference,[24] (b) that overall legal framework must be of sufficient quality to protect against arbitrary rights interferences, i.e. it must be 'foreseeable' as to its effects,[25] and (c) the legal framework must limit the scope of permissible activity to that which is necessary in a democratic society.[26]
    b. It is generally accepted that policing activity pursues the 'legitimate aim' of preventing disorder or crime, protecting the rights and freedom of others, protecting public safety, or – depending on the nature of the police operation – protecting national security.[27]
    c. The 'necessary in a democratic society' requirement is intended to ensure the overall human rights compliance of a measure; i.e. can that measure be considered necessary in a democratic society, bearing in mind the values associated with such a society.[28] Particularly in the context of surveillance technologies, a core objective of the necessity test is the resolution of the 'competing interests' at play in a specific context.[29] That is, on the one hand, the potential benefit to human rights associated with a surveillance measure and, on the other hand, the potential harm linked to that measure. In the context of facial recognition the competing interests may be the potential benefit to public order or the prevention of crime, while potential harm may be caused by interference with the rights to privacy, freedom of expression, freedom of assembly, and so on. The necessity test also requires an assessment of whether less intrusive 'alternative means' may achieve the same objective.

Assessing FRT's utility and harm

19. The two strands of the 'competing interest' test may be unpacked briefly.
    a. Intended utility: The utility of facial recognition technology is uncertain. While in principle it may prove to be a valuable policing resource, this has yet to be demonstrated. Relatively little information detailing the effectiveness of facial recognition deployments is available, although some information relating to UK deployments has been released. From 2023 to-date the Metropolitan Police Service deployed live facial recognition a total of 24 times, resulting in an estimated 340,672

[22] Jonathon W. Penney, 'Understanding Chilling Effects' (2022) 106 Minnesota Law Review, 1516.
[23] Julie E. Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' (2000) 52 Stanford Law Review, 1425; Neil M. Richards, 'The Dangers of Surveillance' (2013) 126 Harvard Law Review, 1949.
[24] *Kennedy v. the United Kingdom*, Judgment, ECtHR, App. No. 26839/05, 18 May 2010, para. 151.
[25] *Roman Zakharov v. Russia*, Grand Chamber, ECtHR, App. No. 47143/06, 4 December 2015, para. 228.
[26] *Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 106.
[27] See, for instance, *Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 108; *Glukhin* v *Russia,* Judgment, ECtHR, App No. 11519/20, 4 July 2023, para. 84.
[28] *Klass and Others v. Germany*, Judgment, ECtHR, App. No. 5029/71, 6 September 1978, para. 55.
[29] *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 112.

faces scanned, and 57 arrests or disposals.[30] On average for each deployment, the watchlist consisted of 11,466 individuals, and there were 2.4 genuine matches to the watchlist. This indicates an average 'success' rate – where an individual on the watchlist is correctly identified – of 0.0002%.[31] Results from South Wales Police deployments in 2023 are broadly similar. There were a total of 29 live facial recognition deployments, resulting in an estimated 1,328,455 faces scanned, 14 matches to the watchlist, and 8 arrests or disposals, resulting in an average 'success' rate of 0.0008%.[32]

b. Potential harm: The use of facial recognition technology poses a concrete risk in relation to the prohibition of discrimination, given known problems with respect to performance over certain protected characteristics.[33] Beyond this, specific harm is difficult to demonstrate conclusively in the immediate term. The potential for chilling effects is evident, however, and the harm linked to chilling effects is potentially severe.

Head 4: Power to use Biometric Information

20. Human rights law requires that any rights interference be 'in accordance with the law', including that the legal framework be of sufficient quality to limit the scope for police discretion. In *Bridges* the Court of Appeal addressed whether South Wales Police's LFR policy framework was 'in accordance with the law' by reference to what it termed the 'who' and the 'where' questions: 'who' may be included on the watchlist, and 'where' LFR may be deployed.[34] The Court found that South Wales Police's 'policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law.'[35]
21. The 'who' and the 'where' questions remain pertinent to the current Bill. However, it is suggested that other criteria are also relevant, including the nature of offences for which FRT may be used, and whether additional algorithmic analysis may be applied.
22. These four criteria are relevant to the powers established under 43B(1) and 43B(2).
23. New Section 43(B)(1) allows for the use of FRT in relation to a wide range of offences. Two concerns are raised:
    a. The severity of the offences for which FRT may be deployed varies significantly, ranging from robbery to homicide. Given the 'highly intrusive' nature of FRT a 'high level'[36] of justification is required for its use to be considered 'necessary in a democratic society'. It is unclear as to whether the use of FRT in relation to any of the offences included can be considered justified. As noted in §19 above, there is insufficient information available in relation to both the utility of FRT and its harm. Evidently, any concerns in this regard will be amplified in relation to 'less serious' offences. These concerns apply equally to the additional offences for potential inclusion.
    b. The inclusion of offences relating to 'riot' and 'violent disorder' has implications vis-à-vis the rights to freedom of expression and freedom of assembly. Two elements of the right to peaceful assembly are relevant. First, while assemblies with violent intent are not protected by the right to freedom of assembly, isolated acts of violence do not deprive an assembly as a whole of protection, and individuals do not lose the right to peaceful assembly as a result of acts of violence committed by others.[37] Second, a

[30] A disposal is an out of court mechanism for dealing with low level offences.
[31] https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/lfr-deployment-grid.pdf
[32] https://www.south-wales.police.uk/SysSiteAssets/media/downloads/south-wales/about-us/frt/live-facial-recognition/results-of-all-deployments---lleoliadau-for-live-facial-recognition-lfr.pdf
[33] Abeba Brihane, 'The unseen black faces of algorithms' (2022) Nature; J Buolamwini & T Gebru, 'Gender shades: Intersectional accuracy disparities in commercial gender classification' (2018) Conference on fairness, accountability and transparency.
[34] The *Bridges* cases before the High Court of England and Wales, and the Court of Appeal are the only cases in the UK to address police use of live facial recognition.
[35] *R (Bridges)* v *The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, para 94.
[36] *Glukhin v. Russia*, Judgment, ECtHR, App. No. 11519/20, 4 July 2023, para. 86.
[37] *Frumkin v Russia*, Judgment, ECtHR, App. No. 74568/12, 5 January 2016, para. 99.

certain degree of disruption to daily life is a feature of protest.[38] The concern is that the use of facial recognition to identify protestors will give rise to a chilling effect,[39] and that in responding to the actions of certain individuals, the rights to assembly and expression of participants of the protest as a whole are undermined. It is recalled that these two rights are considered to be the 'foundations' of a democratic society.[40]

24. New Section 43B(2) grants extensive discretion to police officers in relation to how FRT is used. Specifically, the 'measures required to progress an investigation' is a subjective criterion that could, in effect, cover any individual who is of interest to the police. It could, for example, include the suspect, a witness, individuals who may have information about a witness or a suspect, and so on. Notably, the *Bridges* Court of Appeal found that a similar criterion – 'persons where intelligence is required' – left too broad a discretion to the police, and so did not satisfy the 'in accordance with the law' requirement.[41]
25. The powers to use FRT should be based on objective criteria, both to limit the scope for discretion/arbitrariness, and to ensure that FRT can be subject to effective oversight.
26. The power in 43B(2)(a) to locate or to follow the movements of a person grants extensive surveillance powers to An Garda Síochána, significantly extending their existing capabilities. While An Garda Síochána may currently have the authority to track individuals, this will necessarily be limited by the availability of appropriately trained officers. The use of facial recognition to perform this task reduces the human resources implications dramatically, allowing for more surveillance operations to occur, in relation to a wider variety of offences. As currently framed this power is unbounded, and no limits or safeguards are established in relation to how it is exercised: it can be applied to virtually any individual of interest to the police in relation to a wide variety of offences.
27. The ability to locate and track an individual must be regarded as highly intrusive in relation to the right to privacy. The fact that this power is essentially unlimited is likely to give rise to significant chilling effects.
28. In the absence of objective criteria limiting the purposes for which FRT may be used to locate and follow individuals,[42] this power is effectively subjective. This leaves extensive scope for discretion/arbitrariness and is unlikely to satisfy the 'in accordance with the law' requirement.
29. Importantly, as currently drafted, 43B(2)(a) can also act as an enabler of more invasive surveillance. As the Bill does not establish any real limits with respect to how this power is used An Garda Síochána can combine this power with the application of more advanced analytical tools. It could be used, for instance, to establish patterns of life, to generate alerts when an individual meets a particular person, enters a particular area, or engages in any form of 'suspicious' activity.
30. There is a lack of clarity in relation to Section 43B(5). It is unclear whether this constitutes an absolute prohibition of live facial recognition, or whether live facial recognition can, in fact, be used in the context of 43B(2).
31. The presumption in 43B(6) that biometric identification is necessary and proportionate if it is used in accordance with the applicable code of practice is problematic. Three issues can be highlighted:
    a. 43B(6) assumes that the use of FRT is justified in relation to all of the offences included in the Schedule. As noted in 22(a), this is questionable.
    b. Both the utility and harm linked to the use of facial recognition will vary, depending on the context. For instance, the extent of the human rights harm linked to the use of FRT at a border crossing will differ significantly from that linked to the use of FRT at

[38] *Kudrevicius and Others v. Lithuania*, Grand Chamber, ECtHR, App. No. 15 October 2015, para. 155; *Laurijsen and Others v. the Netherlands*, Judgment, ECtHR, App. Nos.56896/17, 56910/17, 56914/17, 56917/17 and 57307/17, 21 November 2023, para. 54.
[39] Gl *Glukhin v. Russia*, Judgment, ECtHR, App. No. 11519/20, 4 July 2023, para. 88.
[40] *Navalnyy v. Russia*, Grand Chamber, ECtHR, App. Nos. 29580/12, 36847/12, 11252/13, 12317/13 & 43746/14, 15 November 2018, para. 98.
[41] R *(Bridges)* v *The Chief Constable of South Wales Police* [2020] EWCA Civ 1058, para. 124.
[42] See above §24.

a protest. Equally, the use of FRT to investigate murder will be easier to justify than the investigation of robbery. A blanked assumption of necessity and proportionality does not reflect this nuance.

c. This means that the approval process referred to in Head 6, Section 43D is unlikely to assess the facts or the merits of the application. Instead, it will arguably be reduced to an examination of compliance with the Code of Practice. It is unlikely that the Code of Practice will be able to anticipate all eventualities.

Head 5: Application for Approval

32. New Section 43C(1) outsources significant substantive detail to the Code of Practice. This makes it difficult to analyse this Section in the absence of the Code of Practice. However, a number of issues not included in the Bill, but relevant to the approval process, are highlighted.
33. Key additional elements that could be considered as part of the application for approval process include (a) the context in which FRT will be used, and (b) an impact assessment setting out the anticipated benefit of FRT and the potential harm to human rights. This additional information is important to ensure that the authorisation process anticipated in Section 43D is effective; without this information it is arguably impossible for the authorising officer to assess necessity and proportionality.
    a. The context in which FRT is used will have a significant impact vis-à-vis the potential harm to human rights, which will in turn inform the necessity assessment. In order to facilitate an effective approval process, it is therefore essential that information as to the context is included as part of the application for approval. Relevant context includes, but is not limited to: background as to why FRT is needed, e.g. does it form part of a broader investigation, is that investigation particularly complex (say involving organised crime), is it seeking to identify a witness, or a suspect, is it seeking to develop an intelligence picture; does it bring additional considerations into play, e.g. does the footage relate to a protest, or a religious site, is it likely that political opinion, or other sensitive data, can be inferred.
    b. Setting out the anticipated benefit links to the context (particularly if undertaken as part of a broader investigation) but should be cantered around an articulation of what the officers hopes to achieve, and why this is useful. This links to the requirement that 'relevant and sufficient' justifications for a rights interference be 'convincingly established'. Providing this detail will also facilitate an analysis of the 'alternative means' available.
    c. Identifying the potential harm linked to the use of FRT is essential to the 'necessary in a democratic society' test. Depending on how the application process is approached, the applicant may identify potential harms as part of the application process or,[43] if sufficient information is provided, the authorising officer may identify the harm.
34. As currently formulated, 43C(1)(a) arguably limits the application for approval to technical parameters, and has the potential to result in boilerplate applications and approvals.
35. Explicit reference to the intended utility of FRT (why is it needed?) and the potential harm linked to its use should be included.

Head 6: Approval

36. The question as to what entity should be responsible for approving FRT applications remains open. Typically, the use of overt surveillance does not require independent approval, while the use of covert surveillance does. Whether FRT can be classified as overt or covert is open to debate, as is the appropriateness of this distinction given significant advances in 'overt' surveillance capabilities, including the ability to track, monitor, and profile.

[43] Of course, if the applicant identifies harm, the authorising officer should also undertake this analysis as part of the approval process.

37. RFR is perhaps the most straightforward FRT application to address. RFR occurs without the knowledge of those affected, and without any indication that RFR is being used. As such, it is arguably a 'covert' technique, comparable to communications data requests.
38. LFR is slightly more complex. It occurs in public, where the taking of photographs is typically classified as 'overt'. However, a number of factors differentiate LFR from police photography:
    a. Police officers taking photographs in public are uniformed, and it will typically be evident that they are taking photographs. LFR is different. As it runs on surveillance cameras, and given that surveillance cameras are so prevalent that they fade into the background, it is unlikely that individuals will have any indication that LFR is being used.
    b. The surveillance capability made possible by LFR is markedly different from taking photographs. In *Friedl* the European Commission on Human Rights held that police taking photographs was not intrusive on privacy, but in reaching this conclusion 'the Commission attached weight to the fact that the photographs taken remained anonymous in that no names were noted down, the personal data recorded and photographs taken were not entered into a data-processing system and no action had been taken to identify the persons photographed on that occasion by means of data processing'.[44] LFR evidently changes this calculation completely.
39. In light of its inherent surveillance capability, which the European Court of Human Rights has classified as 'highly intrusive', LFR should be treated as equivalent to a 'covert' surveillance technique.
40. As such, both LFR and RFR should be subject to an authorisation process that is independent of An Garda Síochána. In principle, the authorising body should be judicial in nature, but other forms of independent and impartial bodies are also possible.[45]
41. Accordingly provision 43D(1)(a) which establishes that authorisation may be made by a member of An Garda Síochána, who is independent of the investigation to which the application relates, is arguably inappropriate. This is most clear with respect to RFR.
42. 43D(1)(b) requires that the approving officer must believe that the use of FRT is 'necessary and proportionate'. However, as noted in §33 and §34 above, there is currently insufficient information within the approval process to enable the authorising officer to make this decision.
43. Missing is: information as to the context, why FRT is needed in relation to the case at hand, and the potential human rights harm. A revised authorisation process should include this information.
44. 43D(1) establishes that a chief superintended of An Garda Síochána may approve FRT applications. However, 43C(2) states that applications for approval may be made by a member of An Garda Síochána not below the rank of chief super intendent. This is problematic as approvals will be made by individuals of the same, or lower, rank than the applicant. This reduces the scope for independent and impartial decision-making, as issues of rank, hierarchy, and organisational culture – including possibilities for professional advancement – are likely to come into play.
45. 43D(3) is an important provision in terms of facilitating oversight. This information should be made available to an oversight body. The Code of Practice should ensure that this information is in an easily accessible format, and that the database can be easily analysed to identify trends, facilitate oversight, and so on.

Recommendations

46. In light of the uncertain utility of facial recognition, and the potential to cause significant harm to human rights, the decision to deploy facial recognition should be reconsidered. Police use

[44] Referred to in *Peck* v *United Kingdom*, Judgment, ECtHR, App. No. 44647/98, 28 January 2003, para. 61.
[45] For further discussion on this point see, Daragh Murray, Pete Fussey, Lorna McGregor & Maurice Sunkin, 'Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective' (2021) 11 Journal of National Security Law & Policy.

of facial recognition should be subject to a moratorium until further research can be conducted.

47. Notwithstanding §46, Head 4 is currently drafted in an overly broad manner that grants extensive powers to An Garda Síochána, while allowing excessive discretion with respect to how those powers are exercised. Specifically, the use of FRT to 'progress an investigation' introduces inappropriate subjectivity, while the power to use FRT to locate or follow individuals is unbound. This is problematic in and of itself, and also with respect to the more invasive surveillance capabilities that it makes possible. As it stands, it is unlikely that 43B(1) and 43B(2) satisfy the 'in accordance with the law' requirement. If the Bill progresses further, limits on how FRT is used should be established. These may include defining a range of permitted investigative measures, requiring more concrete links between an individual and the offence in question,[46] and setting limits on the type of algorithmic analysis that may be performed alongside the use of FRT. The powers to use FRT should be based on objective criteria, both to limit the scope for discretion/arbitrariness, and to ensure that FRT can be subject to effective oversight.
48. There is a marked absence of any consideration of harm to human rights. Evaluation of potential harm is central to ensuring that each use of FRT is 'necessary in a democratic society'. An evaluation of harm should be built into the approval and authorisation process, sufficient detail to allow analysis should be included in the Code of Practice, and a requirement that Authorising Officers are trained on how to assess human rights impacts should be included under Head 6.
49. The Bill does not include safeguards. It is important that the application for approval, and the approval itself are auditable. Case law indicates that, with a surveillance capability as intrusive as FRT, it is in principle desirable to entrust supervisory control to a judge, or a non-judicial body, that can ensure guarantees of independence, impartiality and a proper procedure. An independent oversight body, capable of supervising the use of FRT should be established.

