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.