laws

MDPI

Article

Facial Recognition Technology in Policing and Security—Case Studies in Regulation

Nessa Lynch [1,2]

[1] School of Law, University College Cork, T12 K8AF Cork, Ireland; nessa.lynch@ucc.ie
[2] Faculty of Law, Victoria University of Wellington, Wellington 6011, New Zealand

Abstract: Technology-enabled state surveillance has evolved rapidly to allow real-time remote tracking and surveillance of people and vehicles and the aggregation of vast amounts of data on people and their movements, networks, and relationships. Facial recognition technology (FRT) comprises a suite of technologies that allows verification, identification, and categorisation by analysing a person's facial image. Such technologies impact fundamental rights, such as privacy, freedom of expression, and freedom of assembly, but can also be used to detect, investigate, and deter serious crime and harm and to counter threats to security, thus promoting collective interests in security and public safety. These impacts have been considered in terms of scholarship and advocacy, but the shape of principled regulation is less well traversed. This contribution examines three contemporary case studies of the regulation of FRT in policing and security to analyse the challenges in regulating this technology.

Keywords: biometrics; emerging technology; policing; artificial intelligence

Citation: Lynch, Nessa. 2024. Facial Recognition Technology in Policing and Security—Case Studies in Regulation. *Laws* 13: 35. https://doi.org/10.3390/laws13030035

Academic Editors: Colin Gavaghan, Jeanne Snelling and Debra Wilson

Received: 19 April 2024
Revised: 23 May 2024
Accepted: 2 June 2024
Published: 7 June 2024

1. Introduction

This Special Issue focuses on the regulation of emerging technologies. Technology-enabled state surveillance encompasses biometric surveillance technologies such as facial recognition technology, large-scale data analytics in the online space, and other forms of tracking technology such as automatic number plate recognition technology (ANPR). These technologies have evolved rapidly to allow real-time remote tracking and surveillance of people and vehicles and the aggregation of vast amounts of data on people and their movements, networks, and relationships. State surveillance can occur in the physical public space (such as ANPR tracking in the town centre or motorway) and the online public space (such as the analysis of publicly posted social media content to monitor potentially harmful speech). Such technologies impact on fundamental rights, such as privacy, freedom of expression, and freedom of assembly, but can also be used to detect, investigate, and deter serious crime and harm and to counter threats to security, thus promoting collective interests in security and public safety.

My contribution to this Special Issue is centred on facial recognition technology (FRT), an emerging but increasingly established technology that allows the identification of individuals through an analysis of that person's facial image against an already collected image or database of images (Akbari 2024). The usage of this technology by the police and security services globally has been largely innovation-led and technology supplier-led, rather than implementation through legislative authorisation or deliberative policy choices. While FRT underpins everyday-use cases such as building access, unlocking smartphones, and automated border control, its use in policing and state security generally is more controversial. This is because the technology may be used to track and/or surveill individuals in real time or retrospectively, giving the state considerable power, which may infringe collective and individual rights, particularly privacy and freedom of expression. Societal concerns about impacts on people are growing, and this has led to rapid developments in

regulation, both in terms of specific responses and in the context of larger-scale regulation of artificial intelligence (AI).

I use the collective terms policing and security to encompass policing, border, intelligence, and security agencies, but also where more general agencies (e.g., immigration) exercise policing and security powers such as physical and digital surveillance. In this contribution, I will first discuss common-use cases for FRT in policing and security using global examples. I discuss the risks and opportunities associated with the use of FRT in policing, including case law analysis. I then discuss three diverse global case studies for the regulation of FRT and how such regulation has sought to protect individual and collective human rights, but also to weigh societal interests in preventing, detecting, and prosecuting crime and reducing risks to public safety.

I conclude by assessing the potential impact of these types of regulatory response and looking towards the future of regulation of FRT.

2. Facial Recognition Technology

2.1. Defining FRT

Facial recognition technology (FRT) is in use in a range of applications in the general and the policing, and security contexts. In broad summary, FRT is a technology that involves the analysis of a computer-generated template derived from a person's facial image and the comparison by means of computer analysis with images already collected (Akbari 2024). Its primary uses are verification, identification, and categorisation (Lynch and Chen 2021, EU AI Act 2024: Recital at (14)).

2.2. Facial Images as a Biometric

A facial image is a type of biometric akin to fingerprints, iris scans, voiceprints, and DNA. This means that it is a unique identifier that distinguishes one individual from another. It contains sensitive information unique to the individual. Biometric data are defined in European Union (EU) law as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". (Art. 4 (14) of Regulation (EU) 2016/679 (the General Data Protection Regulation)). Many jurisdictions now classify biometric information as highly sensitive data (Jasserand 2016). Biometric information is considered particularly sensitive because of its ability to identify the person but also to reveal aspects of a person, such as their ethnic origins or familial connections. As discussed, FRT systems operate on computer-derived templates of the person's face. This type of data may contain less sensitive information than the actual facial image. This is analogous to forensic DNA, where the profile generated from the sample (e.g., the blood or skin cells) contains much less information (Bright et al. 2020; Williams and Johnson 2005). Nonetheless, this does not diminish the potential for impact on individual and collective privacy rights.