[46] These could include limiting the use of FRT to suspects, indicating the degree of suspicion required, and setting limits on the use of other surveillance tools in conjunction with FRT.

Safe Ireland Submission to the Joint Oireachtas Committee on Justice on the Garda Siochana (Recording Devices)(Amendment) Bill General Scheme 2023

Introduction: Safe Ireland

Safe Ireland is the national development and co-ordination body working to eradicate Domestic Violence (DV). We have five distinct functions: investigating the causes and effects of violence and coercion based on sex, gender and sexuality; delivering frontline refuge, support and outreach services; supporting the development, delivery and coordination of frontline Domestic Violence member services; developing best practice guidelines for skilled community-led domestic violence response; and influencing civil society and national strategic policy. This is achieved through collaboration with our network of affiliated independent frontline DV services, local communities, professionals, public bodies, academic institutions, philanthropists and corporate partners.

There are 38 DV services across Ireland affiliated as members to Safe Ireland. Each delivers various combinations of services including national and local crisis helplines, emergency accommodation, housing and practical supports, one-to-one emotional and therapeutic support, information and advocacy, Garda / Court accompaniment, and Welfare advice. 20 out of the 3 services operate staffed DV Refuges.

Our core strategic focus is to change culture, transform responses to sex, gender, and sexuality-based coercion and violence in communities across Ireland, and to progress towards creating a free and Safe Ireland for women, for young people, and for children.

Introduction: This submission

Safe Ireland welcomes this opportunity to make submissions on the General Scheme of the Garda Siochana (Recording Devices) (Amendment) Bill 2023. As requested, we will comment on selected Heads of the Bill in the order in which they appear in the General Scheme. Where we have any recommendation to make, it will be found underneath the Safe Ireland Commentary after each Head. For convenience, the relevant Heads themselves will each be reproduced in contrasting type. Also as requested, we will provide our views on whether any or all of the proposed list of Notable Offences should be added to the Schedule to the Bill, at the end of the section providing commentary on selected Heads of the Bill.

Safe Ireland's position in summary is that the use of facial recognition technologies in criminal investigations should be controlled strictly to avoid challenges by defendants on the basis that it infringes their rights unfairly and unacceptably. Such challenges would be an unwelcome and unintended consequence of any failure to regulate identification by facial recognition in a way that is fair, necessary and proportionate. While it is true that most victims of domestic violence are in no doubt as to the identity of their attacker, a defence may always be put forward to the effect that any particular attack was carried out not by the person responsible for subjecting

the victim to repeated abuse, but by someone else entirely. In these circumstances, the prosecution must have every appropriate tool available to it to help prove its case. That is the context in which Safe Ireland gives its broad support to the introduction of this legislation, which is confined entirely to the use of facial recognition technology to identify suspects, used in any context which is not live. This legislation does not allow the use of facial recognition technology on live moving images as they are being recorded or broadcast in real time, but allows only the later comparison of previously captured images with images already in the possession of law enforcement on a proper legal basis, in order to identify a suspect. This is referred to as "biometric identification" in the draft legislation. The "Principal Act referred to" is the Garda Siochana (Recording Devices) Act 2023.

Head 3: New Section 43A – Applicability of this Part

"3. The Principal Act is amended by the insertion of the following:

'43A. (1) An Garda Síochána's power to utilise biometric identification, shall be limited to the circumstances prescribed in this Part.

(2) Subject to subsection (1)

(i) nothing in this Part shall prevent An Garda Síochána from processing and storing images which have been legally provided by other national or international organisations;

(ii) nothing in this Part shall prevent An Garda Síochána from cooperating with international law enforcement bodies;

(iii) nothing in this Part shall prevent An Garda Síochána from recording or processing images utilising biometric identification, where such recording or processing is a requirement of a measure under European Union Law and Ireland is bound by that measure.

(3) The use of biometric identification under this Part must be in compliance with a Code of Practice as set out in section 47.'" […]

Safe Ireland Commentary:

This section limits the use of biometric identification to the circumstances set out in Part 6A of the Bill, and also, stipulates that its use must follow what is laid down in the Code of Practice provided for at Section 47, while at the same time ensuring that international co-operation will not be hampered by this Bill, provided that it is in accordance with Part 6A. In Safe Ireland's view, this is a cautious yet balanced approach which introduces the safeguard of compliance with a code of practice.

Head 4: New Section 43B – Power to use the Biometric Identification

"4. The Principal Act is amended by the insertion of the following:

'43B. (1) A member shall not utilise biometric identification unless for one of the following principal purposes:

(a) the prevention, investigation, detection or prosecution of one or more of the criminal offences listed in the Schedule;

(b) the protection of the security of the State.

(2) Without prejudice to the generality of subsection (1), a member of Garda personnel may use biometric identification:

(a) to locate a person or to follow the movements of a person in order to progress an investigation into one or more of the offences specified in the schedule or a matter relating to the protection of the security of the State;

(b) to identify a person in order to progress an investigation into one or more of the offences specified in the schedule or a matter relating to the protection of the security of the State.

(3) Biometric identification referred to in subsection (1) will only utilise images and video that has already been gathered and are legally held or legally accessed by An Garda Síochána.

(5) Biometric identification referred to in subsection (1) in the context of live feeds is prohibited.

(6) Biometric identification referred to in subsection (1) will be presumed to be necessary and proportionate if its use is in accordance with the applicable code of practice under section 47.'"

Safe Ireland Commentary:

This section confines the use of biometric identification to the scheduled offences and to any "matter relating to the protection of the security of the State". It also puts it beyond doubt that biometric identification in the context of live feeds is not allowed, and that this form of identification can only use images and video already gathered and legally held or accessed by An Garda Siochana. Finally, it mentions again the importance of compliance with the Code of Practice if its use is to be presumed to be "necessary and proportionate". So, facial recognition technology is only to be used in connection with the prevention, investigation, detection or prosecution of a very short list of serious offences and only if all the other conditions are also met. Safe Ireland's view is that this cautious and restrictive approach is appropriate in these circumstances, because legislation must be robust enough to withstand inevitable legal challenges. However, we do think that the list of scheduled offences is unnecessarily short and that there are some serious offences which should also be included. We will set out our views on which offences should be added to the Schedule under the last [Schedule] Head below and underneath that, we will set our views on which offences from the separate list of Notable Offences circulated on behalf of the Committee, should be included in the Bill.

Head 5: New Section 43C – Application for Approval

"5. The Principal Act is amended by the insertion of the following:

'43C. (1) A member of the Garda Síochána may make an application to use biometric identification in accordance with section 43B. That application shall be made in writing and include the following information:

(a) the purpose of the request and the parameters of the search;

(b) any other detail that may be specified in the associated code of practice under section 47.

(2) An application under subsection (1) may be made to a member of Garda Síochána not below the rank of chief superintendent.'"

Safe Ireland Commentary:

We approve the autious approach to biometric identification procedure which involves seeking the approval of a Chief Superintendent or higher-ranking officer and obliges the Garda seeking such approval to set out in writing the rationale for the request and its limits and also, to include any detail required by the Code of Practice.

Head 6: New Section 43D – Approval

"6. The Principal Act is amended by the insertion of the following:

'43D. (1) The chief superintendent of the Garda Síochána to whom an application is made under subsection (1) of section 43C, may approve the application if:

(a) he or she is independent of the investigation to which the application relates;

(b) he or she believes on reasonable grounds that the use of biometric identification is necessary and proportionate; and (c) he or she believes on reasonable grounds that the use of biometric identification is connected to an investigation of an offence specified in the schedule or a matter relating to the protection of the security of the State.

(2) An approval granted under subsection (1) may be subject to conditions as the approving member of the Garda Síochána considers appropriate, having regard to the information contained in the application.

(3) The Garda Síochána shall create and maintain a written list of applications for the utilisation of biometric identification, which shall contain the details of each application and the reasons why each application was approved or refused, and any further information provided for in an applicable code of practice.'"

Safe Ireland Commentary:

Once again we note with approval the additional safeguards of the independence of the superior Garda officer from the investigation, the use of the expression "necessary and

proportionate" as a criterion for the use of biometric identification, the power to impose conditions on the permission to use biometric identification, and the stipulation that the superior officer must believe on reasonable grounds that the use of biometric identification is connected to the investigation of an offence specified in the Schedule (or to the protection of the security of the State). We are also glad to see that there will be an obligation on An Garda Siochana to create and maintain a list of applications for the use of biometric identification which will include the details of each one and the reasons why it was granted or refused.

Head 7: New Section 43E – Use of the Biometric Identification

"7. The Principal Act is amended by the insertion of the following:

'43E. (1) Where an approval is granted under section 43D, and subject to the parameters set out in an application made under section 43C(1) and any conditions set out under 43D(2), a member of Garda personnel may utilise biometric identification to search the following in order to locate, follow the movements or identify a person:

(a) any images or footage that An Garda Síochána legally retains;

(b) any images or footage that An Garda Síochána can legally access.

(2) The results from any use of the biometric identification must be verified by a member of Garda personnel prior to that result being forwarded to the investigation team.'"

Safe Ireland Commentary:

Once more we note the cautious approach which spells out exactly the uses to which biometric identification can be put, in effect confining it only to images or footage legally retained or accessible by An Garda Siochana, and which also introduces the further safeguard of verification of the results by a Garda member before they are forwarded to the investigation team. We think this is entirely appropriate and that together with the other safeguards already referred to above, this will help create a robust legal framework for the use of biometric identification likely to withstand legal challenges.

Head 9: New Section 43G – Offences

"9. The Principal Act is amended by the insertion of the following:

'43G. (1) A person who, without lawful authority or reasonable excuse, knowingly does any of the following:

(a) falsifies, conceals, destroys or otherwise disposes of any information derived from the utilisation of biometric identification;

(b) permits the falsification, concealment, destruction or disposal of any information derived from the utilisation of biometric identification; will be guilty of an offence.

(2) A person who induces, coerces or requests, without lawful authority or reasonable excuse, a member of Garda personnel to commit an offence under subsection (1) shall be guilty of an offence.

(3) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or

(b) on conviction on indictment, to a fine or imprisonment for a term not exceeding 5 years or both.'"

Safe Ireland Commentary:

It seems to us that a maximum penalty of five years is if anything, on the light side. We would suggest that this maximum be increased to at least 7 if not 10 years.

Head 14: Amending section 47

"14. The Principal Act is amended by the insertion of the following after subsection (4) of section 47:

'(4A). Where the Minister proposes to make an order under this section relating to Part 6A:

(a) a draft of the order shall be laid before each of the Houses of Oireachtas and

(b) the order shall not be made until a resolution approving the draft has been passed by each House of the Oireachtas and

(c) an order under this subsection shall set out the text of the code of practice to which the order relates and (d) the code of practice shall come into operation on the date specified on the order.

Safe Ireland Commentary:

We think it is entirely appropriate that every edition of the Code of Practice for use of biometric identification should be subject to the approval of each House of the Oireachtas.

Schedule of Offences

- Abduction
    - False Imprisonment: Section 15 of the Non-Fatal Offences against the Person Act 1997.
- Aggravated Sexual Assault:
    - Criminal Law (Rape) (Amendment) Act 1990, section 3(1) and section 4(1)
    - Criminal Law (Sexual Offences) Act (2017), section 21(4).
- Aggravated Burglary
    - Criminal Justice (Theft and Fraud Offences) Act, 2001, section 13
- Causing serious harm

  - Non-Fatal Offences against the person Act 1997, section 4 and section 4A •
- Homicide
  - Offences Against the Person Act 1861, section 4
  - Any offence under section 3 of the Criminal Justice Act 1990
  - The Common Law offence of Murder
  - The Common Law offence of Manslaughter
- Rape
  - The Common Law offence of Rape
  - Criminal Law (Rape) (Amendment) Act 1990, section 4
- Riot and Violent Disorder
  - Criminal Justice (Public Order) Act 1994, sections 14 and 15
- Robbery
  - Criminal Justice (Theft and Fraud Offences) Act (2001), section 14
- Child Sexual Abuse
  - Child Trafficking and Pornography Act 1998, section 3
  - Criminal Law (Sexual Offences) Act 2006, section 2

Safe Ireland Commentary:

Our view is that all offences against the person included on this list should remain on it. However, we think the list is too short, having regard to the variety of forms which domestic violence and abuse can take and also, to their many, diverse, durable and often devastating effects on their victims. See further under the next Section.

List of Notable Offences not included in Schedule:

Notable offences not included in Schedule

• Non-Fatal Offences Against the Person Act (1997), sections 16 & 17 (abduction of a child by a parent and abduction of a child by a person other than their parent is punishable by imprisonment for a term not exceeding 7 years.

• Criminal Law (Rape) (Amendment) Act 1990, section 2 (sexual Assault, punishable by imprisonment for a term not exceeding 14 or 10 years).

• Criminal Law (Sexual Offences) Act 2006, section 3 and 3A (defilement of child under 17 years and the same offence but by a person in authority, punishable by imprisonment for a term not exceeding 15 years and 10 year respectively).

• An offence under any of the following provisions of the Child Trafficking and Pornography Act 1998:

➢ Section 4 (allowing child to be used for child pornography, punishable by imprisonment for a term not exceeding 14 years).

➢ Section 4A (organising etc. child prostitution or production of child pornography, punishable by imprisonment for a term not exceeding 14 years).

➢ Section 5 (producing or distributing child pornography, punishable by imprisonment for a term not exceeding 14 years).

➢ Section 5A (participation of child in pornographic performance, punishable by imprisonment for a term not exceeding 10 years).

• Criminal Law (Human Trafficking) Act 2008, section 5 (soliciting or importuning for purposes of prostitution of trafficked person, punishable by imprisonment for a term not exceeding 5 years).

• Criminal Justice Act 2006, section 176 (reckless endangerment of children, punishable by imprisonment for a term not exceeding 10 years).

• Children Act 2001, section 249 (causing or encouraging sexual offence upon a child, punishable by imprisonment for a term not exceeding 10 years).

• An offence under any of the following provisions of the Criminal Law (Sexual Offences) Act 2017:

➢ Section 4 (invitation to sexual touching, punishable by imprisonment for a term not exceeding 14 years).

➢ Section 5 (sexual activity in presence of child, punishable by imprisonment for a term not exceeding 10 years).

➢ Section 6 (causing child to watch sexual activity, punishable by imprisonment for a term not exceeding 14 years).

➢ Section 7 (meeting a child for the purposes of sexual exploitation, punishable by imprisonment for a term not exceeding 14 years).

➢ Section 8 (use of information and communication technology to facilitate sexual exploitation of child, punishable by imprisonment for a term not exceeding 14 years).

• Property

➢ Criminal Damage Act (1991), section 2 (includes arson and criminal damage with intent to endanger life)

• Other

➢ Criminal Justice (UN Convention against Torture) Act (2000), section 2

➢ Misuse of Drugs Act (1977), sections 15A and 15B (drug trafficking offences for drugs over the value of €13,000, which subject to maximum penalties of life imprisonment)

➢ Criminal Justice (Public Order) Act 1994, section 19 (Assault or obstruction of peace officer)

Safe Ireland Commentary:

We have no comment to make on the offences in the last group with the heading "Other". Our view is that it is appropriate, indeed "necessary and proportionate", for all the others on this list of Notable Offences to be included in the Schedule, having regard to their maximum sentences and to the gravity of every one of them, in terms of the serious and long-lasting effects which they are capable of having on the lives of their victims. We would also like to add:

In our view, certain domestic violence-related offences should also be on this list, for the same reasons – they are all likely to have serious and often very long-lasting effects on the lives of their victims, and this is very often reflected in the length of the maximum sentences for these and similar offences.

