

Human Rights and Facial Recognition in the Digital Age*

Pete Fussey

(Professor and Head of Department for Sociology, Social Policy and Criminology at the University of Southampton, UK)

Daragh Murray

(Senior Lecturer in Law at Queen Mary University of London, UK, and UKRI Future Leaders Fellow in AI and Human Rights)

ABSTRACT This paper analyses the human rights considerations that arise from the growing application of facial recognition technology in public. Although rooted in the experiences of UK deployments of FRT, the paper also seeks to assess wider international implications. In doing so, the discussion is organised over three substantive areas of analysis. The first section defines the core elements of FRT. The second part identifies the diverse operational and jurisdictional applications of this technology before focusing most explicitly on human rights considerations in the third section. The paper concludes with two key points. First, to be considered ‘in accordance with the law’, a legal basis authorising the use of FRT must exist, and this must meet quality requirements established in case law. Second, any use of FRT must be ‘necessary in a democratic society’. This requires that police forces evidence the utility linked to particular FRT uses, and that the associated harms to human rights be evaluated. Essential to this calculation of harm are the chilling effects of surveillance.

KEYWORDS: Surveillance - Facial recognition - Human rights

TABLE OF CONTENTS: 1. Introduction. – 2. The form and function of facial recognition technologies. – 3. Applications and use of facial recognition technologies. – 4. Human rights implications of facial recognition technologies. – 4.1. Range of human rights implicated. – 4.1.1. The right to privacy. – 4.1.2. Prohibition on discrimination. – 4.1.3. Freedom of expression, and of assembly. – 4.2. Legal and procedural implications. – 4.2.1. Uses of facial recognition ‘in accordance with the law’. – 4.2.2. FRT and the ‘necessary in a democratic society’ test. – 5. Conclusion.

1. Introduction

Facial Recognition Technology (FRT) use by law enforcement has expanded at an accelerating rate in recent years. Although the technology itself has been in existence for over 50 years, advances in artificial intelligence have only recently transformed FRT into a viable policing tool. As Gates¹ (2011) documented, Japanese technology company NEC first exhibited the technology at Expo 1970 in Osaka, but its operation was beset with inaccuracies and other failures. Then followed policing experiments around the turn of the millennium in both Florida and London, where evidence of meaningful success is absent (see Fussey and Murray 2025).²

However, from 2014 onwards, new AI architecture - specifically the use of convolutional neural networks to optimise image analysis - led to the deployment of FRT across social media platforms. It is this innovation and its extensive testing that transformed the technology into a viable policing surveillance capability. What is particularly notable is how, in many jurisdictions, this technology has expanded in the absence of meaningful oversight or regulatory points of friction. In the absence of such safeguards, this paper analyses the human rights considerations that arise from the growing application of this technology in public. Although rooted in the experiences of UK deployments of FRT, the paper also seeks to assess wider international implications. In doing so, the discussion is organised over three substantive areas of analysis. The first section defines the core elements of FRT. The second part identifies the diverse operational and jurisdictional applications of this technology before focusing most explicitly on human rights considerations in the third section. The paper concludes with two key

* Article submitted to double-blind peer review.
This work was funded by a UKRI Future Leaders Fellowship grant MR/T042133/2.

¹ K. Gates, *Our Biometric Future: Facial recognition technology and the culture of surveillance*, New York, NYU Press, 2011.

² P. Fussey and D. Murray, *Facial Recognition Surveillance: Policing and human rights in the age of AI*, Oxford, Oxford University Press, 2025.

points. First, to be considered ‘in accordance with the law’, a legal basis authorising the use of FRT must exist, and this must meet quality requirements established in case law. Second, any use of FRT must be ‘necessary in a democratic society’. This requires that police forces evidence the utility linked to particular FRT uses, and that the associated harms to human rights be evaluated. Essential to this calculation are the chilling effects of surveillance.

2. The form and function of facial recognition technologies

FRT is an umbrella term that refers to a diverse array of tools and applications designed for the analysis and comparison of facial images. Many ways of categorising FRT exist. One starting point is to highlight a fundamental distinction that lies between two principal forms of image comparison: ‘one-to-one’ (1:1) and ‘one-to-many’ (1:n) types. It has become common to consider these different modalities of FRT together. However, variances in how each operates, the digital architecture that underpins them, and their application impact differently on those subjected to FRT. This distinction is therefore critical for recognising FRT’s diverse human rights implications.