Facial images may be distinguished from some other biometrics, e.g., DNA, fingerprints, or iris scans, in that facial images can be collected at a far distance and frequently without a person's consent or even their knowledge. Some have sought to distinguish "intrusive" forms of biometric data collection—those that involve intrusions to bodily integrity, such as the collection of DNA directly from the individual's person—from "non-intrusive" forms of biometric data collection—such as the collection of facial images from a distance. A decision of the High Court of England and Wales concerning a judicial review of police use of live-automated FRT drew this distinction and categorised live-automated FRT as "non-intrusive", ruling that only the collection of personal data gained through an intrusion on that person's place of residence or their individual bodily integrity could be classified as "intrusive" and consequently require statutory authorisation (*R. (Bridges) v Chief Constable of South Wales Police* 2019). The recital to the incoming EU AI Act (2024, at (15)) states that biometric identification should be defined broadly as "automated recognition of physical, physiological and behavioural human feature such as the face, eye movement, body shape,

voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes, characteristics, for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not". This suggests less of a distinction between intrusive and non-intrusive biometric identification and a recognition of the high sensitivity of all types of biometric data, including facial images.

It may well be contended that by going into a public space, a person is making their face available for viewing by others. Further, CCTV networks are in common use in both public and commercial spaces, as well as urban and rural environments, in modern society. However, this does not automatically include implied or explicit consent to collection, storage, and/or analysis of the facial image by the state. As I discuss in more detail below, though a single viewing of a person's face by another in the normal course of interactions in a public space may not be intrusive, collection, retention, and analysis by a state-controlled technology will always be, given the short- and longer-term impacts of the data analysis and the potential gravity of outcomes.

2.3. Common-Use Cases for FRT

Common-use cases for FRT range from very intrusive and high-risk use cases such as live-automated FRT and emotion recognition technology to comparatively benign and generally socially acceptable-use cases such as verification of identity in online passport applications, automated passport control at the airport, and "tagging" on social media applications. This spectrum of use and impact is important in the design and parameters of regulation, so as not to rule out legitimate and proportionate uses of the technology. Some calls for banning or significant restriction might impact legitimate and comparatively low-risk usages.

In general terms, there are three categories of FRT usage that are most relevant to the policing and security contexts:

2.3.1. The Verification of a Person's Identity

Verification involves the comparison of a biometric template derived from the person's facial image with one that has already been stored in a system. This is a "one to one" comparison. A common example of this would be automatic passport control at the border, where the static camera captures an image of the person's face and scans their passport. The system then compares the two images to ensure that the person who is presenting the identity document matches the facial image stored in the credential. Another common example is the FaceID function on iPhones, which is a biometric identification method that compares the facial image of the person who logs in with an already stored image, negating the need for alphanumeric passwords. There is also a growing category of use cases related to fraud detection and prevention in banking (Gautam 2023).

This category of use case is generally considered to have a minimal impact on people, as the sole purpose of the technology's operation is to confirm that the individual is the person that she or he claims to be for the purpose of gaining access to a system or premises or unlocking a device for use (EU AI Act 2024: Recital at (17)). However, there are risks relating to fraud, especially in the increasing use of 'deep fakes' to impersonate people (Jain et al. 2021).

2.3.2. The Identification of a Person

This involves a comparison of a person's individual biometric template to an existing database of facial images to find a matching identity. This could be a "one to many" comparison, but it also could be a "many to many" comparison in a surveillance scenario where multiple facial images are found in the input image (Lynch and Chen 2021). Identification by means of FRT can be in real time ('live') or retrospective ('post').

Common examples of this type of use case in policing and security include live-automated FRT, where a camera system scans passing individuals and compares their facial

images against an already stored watchlist of people of interest (Fussey and Murray 2019). This is also known as a form of remote biometric identification. This technology is considered highly intrusive, as it involves the collection of sensitive data remotely and potentially without that person's knowledge (Lynch and Chen 2021). It allows for real-time identification and tracking of individuals and groups, thus significantly impacting privacy rights and having a 'chilling effect' on individuals and society. This type of use case is highly controversial, and it has been the subject of several challenges on human rights grounds (which are discussed in more detail below). Critics have also pointed to the potential for discriminatory outcomes due to concerns about decreased accuracy rates for people from some ethnic groups (Lohr 2022; Limantė 2023).

Using similar processes, a facial image collected from an unidentified person could be compared with a database of identified facial images to establish that person's identity. This use case may be employed for unidentified people coming into police custody who refuse to give their biographical information or are unable to provide this information accurately due to youth, injury, or incapacitation.

2.4. Categorisation and Emotion Recognition

In more experimental and less-established use cases, FRT can be used to extract demographic information from a person's facial image. This could include factors such as age, gender, or ethnicity. Concerns have also been expressed around how datasets could infer gender identity or sexuality (Hall and Clapton 2021). Emotion recognition is a type of technology that purports to detect emotion by scanning individual faces (Canal et al. 2022). This is also known as facial emotion recognition. This type of technology has a range of potential use cases and is particularly attractive to industries such as customer behaviour and marketing (Ribeiro et al. 2017). In policing and security contexts, potential use cases centre around the ability to detect emotions in crowds in an ability to predict risk or potential criminality (Podoletz 2023; Fontes and Perrone 2021).

3. The Impact of FRT on Individuals and Society—Implications for Regulatory Design

3.1. Overview

The impact of FRT on people and society will vary depending on the use case and context and is dependent on such factors as whether the person gives informed consent, the implications of the decision or outcome resulting from the use case, and matters such as storage and subsequent use. Patently, state use of FRT has more potential impact than private sector use due to the gravity of decisions and outcomes resulting from state decisions and the power imbalance between the individual citizen or group of citizens and the state.

FRT has the potential impact a range of collective and individual human rights and fundamental freedoms, particularly the right to a private life, the right to be free from discrimination, and the right to freedom of expression in the context of lawful protests. There is considerable scholarly and advocacy literature on these potential impacts on individual rights, particularly in the context of the right to peaceful and lawful protest (see Purshouse and Campbell 2019, 2022).