Safe Ireland recommends that the following domestic violence-related offences which correspond to very common forms of domestic abuse - are added to the list:

- Assault causing harm contrary to Section 3 Non-Fatal Offences against the Person Act 1997 (maximum penalty was recently increased to 10 years);
- Non-fatal strangulation or suffocation contrary to Section 3A Non-Fatal Offences against the Person Act 1997 (maximum penalty is 10 years);
- Stalking contrary to Section 10(2) Non-Fatal Offences against the Person Act 1997 as amended (maximum penalty is 10 years) and its alternate
- Harassment contrary to Section 10(1) Non-Fatal Offences against the Person Act 1997 as amended (maximum penalty is 10 years also); and
- Coercive control contrary to Section 39 Domestic Violence Act 2018 (maximum penalty is 5 years, but in our view, that is too low, having regard to the gravity of some examples of this form of offending).
- Publishing or distributing intimate images of the victim without their consent, or threatening to do so with intent to cause harm to that person or being reckless as to whether such harm is caused, contrary to Section 2 of the Harassment, Harmful Offences and Related Offences Act 2020. It has a maximum penalty of 7 years.
- We also think that the offence of making unwarranted demands with menaces contrary to Section 17 of the Criminal Justice (Public Order) Act 1994 (often called blackmail) should be considered for inclusion on this list as we have seen such demands in the context of domestic abuse. It has a maximum penalty of 14 years.

Please do not hesitate to contact us in relation to any point made in this submission.

Safe Ireland

SI/LSM/Final

Dated this 18th day of January 2024

Contact: Caroline Counihan BL, Safe Ireland Legal Support Manager

GSRDA_06

An Garda Síochána

Oifig an Choimisinéara
An Garda Síochána
Páirc an Fhionnuisce
Baile Átha Cliath 8
Éire
D08 HN3X

Office of the Commissioner
Garda Headquarters
Phoenix Park
Dublin 8
Ireland
D08 HN3X

Láithreán Gréasáin / Website:
www.garda.ie

Ríomhphost / E-mail:
commissioner@garda.ie

Tionscadal Éireann
Project Ireland
2040

Please quote the following ref. number:
Luaigh an uimhir tharaghte seo a leanas le do thoil:

CMR_ 79-659475/19

Mr. Alan Guidon
Clerk to the Committee
Joint Committee on Justice
Leinster House

Re: Submission on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023

Dear Mr Guidon

With reference to the above, I am pleased to attach a submission from An Garda Síochána regarding Garda Síochána (Recording Devices) (Amendment) Bill 2023 (hereafter "the Bill"). An Garda Síochána has provided technology and policing-related input to the Department of Justice throughout the development of the Bill.

This organisation has also provided detailed briefings to members of the Oireachtas. An open invitation stands to all members of the Committee to visit the Garda Digital Innovation Centre to review related technologies such as body worn cameras and also the image analysis tools currently used in investigations.

An Garda Síochána has invested significantly in digital policing, as recommended by the Commissioner on the Future of Policing in Ireland (CoFPI), over the last four years. There has been consistent progress and a number of notable successes including the lifting of the Central Statistics Office reservation on the quality of Recorded Crime Statistics, the roll-out of international policing systems such as the Schengen Information System, multiple national policing systems including one of the first national scale police computer aided dispatch systems in Europe and the rollout of over 14,000 mobile devices with associated policing applications.

This delivery has been supported by the development of in-house data and technology leadership capabilities. This technical and data protection expertise along with operational policing experience and close partnerships with other law enforcement agencies is reflected within the attached submission.

My team would welcome the opportunity to discuss the essential importance of digital policing and biometric data processing to ensuring An Garda Síochána continues to fulfil its mandate in a modern, and rapidly changing, digital society.

For favour of consideration.

Yours sincerely,

J A HARRIS
COMMISSIONER
AN GARDA SÍOCHÁNA

18 **January 2024**

An Garda Síochána

GSRDA_06 (1)

SUBMISSION TO THE JOINT COMMITTEE ON JUSTICE

General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023

18 January 2024

1 Executive Summary

1.1 An Garda Síochána welcomes the opportunity to make this submission to the Joint Committee on Justice on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill (the Bill). The support for digital policing envisaged in the Bill will be a key enabler for An Garda Síochána to fulfil its mandate to prevent and detect crime while maintaining a community and human rights approach to policing. This submission is based both on in house expertise and best practice from close partnerships with other Law Enforcement Agencies (LEAs) and technology suppliers.

1.2 Section 4 includes feedback on the individual heads of the Bill. In order to provide background context, Section 2 outlines the operational policing environment driving the need for digital policing and biometric data processing in particular. Sections 3 expands on this to provide examples of current and anticipated usage of biometric use cases both nationally and internationally.

1.3 An Garda Síochána has the following high level observations on the Bill:

- It is important that the legislation focuses on precise legal and associated technical definitions of what is permitted. Where any prohibition is considered, equal care must be taken to be precise in its scope and application, so as not to inadvertently restrict legitimate and proportionate use of technology;
- The use of new technologies must be subject to appropriate codes of practice and safeguards. However, this must be balanced against avoiding overly cumbersome or bureaucratic processes. For example, the ability to cluster occurrences of victims and suspects in high volume child sexual abuse repositories needs to be standard procedure, not an exception requiring Chief Superintendent signoff every time. Authorisation and oversight mechanisms should distinguish and account for the different forms of biometric processing available and the level/extent of intrusiveness associated. The introduction of excessive steps in routine processes is likely to jeopardise investigations and prosecutions;
- Online sexual abuse crimes do not in many cases carry life sentences. It is essential that we ensure that these abhorrent crimes and cases involving imminent threats to personal safety (such as missing vulnerable persons) are in scope.

2 Introduction

2.1 Digitalisation in society has fundamentally changed the nature of crime and criminal investigations with further disruption inevitable. This includes:

- The ability to collect and process vast amounts of complex digital evidence is now an essential success factor in the prevention and detection of crime as well as wider public and police safety;
- Citizen expectations around transparency and engagement channels with police will continue to evolve significantly. The expectations of partner Law Enforcement Agencies on cooperation in transnational criminal investigations has similarly increased substantially;
- Criminal enterprises are leveraging digitalisation for large scale serious and organised crime. These groups operate on a trans-national basis with no regard for borders. They will seek out the weakest link in the chain in order to limit the impact of law enforcement on their activities. In this regard it is crucial that the technological capabilities of Ireland and An Garda Síochána are at least on a par with other jurisdictions.

2.2 Digital crime can only be detected with digital tools. An Garda Síochána must continue to digitalise in order to anticipate and respond to these trends. The key point is the definition of digitalisation – which is a blend of the electronic world (data, devices and systems) with the human skills of Gardaí (human rights focus, tradecraft and decision making). Increasingly, one is of limited value without the other. An Garda Síochána is strongly committed to this blended model and in particular to the principle that electronic tools exist only for decision support. All decisions that could have significant impacts on a person will be only ever be made by trained, accountable and authorised Garda personnel.

2.3 The 8th principle of the CoFPI[1] report is that policing must be information-led, with associated recommendations on support for effective processes, data quality and access, and increased analytics capability. The 10th principle is that policing must be adaptive, innovative and cost effective, including recommendations on modernising core technology platforms, body worn cameras and timely access to information. CoFPI states that "*The implementation and modernisation of policing in Ireland will depend on the transformation of An Garda Síochána's digital technology in order to supply the information necessary to guide decision-making in all of these areas, and to underpin the accountability of the police."* The Garda Data and Technology Vision[2] supports An Garda Síochána's mission of '*Keeping People Safe*'. Achieving this vision requires full participation in a society which is increasingly digital. An Garda Síochána has made

[1] Commission on the Future of Policing in Ireland Report, 18 September 2018
The Future of Policing in Ireland(web).pdf (policereform.ie)

[2] An Garda Síochána, "Information Led Policing", November 2020, updated and published August 2023
data-and-technology-vision.pdf (garda.ie)

substantial progress to date on digital transformation and data management. This includes the lifting of the Central Statistics Office reservation on Garda data quality, the delivery of multiple national and international policing systems and the establishment of a dedicated data science function staffed by PhD level experts.

2.4 Clearly, it is essential that there is both supporting legislation and public trust in order to continue to deliver modernisation at the pace required. This has to cover support for the ability to both collect and process digital evidence.

3 Use Cases for Image Analysis and Recognition Technologies

3.1 Digital image analysis and recognition technologies are essential policing tools in order to process digital evidence at Big Data scale. Big Data is characterised by its massive volume, velocity (or the rate at which it is generated) and variety (of formats). It is now commonplace for major investigations to include tens of thousands of hours of footage. 10,000 hours of video consists of 900 million images. Even small seized devices such as a mobile phone can contain over a million potential instances of child sexual abuse material (CSAM). Without access to image analysis and recognition technologies, these investigations would become virtually impossible.

3.2 The following is the spectrum of intended use cases for image analysis and recognition technologies by An Garda Síochána, in increasing order of the potential impact on privacy:

1. **Event Detection** – when something changes such as a person appearing on a deserted street;
2. **Object Recognition** – the ability to search for a certain type of object such as a car, a bicycle or a backpack;
3. **Object Clustering** – having identified an object of interest, the ability to search for all occurrences of it in the series;
4. **Person associated non-biometric search** – the ability to search for person wearing, carrying or using an object (such as a hi-vis jacket);
5. **Person associated non-biometric recognition** – having distinguished a person of interest (without associated identity), the ability to search for all occurrences of that person based on their association with objects;
6. **Person biometric recognition and search** – search for occurrences of a person (without associated identity) based on physical characteristics such as facial features;
7. **Person biometric clustering** – having distinguished a person of interest (without associated identity) in a series, find all instances of that person based on physical characteristics;

8. **Retrospective person remote biometric search** – search for all images in a digital evidence series for occurrences of a specific person of interest's image (with or without associated identity established);
9. **Retrospective person remote biometric identification** – Search a database of facial images (with associated identity) for a match with an image.

3.3 An Garda Síochána has never requested the ability to biometrically process data in real time (such as by body worn cameras or other devices). All proposed processing would take place on existing (retrospectively obtained) digital evidence. The similar image analysis and recognition technologies cover all of the above use cases but the nature of the usage determines the potential impact on privacy, not the technology.

3.1 Example: Use of Image Analysis and Recognition Technology in CSAM Investigations

3.1.1 The Garda National Cyber Crime Bureau (GNCCB) is the national Garda unit tasked with the forensic examination of computer media seized during the course of any criminal investigations. Offences 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 crime which are significant or complex in nature network intrusions, data interference and attacks on websites belonging to Government departments, institutions and corporate entities. A large portion of cases (approx. 60%) submitted to GNCCB relate to CSAM (Child Sexual Abuse Material) investigations.

3.1.2 The Bureau is part of Organised & Serious Crime and is staffed by civilian personnel and Garda members of various ranks up to Detective Chief Superintendent. Members of the unit undergo intensive training in the area of forensic computing and cybercrime investigations, and give expert witness testimony in all types of investigations and prosecutions in court. In addition to its forensic and investigative role, GNCCB acts as a liaison with various partner agencies and law enforcement bodies.

3.1.3 The majority of these cases are referred to GNCCB by the Garda National Protective Services Bureau (GNPSB) which receives intelligence and information in relation to CSAM material from outside Law Enforcement Agencies and private entities. GNPSB, on receiving this and subject to legislation will, where appropriate, instigate an investigation which may ultimately lead to Divisional Protective Services Units, operating nationwide, obtaining a search warrant and the seizing of digital devices.

3.1.4 Much of the forensic software used by forensic examiners within GNCCB has inbuilt image analysis and recognition functionality which is intended to deliver enhanced efficiencies and user protections (from the psychological harm associated with continued exposure to CSAM). This image analyser functionality uses biometric and other data to enable Feature, Object and Location recognition. Where such technology

identifies and groups certain images based on an individual's features, it may not necessarily be on the basis of facial features but other characteristics that allow for matching that could fall within the definition of biometric data under data protection legislation. The use of such software is standard practice in every developed country and there have been no legal challenges to its use in Ireland to date in national or trans-national investigations or resultant prosecutions.

3.1.5 Operationally, this means that, within the confines of individual cases, image analysis software will identify and present similar images/videos for review by forensic examiners to assist with identifying and/or locating victims, and suspects, and to enable those processes to occur much more efficiently than they would if this task was undertaken manually. This is made possible by the software clustering multiple images/videos of the same person/people, objects and/or locations together for review by a forensic examiner. The software process supports subsequent manual identification as part of the investigative process but does not actually identify persons.

3.1.6 The experience of the GNCCB is that, as well as being more efficient, this technology is more effective in carrying out the function of analysing images and recognising evidence in the form of faces, objects and locations than human operators are. At the same time, it reduces the invasion of privacy of ordinary citizens innocently captured on such footage by agents of the State, in the form of members of An Garda Síochána.

3.1.7 As previously noted, the software is a decision support tool only. It supports the sifting of evidence but every decision is ultimately taken by an accountable, identifiable member of Garda personnel. Regardless of what decision support technology is utilised by GNCCB, each forensic examiner/investigator is responsible for the evidence gathered and interpretation of same and is accountable for these actions by way of providing a statement which is open to challenge in any future court proceedings.

3.1.8 The use of image analysis and recognition software by GNCCB currently spans use cases 4 to 7 above. An Garda Síochána proposes to modernise and extend its usage (subject to a basis in legislation) to cover use cases 1 and 8 for other types of investigation, but based on newer and even more accurate algorithms than those currently in use.

3.1.9 Virtually every CSAM investigation is digital involving thousands and often millions of images. Putting in place a provision that the use of the Image and Recognition Software (IARS) in respect of each piece of footage must be authorised by a Chief Superintendent carries with it an inherent danger that every such authorisation will be subject of challenge and therefore, must be legally justified by the Authorising Officer; with the result that Chief Superintendents will end up spending lengthy periods in court engaging with this process. It would not be practical to have a Chief Superintendent other than the Head of the GNCCB authorise its use because it is needed in every CSAM case.

3.1.10 It is important that the Bill takes into account the current operation of the GNCCB to avoid the Bureau and An Garda Síochána having to revert to using outdated and manually intensive software tools. This would

be an operational direction that is in the complete opposite to that of every Law Enforcement Agency and would create unnecessary backlogs of work in an already challenging environment.

3.2 Accuracy of Image Analysis and Recognition Software

3.2.1 There has been some commentary about the accuracy of "facial recognition technology" in general such as its potential bias against people with certain demographic attributes. It is important when making these statements to be specific as to the exact algorithm and its version. It is also important to state whether the concern relates to false positives or false negatives for that specific algorithm. The definitive review of the accuracy of facial recognition algorithms is the bi-annual Facial Recognition Technology Evaluation (FRTE) 1:1 Verification by the U.S. Government's National Institute of Standards and Technology[3] (NIST). This evaluates over 500 available algorithms and their variants.

3.2.2 The NIST evaluation demonstrates that some algorithms are *relatively* less accurate for demographics characteristics such as gender and race than others. However, in *absolute terms*, the difference is negligible for the best algorithms. For example, the most recent results published by NIST on FRTE indicate that the algorithm labelled as "cloudwalk_mt_007", submitted for evaluation on the 21st February 2023, provides robust identification scores across demographic variations, with performance exceeding 99% accuracy in the evaluated scenarios:

- Its best False Matching Ratio[4] equals 0.00012 (0.012%) for E. Europe[5] Males aged 20 to 35
- Its worst False Matching Ratio equals 0.00710 (0.71%) for W.Africa[6] Females aged 65 to 99
- Its worst False Non-Matching Ratio[7] equals 0.0016 (0.16%) for S.Asia[8] individuals

3.2.3 These figures and the experience of the GNCCB (on older technology) is supported by testimony given by the Director of the NIST IT Laboratory to the U.S. Congress Committee on Homeland Security[9]. In it, Dr. Romine states that "*The best machine performed in the range of the best-performing humans, who were*

[3] Face Recognition Technology Evaluation (FRTE) 1:1 Verification (nist.gov)

[4] The false match rate (FMR) is the rate at which a biometric process mismatches biometric signals from two distinct individuals as coming from the same individual.

[5] E. Europe indicates subjects from Poland, Russia, Ukraine, see NIST report: nistir_8429.pdf

[6] W. Africa indicates subjects from Nigeria, Liberia, Ghana, see NIST report: nistir_8429.pdf

[7] The false non-match rate (FNMR) is the rate at which a biometric matcher miscategorises two captures from the same individual as being from different individuals.

[8] S. Asia indicates subjects from Iraq, Iran, Pakistan, India, see NIST report: nistir_8429.pdf

[9] Facial Recognition Technology (FRT) | NIST

professional facial examiners. However, optimal face identification was achieved only when humans and machines collaborated." This collaboration is exactly as envisaged in the Garda definition of digitalisation. It is also the approach currently used by the GNCCB and is considered best practice in other Law Enforcement Agencies. An Garda Síochána proposes to use the formal NIST accuracy ratings as a key decision factor in which algorithms to use in the future, following the same approach taken by the Italian National Police when tendering for this type of technology. Dr. Romine's comments are from February 2020 and the accuracy of algorithms has continued to improve rapidly since then. This can be seen in the improvements in the scores for many of the algorithms included in the NIST evaluation over time.