1:1 comparison involves matching an image of a face (the ‘probe’ image) with a stored photograph of the same face (the ‘source’ image). For instance, this form of FRT is employed in smartphones to unlock the device or at e-border gates. This application is generally regarded as less controversial, as it does not require extensive databases to match individuals. In effect, this form of FRT involves a database of one person, the intended user. Such searches are typically (although not exclusively) conducted with the consent of the individuals involved. Furthermore, 1:1 FRT is often considered a form of ‘verification’, as it confirms an individual’s identity based on a predefined reference image, rather than ‘identifying’ an individual from a broader pool of potential matches. This distinction positions 1:1 configurations as a more controlled and less controversial form of FRT. However, cases exist of information collected for 1:1 matching then being repurposed for other uses. This issue currently exists in the expansion of retrospective facial recognition uses in the United Kingdom where the national passport

image database has recently been opened to the police to enable retrospective facial recognition searches, with no constraints on access.³ Here, factors of geography (most of the country being a physical island) and geopolitics (outside both Schengen and the EU) mean passport ownership is particularly necessary (76.7% of citizens own a passport⁴). This demonstrates clear limitations on consent and foreseeability regarding how images become deployed in FRT databases.

1:n matching is the form most commonly used in law enforcement settings. This form is more controversial and has attracted wider criticism. Much of this debate turns on ability to identify previously unidentified persons and the need that 1:n FRT has for a database of potential matches as a basic requirement to function. In anglophonic countries this source database is often referred to as a ‘watchlist’. 1:n (or ‘1:many’) forms of FRT vary across different jurisdictions and applications. While the distinction between these classifications are open to debate (see below), many law enforcement agencies classify three broad subcategories of 1:n FRT. These are:

Live facial recognition (LFR): Also referred to as ‘real time’ in EU legislation, this involves the processing of video feeds as people pass cameras. No recording of images is required (although in practice live feeds are typically also recorded).

Retrospective facial recognition (RFR): The application of FRT algorithms to captured images or video footage.

Operator Initiated Facial Recognition (OIFR): A combination of the above. Typically, this involves a law enforcement officer with a handheld device (such as a smartphone with a dedicated app) that can check a photo taken by the officer against identities on a database.

FRT largely refers to a form of software.⁵

³ Liberty Investigates, *Live Facial Recognition Cameras May Become “Commonplace” as Police Use Soars*, 25 May 2025, London, Liberty, available at: <https://libertyinvestigates.org.uk/articles/uk-police-forces-pursuing-major-expansion-of-facial-recognition-capabilities>.

⁴ Office for National Statistics, *International migration, England and Wales: Census 2021*, London, ONS, 2021.

⁵ For example, facial recognition software can be applied to existing camera infrastructure, or police databases to process captured images and match them against a database. A non-law enforcement example of this process is the way social media platforms automatically detect faces and suggest ‘tagging’ individuals in online photographs. This means facial recognition technology can be used in an extremely

As such, it can be retrofitted to existing surveillance infrastructure - such as street based surveillance cameras - allowing already present assets to become considerably more potent. The software composition of FRT also allows it to interconnect and interoperate with other visual surveillance tools. For example, it can be combined with advanced 'video analytics' such as the automated detection of passenger behaviour at transport hubs, thus matching 'identity' with behaviour' and so on. Other forms of analytics can also be applied on top of facial recognition so that, for instance, alerts can be generated when individuals leave certain areas or meet certain people, or facilitating the development of 'pattern of life' profiles.

3. Applications and use of facial recognition technologies

The acceleration of FRT adoption means it is now used over an expanding range of applications. Beyond law enforcement these include: military uses,⁶ humanitarian contexts (for facilitating access to assistance, entry to facilities, and verifying identities in asylum applications),⁷ borders,⁸ retail,⁹ and as part of regeneration/gentrification programmes.¹⁰ Three issues are notable here. First, many of these uses exist despite a complete absence of meaningful regulation or oversight. Second, interaction exists between these sectors (for example, matches created in retail settings being passed to the police¹¹). Third is the

wide range of settings and applications.

⁶ For examples of Israel Defense Force use of facial recognition tools in Palestine see Amnesty International, *Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT*, 2023, available at: www.amnesty.org/en/documents/mde15/6701/2023/en.