In parallel with suspect and defendants' rights, a human rights-compliant approach also places duties on the state to investigate and resolve serious crimes and harms and provide resolution for victims. This aspect has received less treatment in the literature or advocacy materials. The use of emergent technologies such as FRT may be a proportionate response in some instances where community or individual safety is at risk (Lynch and Chen 2021). How regulatory regimes attempt to draw the parameters of these sometimes-competing interests is drawn out further in the case studies below.

3.2. Social Licence

Before considering human rights frameworks, it would be beneficial to consider the concept of social licence and its application to FRT. Social licence is a concept originally

derived from environmental law and regulation (Hall et al. 2015) and concerns measuring the acceptability of a proposal or issue to the public. This concept is now in wider use, including in justifying surveillance technologies (Paik et al. 2022). The argument goes that a large section of the public uses these and adjacent technologies in regular daily life, and thus there is a common acceptance. Of course, use by state agencies can be distinguished from individual decisions to use technologies due to the impact and span of control.

The public is likely to expect that the police consider the available technology, particularly where these technologies are in common use in the public sphere. This is particularly relevant in the investigation of child abuse imagery, where FRT is in common use by law enforcement agencies globally. Studies have demonstrated public support for FRT use in relation to serious offences (Bradford et al. 2020), but there may be questions about the representation of minority groups in these studies. Public concern coalesces around the potential of abuse of power and concerns about accuracy of the technology (Bragias et al. 2021). Public trust in policing and attitudes about the legitimacy of police use of technologies highly influence public acceptance or mistrust of FRT (Bradford et al. 2020). The socio-political culture and values of various jurisdictions also have a high impact. For instance, Kostka et al. (2023) found significant differences in public opinion in a four-jurisdiction study, with Chinese citizens being more comfortable with FRT and approving of its perceived benefits, while German citizens were more concerned with their rights to data privacy and were interested in robust regulation to mitigate perceived risks of FRT.

Patently, even within a single jurisdiction, different groups may perceive different levels of risk. People from overpoliced and disproportionality-impacted sections of the community will perceive the technology differently (Stevens and Keyes 2021).

3.3. The Impact on Human Rights

Moving now to the human rights impact, the pace of technological development and the rate of adoption of FRT by law enforcement and state agencies has rapidly outstripped law and regulation, leading to societal concern that human rights impacts have not been significantly mapped or appropriately considered in decisions to initiate use or deploy FRT. Legal theory and regulation around the limits of state surveillance globally, but particularly in common-law jurisdictions, are rooted in concepts that do not take into account the speed, scale, or impact of contemporary technology-based surveillance. For example, powers of the state to photograph or gather intelligence on suspects in the public space are still contextualised by printed photographs and written notetaking and do not comprehend developments such as the power of automated FRT to identify people in real time. These are significant challenges for the appropriate regulation of FRT.

3.3.1. The Right to Privacy

The right to privacy (often referred to as the right to private and family life) is traditionally described as the right to be left alone, but may also be conceptualised as the ability to protect oneself from unwanted access by others, secrecy, control over personal information, protection of personhood, and control over information relating to intimate relationships (Solove 2010). It includes spatial privacy and informational privacy (Cohen 2008). Globally, the right to privacy is derived from international human rights frameworks and national privacy protections. Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights state that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, or correspondence, nor to unlawful attacks on his or her honour and reputation. Privacy in the age of rapid technological and digitalisation is an increasing focus at the international level. The United Nations Human Rights Council (2019) adopted a resolution on the right to privacy in the digital age in 2019, highlighting the risks of emerging technologies such as AI on the right to privacy.

The right to privacy can be both collective and individual. A person has individual privacy rights in relation to their own information, but large-scale technological surveillance,

such as in large deployments of FRT, can transcend individual privacy rights into impact on societal values (Mantelero 2016). An example would be where FRT is used to analyse the emotions of crowds or identify patterns of group behaviour.

The right to privacy in public spaces in an era of technology-enabled surveillance is an evolving issue in privacy law that is highly relevant for considering the impact of FRT. Traditionally, there is a lesser expectation of privacy in a public space compared to one's private residence, though there are situations where there may be reasonable expectations of privacy in a public space (Moreham 2006). While this conceptualisation was more suited to analogue 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. While domestic and international judicial decisions (e.g., the recent ECHR decision in Glukhin v. Russia 2023) have touched on this issue, this is another challenge for designing regulatory regimes. The European Court of Human Rights in *Glukhin* found that there is a "a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'". (para. 64).

In the recital of the incoming EU AI Act (at [19]), there is a significant discussion of the definitions of public space, including spaces only accessible by ticket or registration, and foreshadowing spaces, which are a mixture of public and private (giving the example of an airport), but specifically excludes prisons and border control. Interestingly, online spaces are not covered by the regulation, despite the societal trend towards living public and private life in the online world.

3.3.2. The Right to Be Free from Discrimination

Human rights impacts relating to discrimination in the design and operation of FRT are centred around two principal concerns. The first is around the disproportionate impact of technology use against particular groups, which mirrors the disproportionality of other operational aspects of policing. For example, this may be reflected in decisions around which neighbourhoods or event FRT cameras are deployed (Fussey et al. 2021). It is also reflected in where the comparison image dataset is drawn from, particularly whether these are from existing databases of convicted or suspect people. It is important to understand that existing (even 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 impacts must be carefully monitored to avoid perpetrating bias (Lynch et al. 2020; Lynch and Chen 2021).

The second is the accuracy of the technology itself. An earlier analysis of the use of FRT in a policing context identified the potential for bias due to low levels of accuracy. Reports have highlighted reduced accuracy levels on people with darker skin tones and instances of misidentification triggering automated enforcement action (Johnson et al. 2022). This is a major concern for FRT and undermines public trust and confidence (Garvie and Frankle 2016). More recent studies appear to suggest that accuracy rates are improving rapidly as the technology evolves, but this is an aspect that must be monitored closely, and the findings of technology suppliers must be interrogated closely (Wu et al. 2023). Accuracy rates can also be significantly diminished by the context, e.g., low or variable lighting, and whether the person is wearing a mask or headgear.