4 Comments on the Heads of the Bill

Head	Comments from An Garda Síochána
Head 1	No Comments
Head 2 - Interpretation	**1.** The definition of biometric data with reference to Section 69 of the Data Protection Act 2018 may be problematic in applying only to biometric processing of facial images. It is not clear what other elements of the definition provided under Section 69 are retained in this formulation. If the intention is to leave unaffected the existing bases for the processing of DNA and fingerprint data this could be made clearer, with the Bill then providing a broader basis for biometric processing. Such processing should include, but not be limited to, processing of facial images so that gait and other distinct biometric characteristics can be provided with a clear basis for processing going forward. Technological solutions may not be able to align with the distinction made between facial images and other identifying unique biometric characteristics that may be processed. **2.** The definition of biometric identification could also be clarified. The current formulation could be read as restricted only to where technology allows for the unique identification of an individual. This would leave a gap for biometric processing where direct identification of an individual is not the intent (e.g. the recognition of an individual in multiple images or a set of footage, without confirming or attempting to confirm their identity, and the capability to sift and collate relevant footage/images of this individual accordingly).
Head 3 – Power to use Biometric Identification	**1.** The Bill should acknowledge other legal bases that may provide a basis for biometric identification. Suggestion to amend 43A(2)(iii) to "*where such recording or processing is a requirement of or authorised by a measure under European Union Law and Ireland is bound by that measure".* Is it also worth including a proviso that domestic law could also provide an alternative basis for biometric identification in specific circumstances to futureproof the Bill? 2. The heading positively asserts the possibility for An Garda Síochána to cooperate with national and international organisation, including processing and storing images. It is not clear whether head 3 provides for the required legal basis for such activities such as full Garda participation in trans-national investigations. 3. The amendment makes reference to Image and footage throughout. Neither term is defined in the amendment or the primary act. It may be better to use the term "document" throughout as used and defined in the 2023 Act[10].
Head 4 – New Section 43B	**1.** While the clarifications in 43B(2) refer to progressing investigations, it would also be worthwhile to include detection of offences as a valid purpose for the use of biometric identification within the scope of 43B(1)(a). This would be a particular consideration for reviews of large amounts of video material to detect potential child sexual abuse material (CSAM), that may then lead on to an investigation of suspected offences listed under the Schedule to the Bill.

[10] Number 32 of 2023, Garda Síochána (Recording Devices) Act 2023, Part 1, Section 2

	2. 43B(6) is helpful in establishing a clear link between necessity and proportionality, and therefore lawfulness, with use in accordance with both the requirements of the Bill and an applicable code of practice. The development of a relevant code of practice for biometric identification would involve a Data Protection Impact Assessment (DPIA) of the anticipated use cases and approval/oversight mechanisms. 3. Point (5) expressly prohibits the usage of Biometric identification in the context of 'live feeds'. While An Garda Síochána has not requested to utilise Biometric Identification in this context, it is important to note that the Bill contrasts with the latest available draft of the EU AI Act as outlined in the 9 December Press Release[11]: *"The use of real-time remote biometric identification in publicly accessible spaces (i.e. facial recognition using CCTV) for law enforcement purposes is prohibited, unless used in one of the following cases:* *4. Law enforcement activities related to 16 specified crimes;* *5. Targeted search for specific victims, abduction, trafficking and sexual exploitation of human beings, and missing persons;* 6. *The prevention of threat to the life or physical safety of persons or response to the present or foreseeable threat of a terror attack.* 4. Head 4 and General Comment: There is inconsistency in the draft amendment with the terms "*Garda Personnel*" and "*Garda Member"* used interchangeably. For example in Head 4 Section 43 (b)(1) states "A member shall not utilise biometric identification…." And in Section 43(B)(2) it states "a member of Garda Personnel may use biometric identification". It is recommended that the term "*Garda Personnel*" be utilised throughout the amendment except where there is a specific need to differentiate that Garda (member) powers are required to perform a certain function.
Head 5 – Application for Approval	1. The heading defines strict rules for An Garda Síochána (personnel) members with regards to the utilisation of systems and tools that perform 'biometric identification'. The section prescribes that – 43C (1): 2. "*A member of the Garda Síochána may make an application to use biometric identification in accordance with section 43B. That application shall be made in writing and include the following information: (a) the purpose of the request and the parameters of the search;"* 3. Within the context of an investigation and related analysis of large amount of evidentiary material where multiple offences may occur, it is not feasible to expect that the 'parameter of the search' are known *a-priori*. This is particularly the case in CSAM investigations and in the case of riots. As in any analytic work, search terms and hypotheses evolve and change as the material is inspected. Furthermore, search parameters may need to be adapted also depending on the specific capabilities and accuracy of the software used for biometric processing. The current wording is likely to cause an excessive administrative burden and delays to the investigation team.

[11] European Parliament Press Release (EU AI Act: first regulation on artificial intelligence | News | European Parliament (europa.eu))

	4. In the case of CSAM investigations, the analytic software pre-processes biometrically all the images and videos imported (including converting videos to individual frames). This is to facilitate search and matching of 'unknown' CSAM material (i.e. video and images not already catalogued and known to LEAs). The specific details of the biometric processing and search may be proprietary to a vendor, making it difficult to comply with this wording. This could have profound impacts on the use by the GNCCB of the latest forensic and Image Analysis and Recognition Software. 5. The requirement for the "application shall be made in writing" should not prevent the use of a computerised record to record all the relevant details as opposed to using a manual paper record. 6. Head 5 Section 43(C)(1) States "*A member of the Garda Síochána may make an application to use biometric data…*" The use of the words "*to use*" could potentially limit the scope of who can actually perform the "biometric identification" and does it have to be the explicitly the member making the application, if so this should not be the case as it is too restrictive. Head 7 Section 43(E) provides some additional clarity on this. However, it is suggested that the wording be adjusted as follows: "*A member of Garda personnel may make an application for the processing of a document for the purpose of biometric identification*", leveraging the definitions of *document* and *processing* in the 2023 Act (as cited earlier).
Head 6 - Approval	1. The requirements listed under 43D(1) may be impractical in certain scenarios in requiring each authorisation to be investigation-specific in all circumstances and for the authorising Chief Superintendent to be independent of the investigation. Use of biometric identification as a detection tool is not factored in here, and so the use of biometric identification to detect images that may give rise to an investigation does not seem to be possible to be authorised in the absence of an investigation already being underway that informs the rationale for the application. This use of biometric identification as an aid to detection activity would, however, seem a useful facility for certain investigation types to have scope to seek authorisation for under the Bill, subject to the appropriate conditions related to this particular use of biometric identification. Such investigation types would include riots and CSAM material where there is an ongoing requirement to review large amounts of material, as compared to investigation specific authorisations to review CCTV collected within a certain area related to an individual incident. 2. The heading defines procedures related to obtaining approval for 'biometric identification'. Point 43D (1) (a) prescribes that the 'chief superintendent' approving the application is 'independent of the investigation to which the application relates'. The 'independence' requirement increases the administrative burden highlighted in the commentary regarding Head 5. Within the context of the GNCCB, all the case of CSAM investigations rely on analytical software that performs biometric processing of all the evidentiary material. 3. Again, the requirement for a "written list" should not prevent the use of a computerised record to record all the relevant details as opposed to using a manual paper record.
Head 7 – Use of Biometric Identification	**1.** The requirements in 43E(2) seem to imply that the verification of results must be carried out separate to an investigation team. Again this may not be practical in all circumstances and does not allow for circumstances where subject matter experts may be embedded within investigation teams. This section could be removed since

	the biometric processing will be carried out in accordance with legislation and the required code of practice which will make it clear that final identification decisions are made only by Garda personnel which is the fundamental safeguard against automated machine decision.
Head 8	No comments
Head 9 - Offences	**1.** An Garda Síochána supports the strong deterrents against the misuse of biometric identification by Garda personnel.
Heads 10 - 15	No Comments
Head 16 – Amending Section 49	**1.** Given the proposed extension of judicial oversight under Section 49 of the Recording Devices Act 2023 to include the authorisation and use of biometric identification, and the reporting requirements for the designated judge under this Section, there would seem to be scope to extend the authorisation mechanism to account for detection activity as suggested above in addition to the investigation-specific authorisations provided in the current draft. Such activity, rather than investigation specific authorisations would be subject both to specific conditions for their authorisation and the judicial oversight and reporting requirements outlined here, providing necessary transparency as to the use of biometric identification by An Garda Síochána in the performance of its functions.
Appendix II – Notable Offences Not Included	**1.** It is worth noting that the inclusion of offences listed under Sections 16 and 17 of the Non-Fatal Offences Against the Person Act 1997 would not allow for use of biometric identification for missing persons cases where abduction is not believed to be a factor. **2.** It would be useful to have additional offences under Child Trafficking and Pornography Act 1998 considered but the use case for biometric identification in these circumstances may be one primarily of detection of offences (e.g. using biometric identification or similar tools to search a large number of files to identify relevant images for review). It may be difficult to demonstrate the value and necessity of the use of biometric identification for the purposes of a single investigation in such cases in advance of the use of the tool. **3.** Suggestion to include Misuse of Drugs Act 1977 offences but only for drug trafficking offences over the value of €13,000 could prove problematic to implement – there seems to be potential for a scenario where use of biometric identification assists with seizure of drugs below this value threshold. Would the authorisation and use of biometric identification in this case be invalid and/or unlawful?

Submission to the Joint Committee on Justice General Scheme of the *Garda Síochána (Recording Devices) (Amendment) Bill 2023*

18 January 2024

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

Introduction

1) I am glad to see the Joint Committee on Justice's call for submissions on this draft bill, and I am grateful to be asked to contribute to the discussion. There is much potential for strengthening and reforming Irish legal structures to assist An Garda Siochana and increase their capacity to manage and respond to crimes and issues of public order.

2) I am an Assistant Professor in Criminology at Maynooth University School of Law and Criminology and an Adjunct Professor in Criminology at the University of Ottawa. In responding to this submission request:

a) I draw on knowledge obtained through research, study, and teaching on the law, policies, and practices relating to data protection and privacy; of the law, policies, and practices relating to police use of (surveillance) technologies such as body-worn cameras, drones, and facial recognition technologies; and of policing, security, and surveillance technologies and criminal justice policy implementation obtained through my education, training, and ongoing research as a lecturer;
b) I rely on my past written academic papers, reports, and public opinion pieces examining various privacy-related aspects of the use of surveillance technologies and Facial Recognition Technology (FRT). I also rely on a series of think-ins that I have recently run with members of the public on the topic of FRT, specifically.

3) This submission does not address each element of the draft Bill, but focuses on which subject matters I have the most expertise. Further, the order in which my submission addresses the Bill's Heads and Subheads is not a comment on their relative importance.

4) It is my view that, in determining what recommendations to make regarding the draft Bill, the Joint Committee should give the strongest possible weight to:

a) international law and policy frameworks, and related official documents from international governmental bodies, especially the EU Charter of Fundamental Rights and the European Convention on Human Rights (ECHR), the EU Law Enforcement Directive (Directive 2016/680) relating to police processing of personal data, the EU's forthcoming AI Act, the European Data Protection Board's Guidelines (EDPB 05/2022) on the use of facial recognition technology in the area of law enforcement, and the Office of the High Commissioner for Human Rights' (OHCHR) report on The Right to Privacy in the Digital Age;
b) research that addresses the effectiveness of FRT systems, or lack thereof,[1] and new surveillance technologies by police services, and the adherence to/and implementation

[1] See: Fussey and Murray (2019) 'Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology'. Available at: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf; Big Brother Watch (2023) 'Biometric Britain: The Expansion of Facial Recognition Surveillance'. Available at: https://bigbrotherwatch.org.uk/wp-

of related national and international law, including, but not limited to, that undertaken locally; and,

c) international experts on, and experiences of, the use of FRT[2] (especially by police agencies). Ireland is in a strong position to explore work in other jurisdictions and to embrace or discount various approaches, depending on their effectiveness in preventing human rights abuses that occur because of biometric data collection and surveillance.

5) I would like to make the following points at the outset of this submission:

a) **Facial recognition technology (FRT) represents a negative step-change in the way surveillance is carried out**, because it is both qualitatively and quantitatively different from existing visual surveillance technologies, and databases. FRT can be applied live and retrospectively to video and photo imagery. It can be used in conjunction with existing surveillance technologies and databases. FRT can make use of data that is scraped and create enormous volumes of data to profile individuals - including individuals who have never been involved in a crime (see Amnesty International 2022, McSorley 2021).

b) **FRT relies on vast databases of images to operate**, and uses algorithms to "pick out specific, distinctive details about a person's face and make a judgment of its similarity to other faces" (EFF 2023). This can be done through face verification, a type of one-to-one matching, which matches images of a known individual to show both images that represent the same person (Clarke 2003). Face identification determines who a person is, or, in some instances, is not, through one-to-many matching. In this case, individuals may have their faces scanned and checked against a database of known individuals to determine who they are. However, some FRT calculate probability scores for a match in a database rather than identifying an individual positively. Some face recognition systems, instead of positively identifying an unknown person, calculate a probability match score between the unknown person and specific face templates stored in the database. Instead of a single match, the system offers up several matches ranked by probability score (EFF 2023). This puts privacy at risk as individuals who have nothing to do with an event might still be brought into investigation if their probability score is high enough.

c) The data justice and surveillance implications of FRT are clear: **FRT is an invasive technology by design** and thus poses risks to the public when being used for law enforcement purposes. Impacts on civil liberties should not be understated: chilling effects would include but are not limited to undermining the idea of anonymity in public (impacting democratic rights as elaborated on in point 7), function creep is often seen with surveillance technologies where a system is initially introduced for one purpose but later is used in a more widespread manner, and net-widening further points to the

content/uploads/2023/05/Biometric-Britain.pdf; American Civil Liberties Union (2018) 'Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots'. Available at: https://www.google.com/url?q=https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28&sa=D&source=docs&ust=1705578259481692&usg=AOvVaw0kR-qaZFitzsuvxvUNZYH7.

[2] See this example of oversight in the Belgian context: van Brakel, R. (2021). 'How to Watch the Watchers? Democratic Oversight of Algorithmic Police Surveillance in Belgium'. Surveillance & Society 19(2): 228-240. Available at: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14325.

concerns around including individuals in searches (because they are in database on which the software runs) when they are not suspect or party to any crime.[3]

d) More **surveillance is not the panacea for all criminal ills or, indeed, wider challenges facing AGS with public order policing**. While the idea of FRT might seem like the solution to 'catch criminals', such as in the riots in Dublin in November 2023, the technology would largely have been rendered useless by any variety of simple physical barriers like baseball caps, face coverings, glasses, and hoods to name a few examples.[4] This is a small, brief anecdote, of which there are many, quite unbelievable, real-world examples of how (advanced) technologies fail. Moreover, with respect to using FRT in riots, the EDPB guidelines outline such a case and say it is unlawful (EDPB 2023). Therefore, I would ask the Joint Committee to consider whether FRT really is the best allocation of resources.

e) **The use of FRT by AGS calls into question the scope and scale of data collection, use, and storage as well as surveillance of the population**. The legality, necessity, and proportionality of FRT must be considered (Privacy International 2023). At a very minimum, we need to consider extra judicial oversight for such systems, and red-lines for certain uses like mass surveillance of protestors in public spaces should be enshrined in the Bill.

f) **The proprietary nature of these technologies means the algorithms and practices that drive an FRT system are often unexplainable to government institutions and the public alike**. Notwithstanding problems with the technology itself (including bias and inaccuracy, see Birhane et al. 2023, and effectiveness, see Fussey and Murray 2019), I would like to highlight concerns about the practices employed by FRT companies. In 2020 Clearview AI were formally investigated by the Office of the Privacy Commissioner of Canada (OPC), the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta to see if they i) obtained the necessary consent for the collection, use, and disclosure of personal information, and ii) if they collected, used, and disclosed personal information for an appropriate purpose. Canadian police services were also found to be using the technology[5] as part of a free trial service provided by the company, and this was also found to be in violation of the Canadian *Privacy Act*. In 2021, the joint investigation "found Clearview's purposes to be inappropriate where they: (i) are unrelated to the purposes for which those images were originally posted; (ii) will often be to the detriment of the individual whose images are captured; and (iii) create the risk of significant harm to those individuals, the vast majority of whom have never been and will never be implicated in a crime. Furthermore, it collected images in an unreasonable manner, via indiscriminate

[3] See EDPB Guidelines 05/2022, as above. Also: Lehr and Crumpler (2021) 'The Impact of FRT Deployment on Human Rights'. Center for Strategic and International Studies Report. Available at: https://www.jstor.org/stable/pdf/resrep33749.7.pdf; Purshouse and Campbell (2019). 'Privacy, crime control and police use of automated facial recognition technology'. Criminal Law Review (3), 188-204.

