IRISH COUNCIL FOR CIVIL LIBERTIES AND DIGITAL RIGHTS IRELAND

Submission to the Joint Oireachtas Committee on Justice

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.

1.2. 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] 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

1.3. 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.

1.4. 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]

1.5. 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

---

[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/

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]

1.6. 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 the potentially profound chilling effects its use will have on Irish society long-term.

1.7. 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]

1.8. 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.

1.9. 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]

1.10. 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

---

[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

these conditions, and fails to acknowledge the inherent racial and gender biases in FRT.

1.11. 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.

1.12. 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.

1.13. 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]

1.14. 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

---

[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

not indicate that this Bill will meet these thresholds.

1.15. 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:

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

2.1. Head 2: Interpretation

- 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.

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

  - 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.

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

- 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

---

[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

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.

- **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.
- **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

[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

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.

- **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

[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

'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.

- **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)**.

2.3. Head 5: 43C - Application for approval

- **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:
    - A documented and justified argument as to why FRT is the chosen option and why alternative options are not chosen;
    - 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;
    - A fundamental rights impact assessment in respect of the specific search;

---

[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

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

2.4. Head 6: 43D - Approval

- 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:
  - **Section 43D(1)(b)** also fails to appreciate the "*strictly* necessary" requirement to carry out an FRT search, as opposed to "necessary and proportionate".
  - 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.
  - **Section 43D(3)** fails to include the provision of documented and demonstrative proof of how the application meets the strict necessity and proportionality test.

2.5. Head 7: 43E - Use of biometric identification

- **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.

- **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]

[55] Ibid
[56] LED, Article 10, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680

- 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]

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

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

2.7 Head 16: Amending section 49

- 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]

- 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.

---

[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