Contextually, it is important to remember that visual/eyewitness identification evidence by the human eye is notoriously unreliable (e.g., Kovera and Aronson 2023; Shapiro and Penrod 1986), and FRT systems consistently perform better than humans on identification tasks (Phillips et al. 2018). The human eye and mind are also subjected to the biases of that person and of society in general. Nevertheless, human operators are likely to be swayed by perceptions that technology-enabled matches are more accurate and reliable than human assessment. This is why appropriate controls must be set in place (such as multiple reviews, trained operators, and quality assurance processes) before any enforcement or investigative action should be taken based on a match. This is necessary to ensure public trust and confidence that a police or security service is using the technology in a

lawful and justified manner. Without an appropriate level of assurance, the potential for biased or discriminatory outcomes due to misidentification is increased.

3.3.3. The Right to Freedom of Expression

International human rights law provides for the right to freedom of expression. Relatedly, this involves the right to protest (Fenwick 1999). It is in the context of this right that the few judicial decisions involving human rights challenges to FRT have occurred, as these situations offer an example of courts considering the legitimacy of FRT deployment for security and public safety reasons when balanced against individual claims of freedom of expression.

In the R (Bridges) v Chief Constable of South Wales Police (2019, 2020), a person took an action against South Wales Police. He became aware that his facial image had been scanned by South Wales Police during their deployment of live-automated FRT around the event and at another time in a retail premises. His argument was that there was no legal basis for the use of the technology, and if there was, the impact on the right to freedom of expression was not justified. On appeal from a High Court decision, the Court of Appeal found that the policy settings governing South Wales Police's use of the technology afforded too high a range of discretion in where and how to use the technology. This had an effect on privacy, and by implication, the Court found that this could infringe on freedom of expression and deter people from exercising their right to protest.

A more recent decision in the European Court of Human Rights (Glukhin v. Russia 2023) involved a Russian citizen who had engaged in a peaceful solo anti-government protest on the Moscow metro system. He was identified, arrested, and prosecuted apparently by authorities using a combination of automated live FRT and retrospective FRT analysis. One of his arguments was that his right to freedom of expression had been impacted by the deployment of FRT, particularly since there was no apparent threat to public order of safety (at p. 16). The Court agreed, finding that the highly intrusive use of the FRT systems was a disproportionate response to his protest, particularly as it did not involve a risk to public safety. There was no "pressing social need" (at para. 89). The court stopped short of classifying FRT as unacceptable but was clear on the high level of intrusiveness of the technology.

Considering societal impact, commentators have highlighted that technology-enabled surveillance like FRT can have a 'chilling effect' on society as well as individuals (Murphy 2018), particularly in authoritarian regimes. Legitimate protestors may be deterred by the increased possibility of identification and enforcement action by the state or possible consequences for reputation and employment. While police and security agencies have always monitored protests, there is a significant difference between a single or small group of enforcement officers monitoring protest activity in person and the use of a wide-ranging live biometric identification system with the potential for longer-term storage and analysis of biometric data.

3.3.4. Special Protection for Particular Groups

All people have human rights, but the human rights framework has particular protections for certain groups, such as children. Children are an under-recognised group in the analysis of biometric surveillance, despite being significant users of public spaces (Lynch et al. 2024). Further, 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 the collection and retention of children's facial images by law enforcement, except for exceptional circumstances where public safety is at risk (Lynch et al. 2024).

4. Regulating FRT in Policing and Security—Three Contemporary Case Studies

Having set out the potential impacts of FRT on individual and collective interests, I will now move on to examine three contemporary case studies of the regulation of FRT in policing and security, exploring how three forms of regulation have considered and addressed the conceptual challenges discussed above.

4.1. Stages of Regulation of Emergent Technologies

The first stage of regulation was highly aspirational and principle-based in nature (Scherer 2015). Globally, a range of public sector organisations, private sector entities, and non-governmental organisations had a responsible AI, technology charter, or set of principles (de Laat 2021). Examples of these were the New Zealand Government's Algorithm Charter (New Zealand Government 2020), which established principles such as transparency and stressed the importance of a 'human in the loop'. Most technology suppliers also adopted statements of principle, as well as international organisations (de Laat 2021).

There is no doubt that statements of principle are important and useful and have underpinned some progress. The issue is such statements of principle are not in any way enforceable. A person who could be affected by FRT lacks any means of complaint or redress or a firm set of rules to assess appropriateness against. This has been illustrated in several court challenges. In the last few years, but particularly coming to fruition in the past 12 months, legislation and a more robust regulation of AI (including technologies such as FRT) have been successfully agreed upon or implemented.

In this section, I will discuss three contemporary case studies of state attempts to regulate FRT specifically or more generally through reforming AI. These will demonstrate diverse methods of reacting to societal and professional concerns about the risks and challenges of regulating this technology.

4.2. Self-Regulation

The first case study will be referred to as "self-regulation" or self-governance, whereby police and security services' use of FRT is initiated and governed internally, albeit with some input and oversight from independent reviews and state-level regulators. Such practices are now coming under pressure due to societal concerns about legitimacy and oversight. Lynch and Campbell (2024) explored how New Zealand and Australian states are in a regulatory gap, where there is no specific legislative prohibition or empowerment of police use of FRT, though police organisations across the region use this technology. Similar situations exist in the jurisdictions of the United Kingdom. Decisions to adopt the use of FRT and how and when it is deployed depend almost entirely on internal guidance and guidelines, albeit within the more general legal framework applicable to that jurisdiction (for instance, search and surveillance legislation or privacy and data protection legislation and regulation).