[4] See NIST (2020). 'IST finds flaws in facial checks on people with Covid masks'. Biometric Technology Today (8):2. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7494276/#:~:text=Because%20real%2Dworld%20masks%20differ,about%200.3%25%20of%20the%20time.

[5] Office of the Privacy Commissioner of Canada (2021) 'Police use of Facial Recognition Technology in Canada and the way forward - Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI'. Gatineau: Victoria Street. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1.

scraping of publicly accessible websites"[6]. In Europe, numerous actions and judgments have been made against Clearview AI (EDRi 2022).

While the Department of Justice would follow the typical process and tender for an appropriate provider of FRT, it is worth the Joint Committee's time to **consider how FRT companies operate, and whether it is acceptable for AGS to use FRT based on images scraped from a variety of online and public locations**. There are less than a dozen FRT providers internationally, one of the largest of which is Clearview AI. Moreover, there must be clear parameters around the data that AGS can legally access. This is especially significant as questions have already been raised around an unlawful database created with biometric identification from the Department of Social Protection's Public Service Card (see Bowers 2023, ICCL 2020).

PART ONE

6) Head 2: Amendment to Section 2 of Principal Act – INTERPRETATION

In this head, "biometric data" is defined as "the same meaning attached to it in section 69 of the [Irish] Data Protection Act 2018 but does not include DNA, fingerprints or any other data except for facial images." However, "biometric data" in the Irish Data Protection Act 2018, as per its legal definition in EU law, is defined as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual that allow or confirm the unique identification of the individual, including facial images or dactyloscopic data". This new definition of biometric data as introduced in the draft Bill directly contradicts (existing) EU law, which supersedes Irish law.

Furthermore, this head defines "biometric identification" as identifying or attempting to identify individuals by comparing biometric data against biometric data legally held by AGS. Given the potential abuses that could occur through misuse of FRT, additional clarification is needed around what biometric data would be legally held by AGS.

PART TWO

7) Head 4: New Section 43B–Power to use the Biometric Identification

This draft (Amendment) Bill aims to create an appropriate legal framework to authorise the use of biometric identification (or FRT more specifically) by AGS - and must consider the need for the deployment of this technology. Additionally, this draft (amendment) Bill comes at a time when ongoing international and European bodies (Heikkilä 2021) are cautioning against unnecessary biometric data surveillance, as it represents a significant interference with human rights, including the right to privacy.[7]

The legal framework should authorise "the use of the specific technology, by the specific authorities, for the specific purpose – general legislation (e.g. granting blanket powers or

[6] Office of the Privacy Commissioner of Canada (2021) 'Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta'. Gatineau: Victoria Street. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

[7] See the ECHR, specifically Article 7 on privacy, and Article 8: protection of personal data. Available at https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

complete discretion to law enforcement authorities) will not be sufficient" (cite PI). However, with respect to FRT or biometric identification, section 43(B) fails to outline the specific uses and use contexts, who will be operating the systems, and the limits of discretion.

43(B) 1. (a) speaks to the use of FRT for "the prevention, investigation, detection or prosecution of one or more of the criminal offences listed in the Schedule," but there is significant variation in the seriousness of the offences listed in the Schedule, even though the Bill was introduced to address the "most serious offences" (Gataveckaite 2023). Included possible offences such as 'riot' and 'violent disorder' could easily impact peaceful protests under the right to freedom of assembly and freedom of expression. This is a prime example of mission creep and raises concerns for unnecessary and disproportionate use of FRT. Furthermore, 43(B) 1. (b) allows for the use of FRT to protect "the security of the state"[8] which could encompass any number of contexts and scenarios. For this reason, again, there needs to be specific, strict rules around any possible uses.

43(B) 2. outlines how Garda personnel might use biometric information to "progress an investigation with respect to "one or more of the offences specified in the schedule or a matter relating to the protection of the security of the State," but this description is far too vague. This permissive legislative language in this draft (amendment) Bill extends police discretion, and lacks accountability as to who, when, how, and why FRT would operate.

43(B)3. and 6. need to be more precise in their definitions and explanations around what is meant by "data that is legally held or legally accessible by AGS", and the code of practice needs to be expressly outlined.

8) **Head 5: New Section 43C – Application for Approval**

43(C) 1. and 2. specify that a member of AGS apply in writing for approval to use biometric identification to those at the rank of chief superintendent and higher. However, it is unclear whether the usage of biometric identification is accessible to any and all guards as a matter of practice. The highly intrusive nature of biometric data, necessitates perhaps limits as to who should be able to access such technologies and whether these personnel should be part of a dedicated unit with technological know-how.

This provision is also contradictory to the AI Act draft legislation as it currently stands, which requires judicial approval or the approval of an independent oversight body for the use of biometric identification.

Recommendations

9) I question the extent to which FRT companies are compliant with international legislation and guidance in terms of how their systems operate. Furthermore, it is unclear that this legislation will ensure compliance with the laws regulating FRT use by police, and also privacy and human rights laws. **The introduction of this draft (amendment) Bill, and the use of FRT specifically should not move forward until all issues (as outlined above and across**

[8] Issues with the lack of definition for 'the security of the State' outlined in this set of Recommendations from the Council of Bars & Law Societies of Europe. Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Guides_recommendations/EN_SVL_20190329_CCBE-Recommendations-on-the-protection-of-fundamental-rights-in-the-context-of-national-security.pdf.

submissions) have been considered. I would urge the Joint Committee and the Department of Justice to consider drafting more precise guidance (as in point 10 to follow) for FRT use by AGS.[9]

10) If the draft (amendment) Bill does progress any further there must be greater **adherence to relevant EU legislation** and **EU case law**, and the definitions, Code of Practice, and operating standards must be clearly outlined to represent the use case transparently. More clarity is needed about data collection, storage, and access in the event of introducing biometric data. Additional safeguards could include a disposal requirement for biometric data that was collected but not needed (i.e. does not serve a lawful investigation or other lawful purpose).

11) Echoing comments from another submission (by Dr. Birhane and Dr. Farries), the Department of Justice should **engage in consultation with experts that have been discussing FRT from all 7 universities in Ireland and 13 NGOs**, seen in the following texts on the topic:

- Open letter in the Irish Times (June 2022)
- Letter to Oireachtas Cabinet members (June 2022)
- Follow up letter to the Minister of Justice (November 2022)
- Op-Ed in the Irish Times (April 2023)
- Expert Briefing Note to Oireachtas Members (May 2023)

Thank you for considering my submission and giving me this opportunity to comment on the draft Bill. I am more than happy to provide further information or assistance as required.

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

[9] See for example, OPC (2022) 'Privacy guidance on facial recognition for police agencies'. Gatineau: Victoria Street. Available at: https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/.

RCNI Submission to the Joint Oireachtas Committee on Justice on

General Scheme of the Garda Siochana (Recording Devices) (Amendment) Bill 2023

17 January 2024

Introduction – Rape Crisis Network Ireland

Rape Crisis Network Ireland (RCNI) is a specialist information and resource centre on rape and all forms of sexual violence. The RCNI role includes the development and coordination of national projects such as using our expertise to influence national policy and social change and supporting and facilitating multi-agency partnerships. We are owned and governed by our member Rape Crisis Centres who provide free advice, counselling and other support services to survivors of sexual violence in Ireland.

The RCNI welcomes the opportunity to make submissions on the General Scheme of the Garda Siochana (Recording Devices) (Amendment) Bill 2023. We have addressed our concerns and comments in order of the Heads laid out in the Scheme and thereafter a more general discussion on the Schedule of Offences.

Head 2: Interpretation

The term 'biometric data' is in the Data Protection Act 2018 and specifically refers, amongst other things, to dactyloscopic data which is fingerprints and palm prints. The wording of the definition in the General Scheme creates a new definition which only includes facial images. This difference creates an inconsistency between the definitions which is problematic. The General Scheme relates only to facial images and should therefore provide clarity on this.

Recommendation:

'"biometric data" has the same meaning attached to it in Section 69 of the Data Protection Act 2018.'

Insertion under Head 3: Biometric identification is limited to facial images.

Head 8: Section 43F

The RCNI has concerns over the processing of data obtained and the potential impact the use of this data could have on the privacy of victims of sexual violence. This is especially concerning where such data would subsequently be used as evidence. We submit that further protections be included to ensure that in any risk assessment on the collection and processing of the data, the needs and vulnerabilities of victims are specifically considered and addressed.

Recommendation:

The inclusion of specific provisions to protect any personal or identifying data collected and processed which may have a negative or traumatic impact on victims or infringe on their right to privacy.

Schedule of Offences and Notable Offences not included in the Schedule (Appendix II)

Our understanding of the purpose of the introduction of this Legislation, is to provide for the more efficient identification of suspects or criminals. The means and tools available to members of An Garda Siochana should be standard and available to them irrespective of the type of offence they are investigating. Generally, the perpetrators of sexual violence are identified without too much difficulty. There are cases, however, where this technology could be used to identify perpetrators and certainly to assist in the collection of evidence against perpetrators. It is our submission that there should be no limitation of the offences applicable, and the Schedule should include all sexual offences. To exclude even one runs the risk of leaving victims without the necessary assurances and protection that all available evidence can and will be collected. Questions of necessity and proportionality are not appropriate for this stage of the collection of data and have more bearing on how the data is used from that point on.

Recommendation:

The provisions of this Schedule should be applied to all sexual offences without reservation or exclusion.

We thank you for the opportunity to make a submission. Please contact us should you require further or clarifying information.

Date: 17 January 2024

Rape Crisis Network Ireland (RCNI)

Carmichael Centre

North Brunswick Street

Dublin D07 RAH8

Email: legal@rcni.ie

Website: www.rcni.ie

GSRDA_09

Digital Rights Ireland

Submission to the Joint Oireachtas Committee on Justice
by the Irish Council for Civil Liberties and Digital Rights Ireland

Draft General Scheme of the Garda Síochána
(Recording Devices) (Amendment) Bill 2023

18 January 2024

1. Introduction:

1.1 The Irish Council for Civil Liberties (ICCL) and Digital Rights Ireland (DRI) thank the Committee for this opportunity to make submissions on the Draft General Scheme of the Bill. Our chief concerns are that this proposed Bill:

i. Is unlawful under EU law (Recital 33 of the Law Enforcement Directive (LED),[1] and the Court of Justice of the European Union (CJEU) decisions in the cases of *DRI v Ireland*[2] and *Ligue des droits humains v Conseil des ministres*[3]);
ii. Fails to meet the EU law requirements for any national legislation governing processing of data under the LED[4] for the purposes of criminal investigation to be "clear, precise and its application foreseeable to those subject to it";
iii. Creates a model of indiscriminate surveillance of people in Ireland;
iv. Unlawful provisions leave the state open to face *Dwyer*-type[5] cases in which evidence is challenged and otherwise strong cases can be undermined;
v. Fails to meet the requirements of Charter of Fundamental Rights, as confirmed by the CJEU;[6]
vi. Is not in compliance with Article 10 of the LED, as does not limit use of facial data to when it is "strictly necessary" as required;[7]
vii. Fails to ensure that any Facial Recognition Technology (FRT) use would be targeted in terms of the individuals to be identified (as proposed under the upcoming EU AI Act);[8]
viii. Fails to ensure that anyone whose biometric data is processed is directly linked to a specific crime, as required under the EU law principles of necessity and proportionality;
ix. Fails to require prior judicial approval of any use of FRT but instead allows for problematic internal Garda approval,[9] similar to the system struck down following *GD v Ireland*;[10]
x. Fails to acknowledge or appreciate the inherent racial and gender biases within FRT, breaching the Article 11.3 LED requirement for the processing of data laws to be non-discriminatory;[11] and
xi. Fails to acknowledge or appreciate the need for thorough public consultation with communities who will be disproportionately impacted by these biases.

1.2 Facial Recognition Technology (FRT) is a very powerful flawed technology that can be compared to fingerprinting but is much more intrusive concerning fundamental human rights. As a biometric technology working based on probability, it attempts to identify a person by comparing a biometric template created from a face detected in an image or video against a reference database of biometric templates. An FRT search generally results in the production of potential candidates accompanied by similarity scores. A threshold value is fixed to determine when the software will indicate that a probable match has occurred. Should this value be fixed too low or too high, respectively, it can create a high false positive rate (i.e. the percentage of incorrect matches identified by the technology) or a high false negative rate (i.e. the percentage of true matches that are not detected by the software). There is no single threshold setting which eliminates all errors.[12] The multiple components of an FRT system, together with the steps involved in the working of such a system, and the multitudinous outside factors which can affect

the performance of that system, makes attempts to identify a person with FRT a probabilistic, and therefore problematic, endeavour.[13] It is not a silver bullet.

1.3 Yet, however defective FRT may be in respect of a given application, it is a technology which can enable powerful mass surveillance by stripping people of their anonymity, reducing people to walking licence plates[14] and tilting the power dynamic inherent in police-civilian interactions further into the hands of police.[15] The implications of police use of this "novel and untested"[16] and "highly intrusive"[17] technology can vary depending on the purpose and scope of its use. But the use of FRT by gardaí, as proposed - to use *any* images or footage that An Garda Síochána legally retains, or can legally access, to locate, identify, track people, at scale, from a distance, without their knowledge, and with significant discretion left to the gardaí regarding such searches - would result in a seismic shift in the surveillance capabilities of Irish policing.[18] There is an important backdrop to this proposal: (i) the Garda Síochána Recording Devices Act 2023 has already vastly expanded the ability of gardaí to record people;[19] and (ii) the State has unlawfully built a national biometric database of 3.2 million cardholders' unique facial features since 2013 and we have been awaiting a Data Protection Commission report on this since 2019.[20]

1.4 There is a stark lack of safeguards and limitations on the use of FRT within the scheme, while there is no specific explanation as to the source of "biometric data which is legally held by An Garda Síochána" against which FRT searches would be run. The scheme essentially provides for gardaí to press "rewind" on a person's movements without any requirement that there is an evidentiary link that the person being sought, identified and tracked has committed, or is even suspected of having committed, a crime. Crucially, it is proposed that such intrusive searches will be subject to internal Garda approval as opposed to judicial approval or approval from an independent authority. This is a form of oversight and control which has been specifically attempted and found unlawful in earlier CJEU case law.[21]

1.5 This indiscriminate surveillance concern is why hinging a decision on whether gardaí should use FRT on a vendor's "accuracy" figure is to misunderstand the complexity of this technology and to fail to consider potentially profound chilling effects will have on Irish society long-term.

1.6 The lifetime of an FRT system, its connection to other surveillance systems, the use, storage and destruction of facial biometric identifiers, and the technical and organisational safeguards in place, or lack thereof, to protect those identifiers when in use - all details which are notably absent from this scheme - have to be fully considered. The committee must also bear in mind that an internal 2022 data protection audit identified the handling of CCTV footage as an area of high risk for An Garda Síochána,[22] while significant legal problems have resulted from the State's approach to mobile phone data retention[23] and CCTV schemes.[24]

1.7 Consideration must also be given to the transparency and oversight mechanisms in respect of each component of FRT and each step of its use; the independence and efficacy, or lack thereof, of those mechanisms; and questions of how to hold manufacturers and users of FRT systems accountable.

1.8 The serious concerns raised above do not belong to legal, technology and human rights experts[25] alone. Due to the inherent risks, jurisdictions in the US have banned law enforcement from using FRT, including cities such as San Francisco,[26] Oakland,[27] and Boston.[28] Several Big Tech companies, such as IBM, Amazon, and Microsoft, have backed away from offering, developing or researching FRT because of the serious fundamental rights risks involved.[29]

1.9 The Office of the High Commissioner for Human Rights has called for a moratorium on FRT use in public spaces until at least key safeguards are in place and stated: "If used at all, such technologies should only be deployed to respond to situations such as serious crime and serious public safety threats, if discriminatory effects can be excluded and subjected to adequate and effective oversight, including independent authorisation and regular independent human rights audits".[30] This scheme fails to fulfil these conditions, and fails to acknowledge the inherent racial and gender biases in FRT.

1.10 The discriminatory effects of FRT are well documented. While error rates will vary depending on the multiple factors which can affect the performance of an FRT system, including but not limited to the quality of images used, the lighting, the pose of the person in the image/video, the creation of the database of images against which an image will be compared, and the selected threshold setting for 'similarity', these errors do not affect all individuals equally. Studies have clearly demonstrated deeply inherent racial and gender biases in FRTs due to how they have been trained,[31] meaning women and people of colour are more likely to be misidentified,[32] and therefore wrongly accused by police who use FRT, than light-skinned men. Computer vision models, the basis for FRT, have demonstrated how Black men and women have the highest rate of being classified as a "criminal" and "suspicious person".[33] Some authorities have applied FRT to marginalised communities already over-surveilled,[34] meaning FRT can be used to deepen structural inequalities.