⁷ See UNHCR, *Biometrics*, 2022, available at: https://help.unhcr.org/jordan/wp-content/uploads/sites/4/6/2022/04/Biometrics-EN_Final_April2022.pdf.

⁸ See Amnesty International, USA: *Mandatory use of CBP One Application Violates the Right to Seek Asylum*, 2023, 10, available at: www.amnesty.org/en/documents/amr51/6754/2023/en.

⁹ In January 2024, The Observer documented how many retail uses of FRT were concentrated in poorer neighbourhoods. See *Facial Recognition Cameras in Supermarkets "Targeted at Poorer Areas" in England*, available at: www.theguardian.com/uk-news/2024/jan/27/facial-recognition-cameras-in-supermarkets-targeted-at-poor-areas-in-england.

¹⁰ For detail on many of these applications see P. Fussey and D. Murray, *Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence*, Oxford: Oxford University Press, 2025.

¹¹ Financial Times, *London's Kings Cross Uses Live*

rapidly expanding footprint of use. In the UK, South Wales Police have recently covered large parts of the city in facial recognition equipped cameras to cover sporting events,¹² FRT is increasingly deployed in a range of retail outlets across the country,¹³ while technologies such as Clearview allow FRT to be used in any location.

Recent years have also seen the spread of FRT to new jurisdictions. Accurately mapping this distribution is challenging, given the inconsistent methodologies and approaches used to capture this information, and lack of transparency by users. Nevertheless, documented public uses of FRT in Europe and North America include, the UK, US, Germany, France, Greece, Netherlands, Italy, and by Europol. Additional to these are documented plans to use the technology in Hungary to surveil Pride celebrations and explicitly persecute LGBTQ+ communities.¹⁴ In the Majority World, documented uses of FRT exist in, but are not limited to, India, China, Brazil, Uganda, Zimbabwe, and by Israel in Palestine.¹⁵

4. Human rights implications of facial recognition technologies

Understanding the human rights implications of facial recognition technology implicates several human rights law considerations. These include the range of rights affected and the processes required to ensure any uses of such technology are human rights compliant. Before exploring these, it is also important to explain how human rights are engaged, and how the lawfulness of any interference with human rights is evaluated. Generally speaking, the concept of a human

Facial Recognition in Security Cameras, 12 August 2019, available at: www.ft.com/content/8cbcb3ae-babd-11e9-8a88-aa6628ac896c.

¹² South Wales Police, *Live Facial Recognition Deployments*, 2025, available at: www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/deployments-for-live-facial-recognition.

¹³ See The Observer, 2024, *above*.

¹⁴ The Guardian Hungary bans Pride events and plans to use facial recognition to target attendees, 18 March 2025. It is relevant to note that the European has issued a declaration that they are "currently assessing"-investigating - this case. See www.politico.eu/article/hungary-eu-watchlist-facial-recognition-surveillance-lgbtq-pride.

¹⁵ P. Fussey and D. Murray, *Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence*, Oxford, Oxford University Press, 2025.

rights ‘interference’ becomes relevant when any specific right (or combination of rights) is affected, i.e. when those rights are ‘engaged’. An important clarification is required here. Interference does not necessarily translate into a ‘violation’ or infringement of a right. Instead, it is important to assess the degree to which an ‘interference’ is *justified* in terms of human rights law. It is this evaluation that confirms whether rights are violated, or not. With respect to the rights engaged by FRT a three-part test is applied. To be legitimate any interference must be (1) in accordance with the law, (2) in pursuit of a legitimate aim, and (3) necessary in a democratic society.¹⁶ Good faith police deployments typically satisfy the ‘legitimate aim’ test as a matter of routine, and this element is not addressed further here.

4.1. Range of human rights implicated

4.1.1. The right to privacy

Privacy is the most prominent area of rights-focused debate with respect to the impact of advanced surveillance technologies. In Europe, privacy is enshrined in Article 8 of the European Convention on Human Rights (ECHR) as “Article 8(1): Everyone has the right to respect for their private and family life, their home, and their correspondence”. The ECHR designates Article 8 as a ‘qualified right’, e.g. that it can be modified in certain circumstances, in other words that an interference can be permitted if certain circumstances, conditions and justifications are met. These conditions are particularly relevant to law enforcement uses of FRT and are set out in Article 8(2):

Public authorities may not interfere with the exercise of this right unless such interference is in accordance with the law and necessary in a democratic society for reasons such as national security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others.