The deficiencies in this type of regulatory response lie principally in a lack of legitimacy. The conversations and decisions around when to initiate the use of a technology is predicated on a relationship between the supplier of the technology and the police or security agency. The parameters of the use of the system and the input images and the decisions around where and why to deploy the system are made internally by the police. In some cases, these may hinge upon robust and good-quality guidelines, but in many cases, these are not publicly available. Partnerships with technology suppliers and third-party camera networks may be opaque. The public is largely excluded from the conversation about whether the technology is required or justified. This lack of public input may negate the principle of policing by consent (Neyroud and Disley 2008). Views and input from minority groups and overpoliced communities may not be properly considered. It would be open for police services to make decisions about parameters and the deployment of usage without recourse to legislative authority or public consultation.

Both societal and regulator concerns have grown around the potential for impacts on people and society where FRT is adopted and used without the transparency and legitimacy of legislative or regulatory foundations and oversight. Although there are no specific legislative initiatives in the region, some agencies have made decisions to commit not to use more intrusive forms of the technology. An independent report in New Zealand was commissioned to make recommendations about current state and the potential use of FRT (Lynch and Chen 2021). As a result, Police agreed to pause any consideration of live-automated FRT and to tighten up their rules around other use cases. These decisions and guidelines are patently welcome developments, but overall, a self-regulatory approach based on commitments is not a sufficient safeguard as organisational and leadership attitudes can engender change without public consultation.

4.3. European Union Law

As discussed in the introduction to this section, there have been recent global moves to transition from principle-based guidance to enforceable regulation. As an example, I will focus on the European Union (EU), and mostly, the EU AI Act. This Act is the first concrete global example of a legislative and regulatory regime for artificial intelligence, with biometric surveillance systems such as FRT being a high-profile issue. The AI Act was approved by the EU's Council in late-May 2024 and will be implemented gradually over a two-year period. This analysis builds on an earlier discussion of the regulation of FRT by the EU (Lynch 2022; Lynch et al. 2024), which commented on earlier versions of the text. What is clear is that what the EU does in this context will have a wide and extra-territorial effect. Another comparable EU regulation—the General Data Protection Regulation (GDPR)—is now a world standard in data protection. The EU is a large and valuable world market, and thus technology suppliers will tend to orientate their product standards and governance towards this market. The regulation is likely to set or influence global norms in relation to AI and biometric surveillance.

4.3.1. Risk-Based Framework

Broadly, the AI Act regulates AI through a graduated risk-based framework with several levels. Some uses of AI are considered unacceptable and completely prohibited (Article 5(1)). This includes the use of AI for social scoring, which risks detrimental treatment, live biometric tracking in publicly accessible places (with some carve-outs for law enforcement, discussed below), emotion recognition systems in the workplace or in educational contexts, biometric categorisation to infer sensitive data, and some categories of predictive policing of individuals and groups where it profiles people or infers their characteristics.

The second category is high-risk systems. These systems can be used but will need strict assessment and monitoring. This category includes the use of AI systems in recruitment and work-related relationships ([57]), assessment in education ([56]) biometric identification surveillance systems ([54]), safety components of systems covered by harmonised legislation (e.g., medical devices and automotives), access to essential private and public services (e.g., creditworthiness, benefits, health, and life insurance), and the safety of critical infrastructure (e.g., energy and transport) ([55]).

Medium- to lower-risk systems encompass the remaining use cases, including biometric verification systems.

4.3.2. Application to FRT

Before the AI Act, European Union law, policy, and guidelines were already orientated towards significant restriction on FRT use in policing and security contexts. The AI Act will clarify the position in some respects but also leave significant discretion around the deployment of FRT in these contexts.

The AI Act has recognised the spectrum of use in relation to FRT, which was discussed above, and set out that verification through FRT is not considered prohibited or high risk

"...AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises (EU AI Act 2024, Recital at (15))".

Moving on to the more contentious issue of live biometric identification (which includes live FRT), previous European Union guidance was very cautious around the use of this technology. For instance, the Guidelines 05/2022 *on the use of facial recognition technology in the area of law enforcement of 26 April 2023*, by the European Data Protection Board set out the Board's view that (at p. 107), "remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into individuals' private lives and does not have a place in a democratic society, as by its nature, it entails mass surveillance". At para. 73, it was said that the processing of the data was only strictly necessary if the interference with personal data rights was limited to that which was absolutely necessary, and all alternatives (e.g., additional staffing or more frequent policing) must be considered (at para. 51) before a decision to use FRT. The Board also highlighted the chilling effect of mass surveillance.

Previous iterations of the AI Act text would have taken a more restrictive approach to the deployment of FRT. A coalition of 120 advocacy groups across the European Union advocated strongly for a complete and comprehensive ban on FRT, particularly live-automated FRT (Civil Society Organisations (120 Authors) 2021). In mid-2023, it appeared as if policing and security use of live-automated FRT would be banned entirely in publicly accessible spaces, with retrospective FRT analysis only permitted with significant restrictions. This was welcomed by a range of human rights groups across the EU (e.g., Irish Council for Civil Liberties 2023).

The final text has stepped back from this more restrictive position. Live remote biometric identification (which includes FRT) will be permitted for policing and security purposes but only under strict and narrowly defined conditions, which include prior authorisation and requirements to notify and record usage. The use must be "strictly necessary to achieve a substantial public interest, the importance of which outweighs the risks" (Recital, at para 33). The permitted conditions are set out as follows: the search for certain victims of crime, including missing persons; situations such as threats to the life or to the physical safety of natural persons or of a terrorist attack; and the localisation or identification of a perpetrator, in relation to suspects accused of offences punishable by more than four years detention, which includes a range of listed high-harm offences such as terrorism and sexual exploitation of children (EU AI Act 2024: Annex II).