1.11 Research has shown that the severe lack of transparency in respect of FRT vendor's algorithms, models, and training data means it's extremely difficult for the public to hold vendors, and/or state authorities using the systems,[35] to account for the inevitable failure and discriminatory consequences of their use. This scheme fails to acknowledge these concerns, and/or include any access to remedy for breaches of rights as a consequence of FRT use by gardaí. We note there has been no consultation by the Department of Justice with communities who will be disproportionately affected by FRT.

1.12 The use of FRT by police engages people's fundamental rights to human dignity, the right to privacy the protection of personal data, non-discrimination, the rights of the child and the elderly, the rights of people with disabilities, the freedom of assembly and association, the freedom of expression, the right to good administration, and the right to an effective remedy and to a fair trial.[36] All of these rights are enshrined in international and regional human rights law, including the EU Charter of Fundamental Rights.[37]

1.13 These rights are not absolute. However, under international human rights law, these rights may only be restricted or limited as long as the restriction is provided or prescribed by law and is not arbitrary; pursues a legitimate aim; is strictly necessary in a democratic society to achieve the

aim in question; and is proportionate to the legitimate aim. As it currently stands, the general scheme does not indicate that this Bill will meet these thresholds.

1.14 We say, from a human rights perspective, the *Draft General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill* is neither lawful nor effective as a practice to introduce into Irish policing. To introduce FRT on foot of ill-defined methods and purposes is to invite not only breaches of innocent people's rights but also to see otherwise secure convictions at risk of successful appeals.

2. Head-by-head concerns:

2.1 Without prejudice to these substantive issues, we now address the Bill's heads:

Head 2: Interpretation

2.2 Head 2 suggests redefining the EU legal definition of "biometric data" by excluding "DNA, fingerprints or any other data except for facial images".[38] EU law is superior to national law.

2.3 The proposed definition of "biometric identification"[39] is problematic for two reasons:

i. Technically, there are different types of 'biometric identification' systems which this definition neither reflects nor appreciates. There are 'post' remote biometric identification systems'; 'real-time' remote biometric identification systems'; and 'remote biometric identification systems'. Based on the proposed FRT use cases outlined elsewhere in the Bill, it would appear that the aim of the Bill is to legally provide for An Garda Síochána to carry out 'post remote biometric identification'.[40] If this is the case, the definition for post remote biometric identification would have to mirror that of the forthcoming EU AI Act.[41]

ii. Secondly, what biometric data is legally held by the gardaí?[42] A mere snapshot is not systematically considered to be biometric data, but a photograph taken under specific technical circumstances for the individual identification of a person (which this system relies upon) is, under Article 4 of the GDPR.[43] This scheme does not appear to give gardaí the power to process imagery in its possession, or that which it can access or gather, such that they can create biometric templates and/or a database of such. This must be clarified.

Head 4: Section 43B - Power to use the biometric identification

2.4 In its guidelines on the use of FRT by police, the European Data Protection Board (EDPB) is unequivocal: the processing of biometric data under *all* circumstances constitutes a "serious interference" with people's rights to privacy and protection of personal data, regardless of the outcome of the FRT search, i.e. whether there is a 'positive match' or not. Given this serious interference, any legal basis providing for the processing of biometric data must be sufficiently precise and foreseeable for citizens to understand the specific conditions and circumstances in which use FRT.[44] Merely passing a law to allow for FRT

use, which fails to meet the basic requirements of clarity and accessibility cannot be considered "lawful". This is to protect against arbitrary interferences with rights.

2.5 **Section 43B(1)** and **Section 43B(2)** are imprecise, unforeseeable, and lack clarity because:

- The full list of scheduled offences has not yet been finalised;
- The offences which *are* listed, including robbery and public order offences, and some of those which could potentially be included as per Appendix II, including obstruction of a peace officer, are considerably less serious than the "most serious of crimes" for which this Bill was said to be earmarked for,[45] indicating real concerns around mission creep. Every use of FRT will have an impact on a person(s) fundamental rights but this will be worsened in respect of less serious offences.
- The vague, subjective and broad provision "to locate a person or to follow the movements of a person in order *to progress an investigation*…" gives excessive discretion to gardaí to identify and track the movements of people without limitation; in an untargeted fashion; without safeguards; without regard or due consideration for whether or not such identification or tracking would take place at a protest or place of worship where other special category data could be processed; and without any requirement for objective and verifiable evidence that a person searched, or a person in a database searched against, has any link to the respective offence, or whether they are a witness or onlooker;
- The scheme fails to provide a definition of national security;
- It fails to provide a definition of the very broad purpose "progress an investigation";
- It fails to provide a definition of "utilise biometric identification".
- Neither **Section 43B(1)** nor **Section 43B(2)** stipulate that any respective Garda member using FRT must have undergone any training prior to use.
- Neither **Section 43B(1)** nor **Section 43B(2)** stipulate that any respective Garda member carrying out an FRT search must not have any knowledge as to the background of the respective investigation to mitigate against confirmation bias.

2.6 **Section 43B(3)** is problematic because:

- It lacks precision and foreseeability as it fails to specify the specific sources of the images and video material to be considered "already…gathered", "legally held," or "legally accessed" by An Garda Síochána.

- It's unclear what, if any, separate legal basis there is for gardaí to create biometric templates from the imagery "gathered", "legally held" or "accessed" in order to carry out an FRT search. This is a distinct form of personal data processing, and would need a specific legislative basis.

- There's no limitation on 'who' would be included in a search, other than what imagery the gardai holds or can access. It fails to outline any required criteria in respect of how a garda would select an image to be searched, and/or what reference database a garda would use in a search, and/or how a garda would decide what images to populate a reference database if they were to make their own database to be searched. By way of example, the EDPB has stated that in respect of police carrying out an FRT search pertaining to a riot, the creation of a database of images for that search, based on material sourced from citizens, public transport CCTV, police-owned surveillance material, and material sourced from the media - without first establishing that a person included in the database has displayed severe criminal behaviour and meeting other criteria - may be unlawful.[46]

- There are no technical or organisational safeguards to protect the rights of people whose biometric data would be used in a search.

2.7 **Section 43B(5)** (sic) states that a live FRT search under Section 43B(1) is prohibited. But there is no such prohibition for live FRT search under Section 43B(2). This must be clarified.

- The use of FRT in live and retrospective scenarios *both* represent a major interference with people's fundamental rights. The risk of persistent tracking and its adverse impact on rights and democracy, due to retrospective FRT, are "at least equivalent" with those of live FRT as the amount of imagery potentially available for 'post' remote biometric identification of a person are always more numerous than those available at a single point in time for real-time identification.[47] As such, they can make it possible to draw a much more complete picture of the activities of any individual, thus representing a major interference with a person's fundamental rights.[48] Experts have warned the use of retrospective FRT "marks a step change in police surveillance capability that may fundamentally alter the balance of power between the state and its citizens".[49]

- The section also fails to state how long after material is recorded it could be subjected to an FRT search retrospectively. Without a time lag defined, a live FRT ban does not mean much as the time lag could be any time gap, however short. If the processing is not to be considered 'live', the processing should be such that it could not be used to identify the current location, to an effective level of precision allowing for 'live-like' tracking, of an individual. This would fall foul of the current proposed EU AI Act, which acknowledges that a 'significant delay' is required before a national provision would not fall foul of a ban on 'real-time' surveillance.[50] Under the requirements of the

LED, that 'significant delay' must be defined in legislation to meet the need for clarity, precision and foreseeability.

2.8 **Section 43B(6)** (sic) fails to respect the "strictly necessary" requirement. A Code of Practice providing a presumption that strict necessity and proportionality thresholds have been met, as this scheme does, risks them not being met.

- As per Article 10 of the LED, processing of biometric data "shall be allowed only where *strictly* necessary, subject to appropriate safeguards for the rights and freedoms of the data subject".[51] As the EDPB has stated, "This [strictly necessary] requirement should be interpreted as being indispensable. It restricts the margin of appreciation permitted to the law enforcement authority in the necessity test to an absolute minimum."[52] This means that FRT can only be used as a measure of last resort, when there are no other less intrusive means to achieve the same goal available. This is not provided for in **Section 43B(6)**.

Head 5: 43C - Application for approval

2.9 **Sections 43C(1)** and **(2)** provide for a garda to seek permission to carry out a FRT search, subject to approval from a Chief Superintendent or a higher-ranking member. The sections provide that the request must be made in writing and include the "purpose of the request and the parameters of the search". The section states applications may include "any other detail" which may be specified in an associated Code of Practice. This is deeply problematic:

- Although the AI Act text is pending, it is understood that retrospective FRT searches of persons under investigation will require prior authorisation by a judicial authority or an independent administrative authority.[53] The AI Act will also require notification to the data protection and market surveillance authority.[54] These safeguards are not included.

- It is also deeply troubling that the Bill appears to provide for the requesting garda to carry out the FRT search themselves, as opposed to an independent expert trained in using FRT who has no knowledge of the case background, in order to mitigate against bias.

- Any application to a judge for approval, at the very least, should include:

  i. A documented and justified argument as to why FRT is the chosen option and why alternative options are not chosen;

  ii. A written assessment as to why an FRT search is strictly necessary and proportionate in the specific instance. This assessment should include evidence describing the problem being addressed by the measure; how the measure will be genuinely effective in addressing the problem; a determination as to whether or not the measure is the least intrusive measure to address the problem; and an explanation as to why existing measures cannot address the problem;

  iii. A fundamental rights impact assessment in respect of the specific search;

iv. Details of the source and quality of the probe image and reason for its selection;
v. Details of the sources and quality of the database images and reason for their selection;
vi. Details of the specific purpose of the proposed search;
vii. The legal basis for processing the probe image and reference database images;
viii. The name and rank of the garda making the request.

Head 6: 43D - Approval

2.10 Similarly to Head 5, Head 6 fails to appreciate that the AI Act is expected to stipulate that retrospective FRT searches will require prior authorisation by a judicial authority or an independent administrative authority, as opposed to approval from a Chief Superintendent, and that such uses will require notification to the data protection and market surveillance authority.[55] In addition:

2.11 **Section 43D(1)(b)** also fails to appreciate the "*strictly* necessary" requirement to carry out an FRT search, as opposed to "necessary and proportionate".

2.12 It is not sufficient that conditions of approval may only be left up to the discretion of the Chief Supt. **Section 43D(2)** presents issues regarding transparency, foreseeability and accountability in this regard.

2.13 **Section 43D(3)** fails to include the provision of documented and demonstrative proof of how the application meets the strict necessity and proportionality test.

Head 7: 43E - Use of biometric identification

2.14 **Section 43E(1)** provides that, once approval from a Chief Supt is secured, a Garda can use "any" images or footage that An Garda Síochána legally retains, or can legally access, to carry out an FRT search to "locate, follow the movements or identify a person". This section begs the question as to where An Garda Síochána will have obtained biometric data. No element of the proposed Bill permits the creation of this biometric data by processing images to create biometric templates, which are required to match against any footage to make an identification.

2.15 **Section 43E(2)** provides that "the results from any use of the biometric identification must be verified by a Garda prior to that result being forwarded to the investigation team". A number of issues arise:

- As stated above in respect of Head 4, the vague and problematically broad provision to use FRT in this manner presents an unjustifiable interference with people's fundamental rights as it fails to require any evidentiary link that the person being sought, identified and tracked has committed, or is even suspected of having committed, a crime.

- Just because An Garda Síochána can legally retain, or can legally access, certain images and recorded footage for a specific purpose, does not mean that *everyone* in that imagery can be subjected to an FRT search. As stated above, as per Article 10 of the LED, processing of biometric data "shall be allowed only where *strictly* necessary, subject to

appropriate safeguards for the rights and freedoms of the data subject".[56]

- The 'verification' provision is unclear as the previous sections provide for the requesting garda to carry out the search. This is also the first, and only, mention of an "investigation team". How an FRT search is to be carried out must be explained explicitly.

- If there is a "verification" process, it's unclear from the Bill what this process involves. It is often said by police forces wishing to assuage concerns about FRT that there is nothing to be concerned about because there will be a "human in the loop" safeguarding against any automated decisions. However, it is not always the case that a human, a police officer or an eyewitness, will correct an incorrect FRT match. Michael Oliver, who has a face tattoo, was wrongfully arrested and detained for almost three days in Detroit after an FRT search returned him as the suspect thief and an eyewitness picked him out of a photo line-up, all despite the photo of the suspect displaying no face tattoo.[57]

- Head 7 fails to include any requirements to ensure an even basic level of responsible use of FRT. For example, if an FRT search is authorised to a police investigation team in The Netherlands, a step-by-step process is undertaken involving a facial examiner who would have no background knowledge of the case to avoid bias and a blind peer review.[58]

Head 8: 43F - power to process data obtained under this part

2.16 This heading presumes the pre-existence of the biometric templates, but does not confer a legislative power to create them.

Head 16: Amending section 49

2.17 This head provides that a designated High Court judge would review the operation of Bill and provide an annual report to the Taoiseach. Experience tells us this is a weak safeguard due to the lack of detail in the reports and the oversight role being bestowed on a busy judge with no staff, specialist training or technical advisor.[59]

2.18 In addition, it has been confirmed by the CJEU that this form of 'after the fact' review does not meet the requirements of judicial oversight of the operation of data processing amounting to mass surveillance.[60]

3. Conclusion:

3.1 As stated at paragraph 1.15, we urge the Government to reconsider introducing FRT to Irish policing and warn that to do so on foot of ill-defined methods and purposes is to invite not only breaches of innocent people's rights but also to see otherwise secure convictions at risk of successful appeals.

[1]Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (LED), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680 Recital 33: "... a Member State law, legal basis or legislative measure should be clear and precise and its application foreseeable for those subject to it, as required by the case-law of the Court of Justice and the European Court of Human Rights. Member State law regulating the processing of personal data within the scope of this Directive should specify at least the objectives, the personal data to be processed, the purposes of the processing and procedures for preserving the integrity and confidentiality of personal data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."

[2] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others*, C-293/12, 8 April 2014: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

[3] *Ligue des droits humains v Conseil des ministres*, C-817/19, 21 June 2022: https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=13059170

[4] LED, Recital 33, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680

[5] *G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, Case C-140/20, 5 April, 2022: https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3210127

[6] See Paras 116 and 117, *Ligue des droits humains* C-817/19, 21st June 2022: https://curia.europa.eu/juris/document/document.jsf?text=&docid=261282&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=13059170

[7] LED, Article 10 provides that processing of biometric data may be allowed "only where strictly necessary", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680

[8] Breyer, P., AI Act threatens to make facial surveillance commonplace in Europe, see leaked Article 29(6a) of EU AI Act, 16 January 2023, https://www.patrick-breyer.de/en/ai-act-threatens-to-make-facial-surveillance-commonplace-in-europe/ and the leaked text: https://patrick-breyer.de/wp-content/uploads/2024/01/LEAK-Document-Artificial-Intelligence-Act.pdf

[9] Coffey, G., An Examination of Proactive Intelligence-Led Policing through the Lens of Covert Surveillance in Serious Crime Investigation in Ireland, Athens Journal of Law - Volume 10, Issue 1, January 2024 – Pages 63-86, https://www.athensjournals.gr/law/2024-10-1-4-Coffey.pdf#page=19&zoom=100,0,938

[10] *G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, Case C-140/20, 5 April, 2022, paras. 106-114, https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3210127

[11] Article 11(3) LED: "Profiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10 shall be prohibited, in accordance with Union law", https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[12] Buolamwini J., Ordóñez V., Morgenstern J., and Learned-Miller E., Facial Recognition Technologies: A Primer, May 29, 2020, https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf

[13] Buolamwini J., Ordóñez V., Morgenstern J., and Learned-Miller E., Facial Recognition Technologies: A Primer, May 29, 2020, https://assets.website-files.com/5e027ca188c99e3515b404b7/5ed1002058516c11edc66a14_FRTsPrimerMay2020.pdf

[14] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted 26 April, 2023, p.15, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

[15] Mozur, P., One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, New York Times, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html; Shahwan, N., From 'blue wolf' to 'red wolf': An automated Israeli occupation, Daily Sabah,

May 15, 2023, https://www.dailysabah.com/opinion/op-ed/from-blue-wolf-to-red-wolf-an-automated-israeli-occupation

[16] Gullo K., Electronic Frontier Foundation, Victory! New Jersey Court Rules Police Must Give Defendant the Facial Recognition Algorithms Used to Identify Him, June 7, 2023, https://www.eff.org/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition

[17] *Glukhin v Russia*, App no 11519/20, (European Court of Human Rights, 10 April 20203, https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-225655%22]}

[18] As stated by the UN Office of the High Commissioner for Human Rights (OHCHR), "[R]emote biometric recognition dramatically increases the ability of State authorities to systematically identity and track individuals in public spaces, undermining the ability of people to go about their lives unobserved and resulting in a direct negative effect on the exercise of the rights to freedom of expression, of peaceful assembly and of association, as well as freedom of movement." See United Nations, Artificial Intelligence Risks to Privacy Demand Urgent Action – Bachelet, 15 September 2021: https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-actionbachelet?LangID=E&NewsID=27469

[19] ICCL and DRI, Secret tracking of people's vehicles using ANPR must be subject to judicial approval in the Recording Devices bill, 5 July, 2023, https://www.iccl.ie/news/secret-tracking-of-peoples-vehicles-using-anpr-must-be-subject-to-judicial-approval-in-the-recording-devices-bill/

[20] ICCL and DRI, Assessment of PSC facial recognition software reveals Department of Social Protection has known its biometric processing arising from the PSC is illegal, 9 June, 2023, https://www.iccl.ie/press-release/psc-facial-recognition-software-dpia/

[21] See footnote 10

[22] Foxe, K., Garda data protection officer warns of insufficient resources to carry out role as well as absence of training for staff, TheStory.ie, 11 October 2022, https://www.thestory.ie/2022/10/11/garda-data-protection-officer-warns-of-insufficient-resources-to-carry-out-role-as-well-as-absence-of-training-for-staff/

[23] ICCL and DRI, Briefing on the Communications (Retention of Data) (Amendment) Bill 2022 July 5, 2022, https://www.iccl.ie/wp-content/uploads/2022/07/Briefing-on-the-Communications-Retention-of-Data-Amendment-Bill-2022.pdf

[24] Data Protection Commission 2018-2020, Regulatory Activity under GDPR, see Appendix 1, p. 63-72, https://www.dataprotection.ie/sites/default/files/uploads/2020-06/DPC%20Ireland%202018-2020%20Regulatory%20Activity%20Under.pdf

[25] Policing Facial Recognition Technologies Expert briefing note 10 May, 2023, https://digitalpolicy.ie/wp-content/uploads/2023/05/Policing-FRT.-10-May-2023-Oireachtas-brief.pdf

[26] Conger K., Fausset R., and Kovaleski S., *San Francisco Bans Facial Recognition Technology*, New York Times, 14 May 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html

[27] Ravani S., Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns, San Francisco Chronicle, 16 July 2019, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php

[28] Jarmanning A., Boston Lawmakers Vote to Ban Use of Facial Recognition Technology by the City, npr, 24 June 2020, https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/24/883107627/boston-lawmakers-vote-toban-use-of-facial-recognition-technology-by-the-city

[29] Heilweil, R., Big tech companies back away from selling facial recognition to police. That's progress, Vox, 11 June 2020, https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police See also Bird S., Responsible AI Investments and Safeguards for Facial Recognition, Microsoft, 21 June 2022, https://azure.microsoft.com/en-us/blog/responsible-ai-investments-and-safeguards-for-facial-recognition/ and Amazon, We Are Implementing a One-Year Moratorium on Police Use of Rekognition, 10 June 2020, https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-ofrekognition

[30] A/HRC/51/17, https://daccess-ods.un.org/tmp/1756789.53528404.html

[31] Buolamwini J., and Gebru T., Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018,

http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. See also Deborah Raji I., and Buolamwini J., Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial ai products, Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society, https://dl.acm.org/doi/10.1145/3306618.3314244. See also Cook C., Howard J., Sirotin Y., Tipton J., and Vemury A., Demographic effects in facial recognition and their dependence on image acquisition: An evaluation of eleven commercial systems. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2019 https://ieeexplore.ieee.org/document/8636231. See also NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, December 19, 2019. NIST wrote: "How accurately do face recognition software tools identify people of varied sex, age and racial background? According to a new study by the National Institute of Standards and Technology (NIST), the answer depends on the algorithm at the heart of the system, the application that uses it and the data it's fed — but the majority of face recognition algorithms exhibit demographic differentials. A differential means that an algorithm's ability to match two images of the same person varies from one demographic group to another." https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

[32] Press, E., Does A.I. Lead Police to Ignore Contradictory Evidence?: Too often, a facial-recognition search represents virtually the entirety of a police investigation, The New Yorker, 13 November, 2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence

[33] Birhane, A., Prabhu, V., Han, S., & Boddeti, V. N. (2023). On hate scaling laws for data-swamps. Ithaca: Cornell University Library, arXiv.org. https://doi.org/10.48550/arxiv.2306.13141

[34] Amnesty International, Israel/OPT: Israeli authorities are using facial recognition technology to entrench apartheid, 2 May 2023, https://www.amnesty.org/en/latest/news/2023/05/israel-opt-israeli-authorities-are-using-facial-recognition-technology-to-entrench-apartheid/

[35] Kalluri P., Agnew W., Cheng M., Owens K., Soldaini L., Birhane A., The Surveillance AI Pipeline, https://arxiv.org/abs/2309.15084?ref=404media.co

[36] Opinion by Michael O'Flaherty, Director, European Union Agency for Fundamental Rights (FRA), Facial Recognition Technology and Fundamental Rights, 2020, https://edpl.lexxion.eu/data/article/15801/pdf/edpl_2020_02-005.pdf

[37] Charter of Fundamental Rights of the European Union (2000/C 364/01), Official Journal of the European Communities, https://www.europarl.europa.eu/charter/pdf/text_en.pdf

[38] Article 3(23) of the Law Enforcement Directive provides, 'biometric data' means 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 data, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680

[39] The scheme states, "'biometric identification' means identifying or attempting to identify natural persons, through the comparison of a person's biometric data with the biometric data which is legally held by An Garda Síochána".

[40] MEPs ready to negotiate first-ever rules for safe and transparent AI, European Parliament, 14 June, 2023, https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai

[41] European Commission, Artificial Intelligence – Questions and Answers*, 12 December, 2023, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683

[42] On November 29, 2023, Garda Commissioner Drew Harris told the Joint Oireachtas Committee on Justice, Defence and Equality in respect of FRT: "We have no database of pictures…" see https://www.kildarestreet.com/committees/?id=2023-11-29a.1194&s=database+of+images#g1330

[43] Article 4(14) of the GDPR states, "'biometric data' means 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 data'; Recital 51 of the GDPR states, "The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person." https://eur-lex.europa.eu/eli/reg/2016/679/oj

[44] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, Adopted on 26 April 2023, p.5, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

[45] Gataveckaite, G., Justice Minister Helen McEntee to face down Greens over facial recognition technology as she returns from maternity leave, Irish Independent, 1 June, 2023, https://www.independent.ie/irish-news/politics/justice-minister-helen-mcentee-to-face-down-greens-over-facial-recognition-technology-as-she-returns-from-maternity-leave/a845781306.html

[46] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Adopted 26 April, 2023, p.43-45, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

[47] European Parliamentary Research Service, Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence, December 2021, p. 55, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/697191/EPRS_STU(2021)697191_EN.pdf

[48] Ibid

[49] Murray, D., Police Use of Retrospective Facial RecognitionTechnology: A Step Change in Surveillance CapabilityNecessitating an Evolution of the Human Rights Law Framework, The Modern Law Review, DOI: 10.1111/1468-2230.12862, https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-2230.12862

[50] See Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

[51] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, Article 10, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680

[52] European Data Protection Board, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, Adopted on 26 April 2023, par. 73, https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf

[53] European Commission, Artificial Intelligence – Questions and Answers*, 12 December 2023, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_168

[54] Ibid

[55] Ibid

[56] LED, Article 10, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680

[57] Vice, Faulty Facial Recognition Led to His Arrest—Now He's Suing, September 2020, https://www.vice.com/en/article/bv8k8a/faulty-facial-recognition-led-to-his-arrestnow-hes-suing

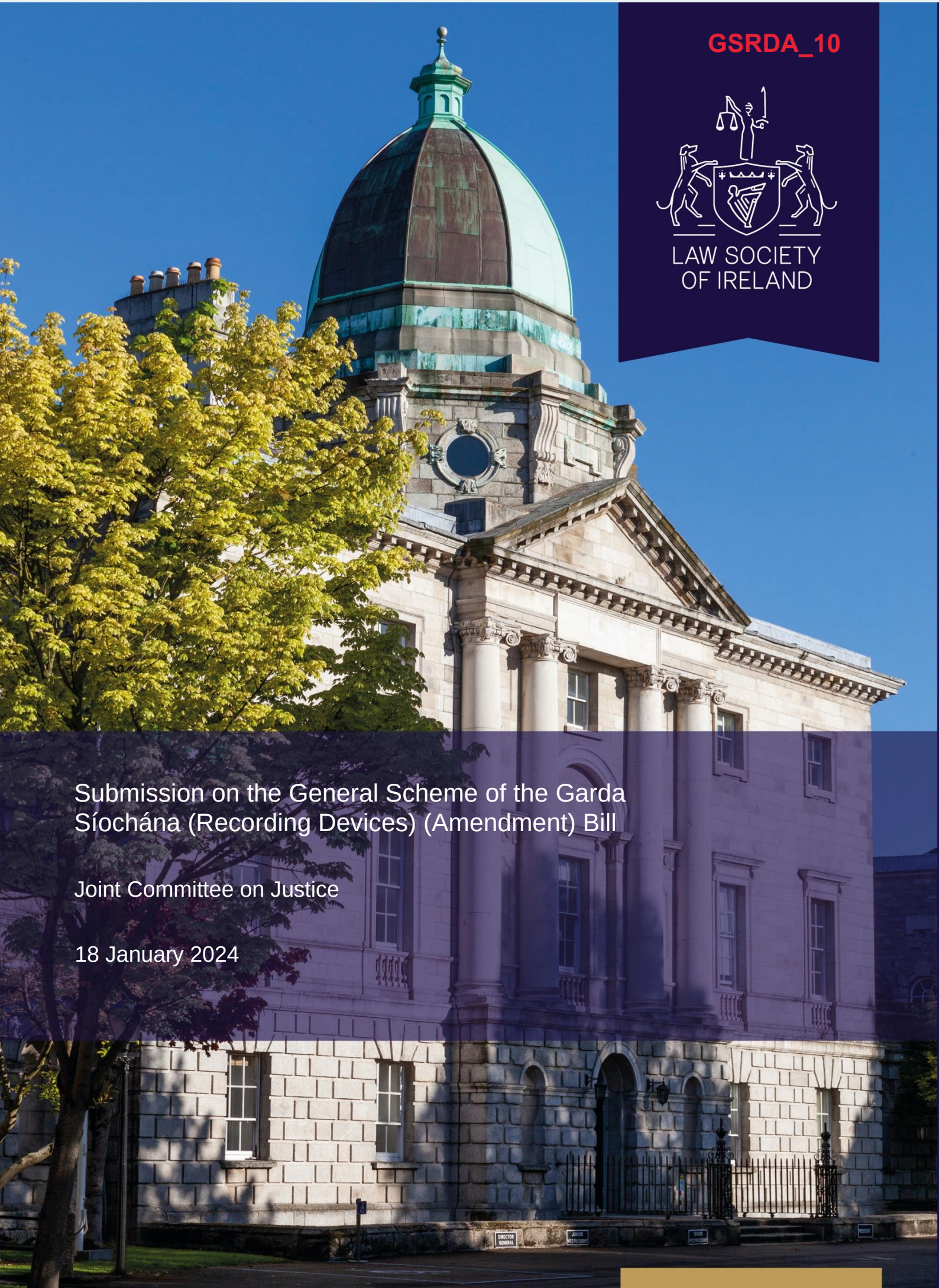
[58] This process involves facial examiners taking the following steps: First manually assess the quality of the probe image; After running a search, they would manually analyse the list of candidates proposed by the FRT system; If the facial examiner confirms the conclusion of a "possible match", the probe image and the image of the potential candidate from the reference database are handed to two facial experts for blind peer reviews; During the blind peer review, the facial experts, independently of each other, perform a full analysis of the probe and the reference image to determine the similarity/dissimilarity of the two faces. The end result to be reported to the investigation team is the final conclusion reached by consensus or, in the event of a lack of consensus, the most conservative conclusion in terms of similarities observed; If the facial examiners reach a conclusion of "no recognition", the probe image is handed to another expert to run the entire search afresh. If the fresh search results in a "possible match", a blind peer review by two other facial experts will additionally be carried out as described above. Following the communication of the final result, the investigation team will proceed to review the results of the search, seeking to corroborate or disregard the proposed candidates. See A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations Insight Report Revised, November 2022, p. 13 https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf

[59] McIntyre, TJ, 'Judicial Oversight of Surveillance: The Case of Ireland in Comparative Perspective,' in Judges as Guardians of Constitutionalism and Human Rights, ed. Martin Scheinin, Helle Krunke, and Marina Aksenova (Cheltenham: Edward Elgar, 2016), accessible here: http://hdl.handle.net/10197/7363

[60] *G.D. v Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, Case C-140/20, 5 April, 2022, para. 112, https://curia.europa.eu/juris/document/document.jsf?text=&docid=257242&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3210127

GSRDA_10

LAW SOCIETY OF IRELAND



Submission on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill

Joint Committee on Justice

18 January 2024

Submission on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill

Introduction

The Law Society of Ireland (the '**Law Society**') appreciates the opportunity to respond to a request from the Joint Committee on Justice on the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023 (the '**General Scheme'**).

Given the limited time available to consult on the General Scheme, any failure to comment on a particular head/note does not indicate a particular position on that head/note. We hope that publication of the General Scheme will be followed by publication of a draft Bill which will be subject to full legislative scrutiny, in which event we may contribute additional technical points at a that stage.

Executive Summary

The Law Society notes possible weaknesses in the General Scheme which give rise to a concern that this legislation will be challenged on several grounds including through the lens of privacy rights, data protection, the right to non-discrimination and the right to a fair trial. The Law Society submits that the tests of necessity and proportionality required for the introduction of biometric identification in the Irish context merits further examination. In this submission, we look at the General Scheme on a Head-by-Head basis and outline our observations in a general manner. The legislation could provide more safeguards and oversight relating to when biometric identification can be used by An Garda Síochána, the recording of the use of this technology, the external monitoring of its use and reviews of the applicable Code of Practice.

Part One – Preliminary and General

Head 2 – Amendment to Section 2 of Principal Act - Interpretation

The definition of **'**biometric identification' means identifying or attempting to identify, natural persons, through the comparison of a person's biometric data with the biometric data which is legally held by An Garda Síochána'.

It is noted that the definition of biometric data is to have the meaning as set out in section 69 of the Data Protection Act 2018, with the exclusion of DNA fingerprints and other data "except for facial images".

Section 69 (1) of the Data Protection Act 2018 defines biometric data;

"Biometric Data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual that allow or confirm the unique identification of the individual, including facial images or dactyloscopic data".

It is noted that section 69 of the Data Protection Act 2018 includes 'physiological or other behavioural characteristics'. If it is the intention that this Bill will only apply to facial images and not other physical characteristics of individuals such as their height, it would be preferable that this is set out more explicitly in the legislation. The definition does not specify what is meant by 'technical processing'. Does this include the creation of facial images by a camera phone or indeed the processing of physical photographs?

The definition of "biometric identification" is as follows:

"identifying or attempting to identify, natural persons to the comparison of a person's biometric data with the biometric data which is legally held by An Garda Síochána"

The definition of biometric identification, given the lack of clarity in the definition of biometric data, arguably does not exclude the comparison by An Garda Síochána without the assistance of intelligent automation, of two photographs.

PART 2 – The insertion of new Part 6A into the Principal Act

Head 3 – New Section 43A – Application of this Part

Section 43A (2)(i)

This subsection provides,

"nothing in this Part shall prevent An Garda Síochána from processing and storing images which have been legally provided by other national or international organisations".

The draft does not specify what national or international organisations it refers to. Is it other law enforcement organisations only? Or is it envisaged that An Garda Síochána could lawfully obtain images from the Department of Social Protection for example, to obtain biometric data for the purposes of identification. The draft could be more explicit as to which type of organisation it refers to.

Also, the draft should place an onus on An Garda Síochána to only use images which have been legally obtained by those organisations. The Department of Social Protection has been implicated in the past for illegally processing biometric data (https://www.iccl.ie/press-release/psc-facial-recognition-software-dpia/). If that data is subsequently transferred to An Garda Síochána then the whole chain could be tainted.

Section 43A (3) provides that the use of biometric identification must be in compliance with a Code of Practice as set out in section 47. Section 47 of the Principal Act provides for consultation in relation to codes of practice and periodic reviews of the codes of practice. It is submitted that the use of intelligent automation to assist with the identification of suspects in the context of the investigation of offences requires more transparency and oversight. It is submitted that this should be explicit in primary legislation.