The AI Act is also careful to distinguish live biometric identification from retrospective systems in order to discourage subversion of the rules. It states (at para. 17 of the recital) that 'Real-time' systems involve the use of 'live' or 'near-live' material, such as video footage, generated by a camera or another device with similar functionality. In the case of 'post' systems, in contrast, the biometric data have already been captured, and the comparison and identification occur. This includes data gathered in "limited short delays" (article 3 [42]). Further, the final text of the AI Act also allows police and security agencies to use biometric identification in the context of border security and asylum, particularly where a person refuses to be identified or is unable to identify themselves (recital, at para. 33). In relation to the parameters of reference image databases, AI systems that "create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage" are prohibited due to the potential for "gross violations" of privacy (recital at (42)).

While having a clearer regulatory regime for the use of FRT in policing and security in European Union law is a positive development in terms of legitimacy and the rule of law, there is still considerable uncertainty around how the exceptions will be implemented, which raises concerns for rights such as privacy and freedom of expression. The parameters, particularly around the broader spread of available offence types, will allow significant

room for the use of these technologies, which has been criticised by advocacy groups. Of course, it is still up to member states as to whether they decide to begin using or continue to use these technologies. An obvious risk is that technologies such as FRT will be seen as more acceptable or even as "approved" due to the wording of the AI Act. As discussed earlier in this contribution, social licences for these types of technologies will differ significantly both between member states of the European Union and within those jurisdictions, for example, by overpoliced communities and ethnic minorities, who may see additional risks in deployment. A result of the regulation may that a more harmonious approach to the *acceptability* of the technology as well as the *restrictions* on the technology will be in place. This may not allow significant inputs from diverse communities and consideration of local sensitivities and culture.

A final challenge for the policing and security contexts is that defence, military, and national security usages of AI are entirely excluded from the regulation (EU AI Act 2024, Recital at (24)). Military and defence are excluded as part of wider EU approaches to these areas, and technology use in this area is regulated by public international law. National security is in the purview of the member state, and this is the reason for the exclusion. The significant implementation challenge here is that the line between national security and law enforcement is blurred in many contexts, particularly around terrorism, cybercrime, financial crimes, money laundering, and cross-border-organised crime. While the EU AI Act states clearly that where military and defence technology is used for law enforcement or other purposes, either temporarily or permanently, it will be covered, this may be very difficult to monitor in practice. For instance, law enforcement in the Act also means "safeguarding and preventing threats to public security" (article 3 [46]). Distinguishing this from national security surveillance systems may be very difficult in practice.

4.4. Specific Legislative Authorisation

The third and final case study that I will discuss is a recent proposal in Ireland to enact specific legislation to empower the national police service (An Garda Síochána) to use some forms of FRT for law enforcement purposes. Though a final decision on the progress of the legislation and its final form is not known at the time of writing, the design and pre-legislative scrutiny stages provide valuable insight into jurisdictional legislative design around this technology. This instance may also prove some of the analysis just set out in relation to how national jurisdictions will respond to the incoming EU regulation. For instance, during the pre-legislative scrutiny process and in the documentation, the responsible department cited compliance with the incoming EU AI Act as a significant safeguard, and in sub-text, it may be seen to justify such proposals to the public as being internationally acceptable.

While some jurisdictions, particularly in the United States, have moved to use legislation to ban or restrict FRT use in the policing context, Ireland's proposals seek to *empower* police to use retrospective FRT in certain circumstances. This proposal was announced in December 2023 by the Minister of Justice Helen McEntee (Department of Justice 2023). Although proposals to use FRT in the context of body-worn cameras had been in play for some time, an apparent catalyst was a serious incident of public disorder in Dublin city centre (Department of Justice 2023). The proposals in the draft legislation are centred around retrospective use in relation to specified serious criminal offences. A detailed analysis of the proposals is outside the scope of this contribution, but the extensive submissions by academics (including the author) and advocacy groups around human rights impacts, legality, and proportionality are collated and analysed in the Justice Committee's report (Joint Committee on Justice, 33/JC/52 2024). In particular, there was significant confusion about the overarching purposes of the proposed use case and, particularly, where the reference images would be drawn from.

In relation to assessing regulatory approaches, a proposal to have empowering legislation is a novel approach that does have the benefit of elevating discussions about the appropriateness and parameters of use of FRT out of simply an interaction between police

and technology suppliers. It also promotes certainty and the rule of law. During this process, it was possible for academics, community representatives, and advocacy organisations to be heard and to test the reasoning behind the proposals. The process elevated the issues of FRT and biometric surveillance more broadly in the public's consciousness.

5. Concluding Remarks

There has been considerable scholarly treatment of the human rights impacts of FRT deployment by police and security services. The parameters and details of principled regulation have had comparatively less analysis, but with recent rapid developments in global regulation, it is possible to observe distinct categories of regulatory approaches to FRT.

This contribution has considered three diverse case studies of regulation of FRT in the policing and security contexts—self-regulation through policy and practice guidelines, wide-ranging cross-national regulation, and national attempts to provide specific legislation. Each shows different challenges and opportunities in regulating the spectrum of use of FRT in policing and security.

The overarching theme in each of these is a struggle to properly define the interests at play. Technology supplier and police-led developments are a feature of early adoption examples. While innovation in technology use in policing and security is absolutely necessary, these instances are unlikely to properly take public and community views into account or have the necessary transparency and legitimacy requirements. There are many examples of good practice in terms of robust guidelines or oversight by independent observers and reviewers, but there is the ever-present risk of internal policy settings changing due to changes in leadership or attitudes.

While the EU AI Act represents the best chance of robust parameters, engagement with concepts such as the proper limits of individual and collective interests in public security and crime prevention usage has been limited. There is a sense that although there was significant ambition to protect individual and collective rights such as privacy and freedom of expression, the carve-outs for law enforcement are such that member states will have significant discretion to use the more intrusive forms of FRT.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflict of interest.

References

Akbari, Ali. 2024. Facial Recognition Technologies 101: Technical Insights. In *The Cambridge Handbook of Facial Recognition in the Modern State*. Edited by Rita Matulionyte and Monika Zalnieriute. Cambridge Law Handbooks. Cambridge: Cambridge University Press, pp. 29–43.

Bradford, Ben, Julia A. Yesberg, Jonathan Jackson, and Paul Dawson. 2020. Live facial recognition: Trust and legitimacy as predictors of public support for police use of new technology. *The British Journal of Criminology* 60: 1502–22. [CrossRef]

Bragias, Adelaide, Kelly Hine, and Robert Fleet. 2021. 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology. *Police Practice and Research* 22: 1637–54. [CrossRef]

Bright, Jo-Anne, Hannah Kelly, Zane Kerr, Catherine McGovern, Duncan Taylor, and John S. Buckleton. 2020. The interpretation of forensic DNA profiles: An historical perspective. *Journal of the Royal Society of New Zealand* 50: 211–25. [CrossRef]

Canal, Felipe Zago, Tobias Rossi Müller, Jhennifer Cristine Matias, Gustavo Gino Scotton, Antonio Reis de Sa Junior, Eliane Pozzebon, and Antonio Carlos Sobieranski. 2022. A survey on facial emotion recognition techniques: A state-of-the-art literature review. *Information Sciences* 582: 593–617. [CrossRef]

Civil Society Organisations (120 Authors). 2021. An EU Artificial Intelligence Act for Fundamental Rights: A Civil Society Statement (30 November 2021). Available online: https://www.amnesty.eu/wp-content/uploads/2021/11/Political-statement-on-AI-Act.pdf (accessed on 1 June 2024).

Cohen, Julie E. 2008. Privacy, visibility, transparency, and exposure. *The University of Chicago Law Review* 75: 181–201.
de Laat, Paul B. 2021. Companies committed to responsible AI: From principles towards implementation and regulation? *Philosophy & Technology* 34: 1135–93.
Department of Justice. 2023. Minister McEntee Receives Cabinet Approval for Draft Facial Recognition Technology Bill. Available online: https://www.gov.ie/en/press-release/797e2-minister-mcentee-receives-cabinet-approval-for-draft-facial-recognition-technology-bill/ (accessed on 1 June 2024).
Fenwick, Helen. 1999. The right to protest, the Human Rights Act and the margin of appreciation. *Modern Law Review* 62: 491. [CrossRef]
Fontes, Catarina, and Christian Perrone. 2021. Ethics of Surveillance: Harnessing the Use of Live Facial Recognition Technologies in Public Spaces for Law Enforcement. *Technical University of Munich Research Brief*. Available online: https://ieai.sot.tum.de/wp-content/uploads/2021/12/ResearchBrief_December_Fontes-1.pdf (accessed on 1 June 2024).
Fussey, Pete, Bethan Davies, and Martin Innes. 2021. 'Assisted' facial recognition and the reinvention of suspicion and discretion in digital policing. *The British Journal of Criminology* 61: 325–44. [CrossRef]
Fussey, Peter, and Daragh Murray. 2019. Independent report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. Available online: https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf (accessed on 1 June 2024).
Garvie, Clare, and Jonathan Frankle. 2016. Facial-recognition software might have a racial bias problem. *The Atlantic* 7: 2017.
Gautam, Ayush. 2023. The evaluating the impact of artificial intelligence on risk management and fraud detection in the banking sector. *AI, IoT and the Fourth Industrial Revolution Review* 13: 9–18.
Glukhin v. Russia. 2023. European Court of Human Rights (Application no. 11519/20).
Hall, Lucy B., and William Clapton. 2021. Programming the machine: Gender, race, sexuality, AI, and the construction of credibility and deceit at the border. *Internet Policy Review* 10: 1–23. [CrossRef]
Hall, Nina, Justine Lacey, Simone Carr-Cornish, and Anne-Maree Dowd. 2015. Social licence to operate: Understanding how a concept has been translated into practice in energy industries. *Journal of Cleaner Production* 86: 301–10. [CrossRef]
Irish Council for Civil Liberties. 2023. ICCL Welcomes AI Act Vote in European Parliament. (14 June 2023). Available online: https://www.iccl.ie/2023/iccl-welcomes-ai-act-vote-in-european-parliament/ (accessed on 1 June 2024).
Jain, Anil K., Debayan Deb, and Joshua J. Engelsma. 2021. Biometrics: Trust, but verify. *IEEE Transactions on Biometrics, Behavior, and Identity Science* 4: 303–23. [CrossRef]
Jasserand, Catherine. 2016. Legal Nature of Biometric Data: From'Generic'Personal Data to Sensitive Data: Which Changes Does the New Data Protection Framework Introduce? *European Data Protection Law Review* 2: 297. [CrossRef]
Johnson, Thaddeus L., Natasha N. Johnson, Denise McCurdy, and Michael S. Olajide. 2022. Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly* 39: 101753. [CrossRef]
Joint Committee on Justice, 33/JC/52. 2024. *Joint Committee on Justice Report on Pre-Legislative Scrutiny of the General Scheme of the Garda Síochána (Recording Devices) (Amendment) Bill 2023*.
Kostka, Genia, Léa Steinacker, and Miriam Meckel. 2023. Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology. *Government Information Quarterly* 40: 101761. [CrossRef]
Kovera, Margaret Bull, and Eliana Aronson. 2023. Eyewitness Identification. In *Routledge Handbook of Evidence-Based Criminal Justice Practices*. London: Routledge, pp. 258–64.
Limantė, Agnė. 2023. Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out. *Nordic Journal of Human Rights*, 1–20.
Lohr, Steve. 2022. Facial recognition is accurate, if you're a white guy. In *Ethics of Data and Analytics*. Boca Raton: Auerbach Publications, pp. 143–47.
Lynch, Nessa. 2022. Beyond the Ban—Principled Regulation of Facial Recognition Technology. In *More Zeros and Ones: Digital Technology, Maintenance and Equity in Aotearoa New Zealand (Bridget Williams Books)*. Edited by Kelly Pendergast and Anna Pendergast. Wellington: Bridget Williams Books, pp. 121–82.
Lynch, Nessa, and Andrew Chen. 2021. Facial Recognition Technology: Considerations for Use in Policing. Report Commissioned by the New Zealand Police. Available online: https://www.police.govt.nz/sites/default/files/publications/facial-recognition-technology-considerations-for-use-policing.pdf (accessed on 1 June 2024).
Lynch, Nessa, and Liz Campbell. 2024. Principled Regulation of Facial Recognition Technology- A View from Australia and New Zealand. In *The Cambridge Handbook of Facial Recognition in the Modern State*. Edited by Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press.
Lynch, Nessa, Faith Gordon, and Liz Campbell. 2024. Facial recognition technology: The particular impacts on children. In *Privacy, Technology, and The Criminal Process*. London: Routledge, pp. 136–55.
Lynch, Nessa, Liz Campbell, Joe Purshouse, and Marcin Betkier. 2020. Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework. Available online: https://www.wgtn.ac.nz/__data/assets/pdf_file/0010/1913248/Facial-Recognition-Technology-in-NZ.pdf (accessed on 1 June 2024).
Mantelero, Alessandro. 2016. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review* 32: 238–55.
Moreham, Nicole A. 2006. Privacy in public places. *The Cambridge Law Journal* 65: 606–35. [CrossRef]