Political agreement was reached at EU level on 8 December 2023 in relation to the Artificial Intelligence Act (**AI Act**). The AI Act classifies what it calls 'Post Remote Biometric Identification Systems' as being high risk processing and requires that such systems by law are equipped with appropriate logging capabilities and that any final decisions impacting persons are made by human eyes.

The principles of this General Scheme should align with the principles agreed at political level on the AI Act, including stating specifically that the final decision around identification should be made by a person.

Searches conducted using biometric identification technology need to be fully documented at every stage of the identification process and logged accordingly. The technology must log the searches made, results returned, and a record of the images maintained for final review. The search and result logs could be available for review by way of disclosure by the defense in the event of prosecution. This could be expressly provided for in the primary legislation.

The General Scheme is silent on the oversight of the use of biometric identification systems. There is a requirement that An Garda Síochána keep a record of all applications but it is not clear whether such records will be reviewed by an independent authority to ensure that the use of biometric data is used in a proportionate manner. The high-risk nature of the processing would require that the use of such technology is the subject of oversight to assure the public

of the compliance by An Garda Síochána with both the legal requirements and the Code of Practice proposed under the General Scheme.

Head 6 – New Section 43D - Approval

Section 43 (D) (1) provides that the Chief Superintendent may approve an application if the following circumstances are met:

a) he or she is independent of the investigation to which the application relates,

b) he or she believes on reasonable grounds that the use of biometric identification is necessary and proportionate, and

c) he or she believes on reasonable grounds that the use of biometric identification is connected to an investigation of an offence in the schedule or a matter relating to the protection of the security of the State.

The provision does not set out how or against what criteria, the Chief Superintendent is to assess whether the use of biometric identification is both necessary and proportionate. It is assumed that such technology will only be required for complex investigations involving significant searches of CCTV footage or other digital data and where there are circumstances of urgency such as a threat to the public security, concern for a person's safety or the protection of life. The objectives of the bill could be set out in clearer detail so that the test as to what is necessary and proportionate can be better assessed and reviewed. It would be preferable if the General Scheme set out more clearly the underlying policy intention. It is submitted that judicial oversight might be more appropriate here namely an Application to a District Court Judge.

Head 7 – New Section 43E – Use of the Biometric Identification

Subsection (1) provides that a Garda

"…may utilise biometric identification to search the following in order to locate, follow the movements or identify a person:

(a) any images or footage that An Garda Síochána legally retains;

(b) any images or footage that An Garda Síochána can legally access."

On one reading of (b) above it infers that an authorisation by a Chief Superintendent would cover biometric identification using images not yet in the custody of An Garda Síochána, but that are legally accessible to them. This appears to contradict an earlier provision, Section 43(B)(3).

That section provides,

"Biometric identification referred to in subsection (1) will only utilise images and video that has already been gathered and are legally held or legally accessed by An Garda Síochána."

This subsection confirms that An Garda Síochána must have already gathered the images and videos. Section 43E(1) could be reworded to make it clear that it refers to videos and images already gathered. It could read, a member "may utilise biometric identification to search the following in order to locate, follow the movements or identify a person, any images or footage already gathered and legally retained or legally accessible by An Garda Síochána."

In addition, it is not clear how images and footage could be gathered by An Garda Síochána but not 'retained' by them. Is the term "legally accessible" required?

PART 3 – The insertion of consequential amendments into the Principal Act

Head 12 - Amending section 47

Retention, erasure, destruction

It is envisaged that retention, erasure and destruction of biometric data and the results of biometric identification is dealt with in a Code of Practice. Given the sensitivity of biometric data and purported fallibility of facial recognition, why would the legislation governing its use leave the destruction provisions to a Code of Practice? In contrast, the Criminal Justice (Forensic Evidence and DNA Database System) Act 2014 includes provisions in relation to the retention and destruction of forensic samples. The facial recognition legislation could do the same so that individuals know how long their data is retained.

Scheduled of Offences

The AI Act, as it currently stands, requires in the context of 'live' biometric identification systems (which is excluded under this General Scheme) that this technology can only be used for specified offences. It is not clear from the information available on the political agreement reached on 8 December 2023 whether that limitation applies equally to 'post review' biometric identification systems captured by this General Scheme.

As set out previously, the objectives against which an application for the use of biometric identification technology is to be assessed could be more clearly articulated. It is submitted that the use of the technology, to be necessary and proportionate, must be used for the more serious offences, where the requirements of efficiency and urgency are most acute. This will depend on the type of the investigation as opposed to the nature of the offence. It will likely apply to many cybercrimes, cyber enabled offences, offence presenting a threat to public safety and investigations seeking to preserve life.

The scheduled offences currently do not include any terrorist related offences such as offences contrary to the Explosive Substances Act 1883, Firearms Act 1925 - 1964 or offences relating to organized crime set out in part 6 of the Criminal Justice Act 2006. The scheduled offences do not include the offence of sexual assault, albeit aggravated sexual assault and rape offences are included.

It is submitted that the requirements of the AI Act be reviewed to assess whether individual offences must be scheduled for post review biometric identification.

Conclusion

The Law Society submits that more attention to precise drafting be given in the Bill to the recording, storing and accessing biometric data and using this data for biometric identification for the investigation or detection of offences.

We have outlined some specific points on the draft wording in this submission but generally the Law Society would like to see a number of strengthened safeguards in the use of these technologies by An Garda Síochána.

The Law society submits that an application made by An Garda Síochána to use biometric identification should be made to a District Court Judge rather than the Chief Superintendent.

We note that this legislation is being developed at the same time as the Data Protection Commission (the **DPC**) investigates surveillance of people for law enforcement purposes by

An Garda Síochána and the DPC has identified significant data protection compliance issues (Data Protection Commission, Annual Report 2020).

The Law Society acknowledges that there is inevitably a tension between vindicating individual rights to privacy and protection of personal data and permitting law enforcement authorities to use and access technology to address the commission of serious crime however the State must balance the different rights at play to ensure justice is done and seen to be done.

We appreciate the opportunity to contribute these comments and observations to the Committee's consideration of the General Scheme. We remain available to further assist the Committee in any way we can.

For further information please contact

Niamh Coyne
n.coyne@lawsociety.ie

Blackhall Place, Dublin 7
t. 01 672 4800
e. general@lawsociety.ie

Briefing for the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill

18 January, 2024

Dr Abeba Birhane
Dr Elizabeth Farries

We recognise that this Draft General Scheme reflects the Department of Justice's purported and ongoing plans to enable An Garda Síochána's use of Facial Recognition Technology systems (collectively Policing FRT).[1] We will therefore refer to Policing FRT for the purpose of this submission.

In reference to the author - Dr Birhane's - research, research from the Centre for Technology and Democracy (Radiya-Dixit & Nuff 2023), and leading recent publications, we submit evidence outlining Policing FRT's disproportionate impact on vulnerabilised communities, the importance of identifying less intrusive methods through democratic consultation, and minimum safeguard thresholds that must be established *prior* to the deployment of policing FRT.

1. Disproportionate impacts on vulnerabilised communities

A person's facial biometric data is sensitive and personal. Processing this data for policing purposes is highly intrusive in that it represents a serious interference with rights including privacy, data protection, expression, assembly, and equality and non-discrimination.[2] Policing FRT disproportionately limits the rights of us all, but particularly those with racial and gender vulnerabilisations, through misidentification, dehumanisation, and over surveillance.[3]

a. Invasive and ineffective

Although often presented as a cost and resource effective aid to policing, FRT has proven to be the least effective and most intrusive technology. In a recent survey by Big Brother Watch reviewing police use of FRT across Wales where over 508,542 faces were scanned, over 3,000 people were wrongfully identified, over 88% inaccuracy recorded in the period of 2016-2023, and only 3 arrests made.[4] FRT, therefore, is extremely invasive and a technology that expands and normalises surveillance state while also largely failing to aid effective policing.

---

[1] See a Minister's statement that the Department of Justice seeks to legalise Policing FRT by amending Garda Síochána (Recording Devices) Bill (now the Garda Síochána (Recording Devices) Act 2023) https://www.irishtimes.com/crime-law/2023/04/06/oireachtas-committee-wants-to-scrutinise-use-of-facial-recognition-technology-by-gardai/

[2] Farries, E. and Cronin, 0. (4 June 2022) Submission to inform the report by the United Nations High Commissioner for Human Rights on the right to privacy in the digital age at its 51th session in 2022, Human Rights Council adopted resolution 48/4 https://files.inclo.net/content/pdf/72/FINAL_%20Right%20to%20privacy%20in%20the%20digital%20age,%20HRC%2048_4%20(1).pdf

[3] Ibid.

[4] Big Brother Watch (n.d.) Stop Facial Recognition https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/

b. Misidentification

There is a current, peer reviewed, and established body of evidence that women, men and people who have darker skin are more likely to be misidentified by FRT.[5] Numerous, rigorous, evidence based studies speak to these findings, not least the author's - Dr Birhane's - own 2023 publication demonstrating how black men and black women have the highest rate of being classified as 'criminals' and 'suspicious person' by computer vision models, the basis for FRT.[6] The larger the data set the higher the misclassification rate. Misclassification is proven to occur at the expense of darker skinned people.

c. Dehumanisation

The author's findings follow the findings of a 2021, Radford et al Open AI audit demonstrating how image classification models tend to mislabel and misclassify images of people that have darker skin colours.[7] This study that evaluated computer vision models using the Fairface dataset, showed that darker skinned men and women are classified as non-human animals, including chimpanzees, gorillas, and orangutans, and suspicious person, criminal and thief at a higher rate compared to other less vulnerable races and genders. The reduction through technology of people to non-human animals and suspicious characters is dehumanising.

d. Over surveillance of us all and vulnerabilised communities especially

Error prone FRT systems create over surveillance as a problematic norm: anyone's facial image captured by this technology is subject to rights implicating surveillance. However, given the historic and discriminatory over surveillance of vulnerabilised communities by law enforcement, including those with darker skin,[8] a particular consequence and risk attached policing FRT is detainment or incarceration without cause of people from vulnerabilised communities. In the US alone, six known cases of law enforcement have been documented, all falsely incarcerating people on the basis of

---

[5] See for example Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 81, 1-15. http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; NIST. (2019, December 19). NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software; UK's Metropolitan Police FRT found to have an error rate of 81 per cent, see 81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says, Sky News, July 2019, https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941 ; MIT and Stanford University tested three different commercial FRT systems; less than 1% eros for light skinned men, 20% of the cases related to faces of dark-skinned women, see Study finds gender and skin-type bias in commercial artificial-intelligence systems, MIT News, February 2018, https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212

[6] Birhane, A., Prabhu, V., Han, S., & Boddeti, V. N. (2023). On hate scaling laws for data-swamps. Ithaca: Cornell University Library, arXiv.org. https://doi.org/10.48550/arxiv.2306.13141

[7] Radford, A., Kim, J. W., Hallacy, C., Ramesh, A., Goh, G., Agarwal, S., Sastry, G., Askell, A., Mishkin, P., Clark, J., Krueger, G., & Sutskever, I. (2021). Learning transferable visual models from natural language supervision. Ithaca: Cornell University Library, arXiv.org. https://doi.org/10.48550/arxiv.2103.00020

[8] See for example "Sus Laws" (stop and search laws) that were critiqued for their discriminatory application amongst black and Irish people in the 1970s. See McCluskey, S. (2016). The crime of being suspicious: British counter-terrorism legislation and the history of discriminatory preventative laws in the United Kingdom. Rutgers Race & the Law Review, 17(1), 131-165.

their incorrect FRT classifications.[9] Every single person was black. It is important to note that these are only reported cases. Many people don't have the resources to know that they were jailed because of a policing FRT error or the means to contest it. Or if they know, they don't have the means to contest or communicate this to wider society or policy makers.

We therefore submit that this invasive and ineffective trend of misidentification, dehumanisation, and over surveillance attached to policing FRT presents the risk of undue interference into our rights that is experienced disproportionately according to race and gender.

2. Identifying less intrusive measures through adequate consultation

In addition to disproportionate rights limits of oversurveilled communities, we submit that the Department of Justice should find less intrusive measures, given the disproportionate negative impact and ineffectiveness of FRT. We highlight here the importance of proactive and direct consultation, prior to the legislative stage, with community representatives, policing and technology experts, and civil society organisations. This would include per (Radiya-Dixit & Nuff 2023):

- Via direct consultation, proactively considering views of the public, especially marginalised communities, on the particular type of Policing FRT and justified a disregard of the views if relevant;
- Conducting transparent, proactive consultations with civil society and independent experts on the particular type of Policing FRT;
- Establishing that it has considered the advice from consultations and transparently explained the outcomes, including providing a justification if the advice is not followed;
- Outlining clear, proactive processes for the public, especially marginalised communities, to influence if and how Policing FRT is implemented;
- Outlining clear, proactive processes for the public, especially vulnerabilised communities, to contest and challenge decisions from FRT, given the ample evidence showing failures of FRT; and
- Approaching the consultation process with materials accessible to people with disabilities and provided in immigrant languages.[10]

We see no evidence that the Department of Justice has engaged proactive consultation or established that policing FRT is less intrusive in comparison to other measures. Indeed we note the government has not adequately engaged with the proactive outreach from a consortium of experts from all **7 universities in Ireland and 13 NGO**s, including experts penning our:

- Open letter in the Irish Times (June 2022)
- Letter to Oireachtas Cabinet members (June 2022)
- Follow up letter to the Minister of Justice (November 2022)
- Op-Ed in the Irish Times (April 2023)
- Expert Briefing Note to Oireachtas Members (May 2023)

[9] Swarns, Christina. (19 Sept 2023) When Artificial Intelligence Gets It Wrong. Unregulated and untested AI technologies have put innocent people at risk of being wrongly convicted. The Innocence Project. https://innocenceproject.org/when-artificial-intelligence-gets-it-wrong/

[10] Radiya-Dixit, E., & Neff, G. (2023). A sociotechnical audit: Assessing police use of facial recognition. Paper presented at FAccT '23. 1334-1346. https://doi.org/10.1145/3593013.3594084

3. Pre-establish minimum thresholds to safeguard Policing FRT deployment

Given 1 and 2, the Department of Justice should pre-establish minimum thresholds before deploying Policing FRT systems. Supporting Radiya-Dixit & Nuff (2023), we submit that the Department should:

a. Carry out proactive expert, community and public consultations, according to criteria itemised in point 2 to determine the least intrusive measures for policing.
b. Established through independent (i.e. a designated conflict-free expert auditor) auditing obligate minimum operational thresholds of selected Policing FRT systems. These thresholds include but are not limited to precision, false positive rate, true positive rate, etc.
c. Establish safeguards precluding the use of Policing FRT with an unsuitable low-quality probe or image.
d. Carry out and publish a data protection impact assessment and appropriate policy document for sensitive data processing
e. Create clear, objective, and limited criteria concerning third-party access to the data collected or retained, including with regard to what data can be shared, with whom it can be shared, and for what specific purpose it can be shared.
f. Establish and deploy accessible communication protocols across ability and languages to inform potential data subjects and most people impacted jurisdiction in advance about when, where, why, and how Policing FRT will be (or is currently being)
g. Establish clear measures to ensure data subjects can exercise their individual rights including the rights to rectification, erasure, and object with clear justifications if exemptions apply Deploy accessible communication protocols as above to be used and how data subjects can exercise their individual rights.[11]

If these criteria are not met and, particularly, if Policing FRT Systems are proprietary and/or independent auditors cannot access the training data sets or models to audit them, then the Policing FRT systems should not be used. We invite the Department of Justice to identify less intrusive measures through the democratic consultation process and to include these measures in any forthcoming legislation.

—--

Abeba Birhane is a cognitive scientist, currently a Senior Advisor in AI Accountability at Mozilla Foundation and an Adjunct Assistant Professor at the School of Computer Science and Statistics at Trinity College Dublin, Ireland. She researches human behaviour, social systems, and responsible and ethical AI – work for which she was recently featured in Wired UK and TIME on the TIME100 Most Influential People in AI list. Birhane also serves on the United Nations Secretary-General's AI Advisory Body and the newly-convened AI Advisory Council in Ireland.

Dr Elizabeth Farries is the Director of the UCD Centre for Digital Policy and a Senior Fellow with the International Network of Civil Liberties Organizations.

[11] *Ibid.*

Houses of the Oireachtas
Leinster House
Kildare Street
Dublin 2
D02 XR20

www.oireachtas.ie
Tel: +353 (0)1 6183000 or 076 1001700
Twitter: @OireachtasNews

Connect with us

Download our App

Download on the App Store

GET IT ON Google Play