Murphy, Julian R. 2018. Chilling: The constitutional implications of body-worn cameras and facial recognition technology at public protests. *Washington and Lee Law Review Online* 75: 1.
New Zealand Government. 2020. Algorithm Charter for Aotearoa New Zealand. Available online: https://www.data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf (accessed on 1 June 2024).
Neyroud, Peter, and Emma Disley. 2008. Technology and policing: Implications for fairness and legitimacy. *Policing: A Journal of Policy and Practice* 2: 226–32. [CrossRef]
Paik, Sejin, Kate K. Mays, Rebecca Giovannetti, and James Katz. 2022. Invasive yet inevitable? Privacy normalization trends in biometric technology. *Social Media+ Society* 8: 20563051221129147. [CrossRef]
Phillips, P. Jonathon, Amy N. Yates, Ying Hu, Carina A. Hahn, Eilidh Noyes, Kelsey Jackson, Jacqueline G. Cavazos, Géraldine Jeckeln, Rajeev Ranjan, Swami Sankaranarayanan, and et al. 2018. Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. *Proceedings of the National Academy of Sciences USA* 115: 6171–76. [CrossRef] [PubMed]
Podoletz, Lena. 2023. We have to talk about emotional AI and crime. *AI & Society* 38: 1067–82.
Purshouse, Joe, and Liz Campbell. 2019. Privacy, crime control and police use of automated facial recognition technology. *Criminal Law Review* 2019: 188–204.
Purshouse, Joe, and Liz Campbell. 2022. Automated facial recognition and policing: A Bridge too far? *Legal Studies* 42: 209–27. [CrossRef]
R (Bridges) v Chief Constable of South Wales Police. 2019. EWHC 2341.
R (Bridges) v Chief Constable of South Wales Police & Ors. 2020. EWCA Civ 1058.
Ribeiro, Bernardete, Gonçalo Oliveira, Ana Laranjeira, and Joel P. Arrais. 2017. Deep learning in digital marketing: Brand detection and emotion recognition. *International Journal of Machine Intelligence and Sensory Signal Processing* 2: 32–50. [CrossRef]
Scherer, Matthew U. 2015. Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology* 29: 353.
Shapiro, Peter N., and Steven Penrod. 1986. Meta-analysis of facial identification studies. *Psychological Bulletin* 100: 139. [CrossRef]
Solove, Daniel J. 2010. *Understanding Privacy*. Cambridge: Harvard University Press.
Stevens, Nikki, and Os Keyes. 2021. Seeing infrastructure: Race, facial recognition and the politics of data. *Cultural Studies* 35: 833–53. [CrossRef]
United Nations Human Rights Council. 2019. *The Right to Privacy in the Digital Age*. A/HRC/RES/42/15. Geneva: United Nations Human Rights Council.
Williams, Robin, and Paul Johnson. 2005. Inclusiveness, effectiveness and intrusiveness: Issues in the developing uses of DNA profiling in support of criminal investigations. *Journal of Law, Medicine & Ethics* 33: 545–58.
Wu, Haiyu, Vítor Albiero, K. S. Krishnapriya, Michael C. King, and Kevin W. Bowyer. 2023. Face recognition accuracy across demographics: Shining a light into the problem. Paper presented at IEEE/CVF Conference on Computer Vision and Pattern Recognition, Vancouver, BC, Canada, June 17–24; pp. 1041–50.