¹⁶ This three-part test is based on the European Convention on Human Rights, and consistently applied in European Court of Human Rights caselaw relevant to the right to privacy, and the rights to freedom of expression, assembly and association, and thought, conscience and religion. However, a similar test is applied in relation to equivalent rights under the International Covenant on Civil and Political Rights. See, e.g., Human Rights Committee, General Comment No. 37, UN Doc. CCPR/C/GC/37, 17 September 2020, para. 36.

Case law on uses of FRT is sparse (but not absent). The core question is whether uses of FRT in public gives rise to an interference with the right to privacy. A key consideration for the privacy impacts of FRT is the distinction made by the European Court of Human Rights (ECtHR) between the mere observation of people in public, and the recording or further processing of public activities.¹⁷ Live FRT systems inherently require processing of individuals’ image data for their basic functionality, while retrospective FRT is applied to recorded imagery: it is on these bases that an interference with the right to privacy arises. The first ECtHR decision to explicitly focus on FRT (*Glukhin v. Russia*) confirmed this conclusion and asserted that FRT is ‘highly intrusive’ with regard to the right to privacy.¹⁸ As such, a high level of justification will be required to legitimate FRT; that is, for specific FRT uses to be considered ‘necessary in a democratic society’.

While the right to privacy is, of course, relevant to any analysis of FRT, the below discussion demonstrates how privacy, of itself, is an insufficient lens through which to view the range of potential human rights harm brought by FRT.

4.1.2. Prohibition on discrimination

A key human rights concern associated with FRT has been its capacity to introduce – or reproduce – biases into policing processes. This debate connects most explicitly to human rights standards that prohibit discrimination. Most commentary in this area has focused on issues of race and gender¹⁹ although considerations of other protected characteristics, notably age, are also relevant. Article 26 of the ICCPR sets out the prohibition on discrimination as does Article 14 of the ECHR.²⁰ Of note here is the

¹⁷ *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019.

¹⁸ *Glukhin v. Russia*, Judgment, ECtHR, App. No. 11519/20, 4 July 2023, para. 88.

¹⁹ J. Buolamwini and T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, in *Proceedings of Machine Learning Research*, 81, 2018.

²⁰ P. Fussey and D. Murray *Facial Recognition Surveillance* highlights how the ICCPR definition is broader. Under the ECHR the prohibition of discrimination applies not as a standalone right, but in relation to the enjoyment of other ECHR rights. However, in a FRT context, the use of FRT will, at a minimum implicate the right to privacy, and so the

prohibition of both *direct* and *indirect* discrimination, e.g. intentional discrimination and when apparently neutral processes have discriminatory outcomes. Considering these prohibitions in light of FRT means that no difference in treatment on the basis of protected characteristics should arise between those scanned by the technology. Added to this is a positive obligation in many states to prevent discrimination.

Much of the discrimination debate turns on the issue of algorithmic bias, and the established empirical fact that FRT algorithms perform differently across different demographic groups, notably race, gender and age. The most comprehensive of these studies analysed 18.27 million images of 8.49 million people through 189 algorithms from 99 developers and found extensive demographic disparities.²¹ However, while these performance-focused debates are significant, it is also important to recognize that FRT is a socio-technical system. An exclusive focus on algorithmic bias fails to account for the human-centric activities that are crucial to the operation of FRT. For example, questions arise over the composition of watchlists, sources of data, and criteria for enrolment. In addition, FRT matches trigger human action, involving decisions over the credibility of computer-issued matches and whether to intervene or intercept an individual. Some jurisdictions without statutory requirements for citizens to carry identity documents, such as the UK, have detailed rules overseeing the confirmation of identities on the street when doubt arises over the credibility of an individual's response to questioning.²² Each of these stages involves human discretion and has scope for discrimination to arise.

Crucially important here is the way statistical 'evidence' has been recruited to claim law enforcement uses of FRT are not biased against specific demographic groups. In the UK, London's Metropolitan Police Service commissioned a report by the National Physical Laboratory (NPL) to assess the degree of bias in its FRT algorithms and concluded their system did not perform significantly different across demographic

groups when used at certain settings (NPL 2023). Interesting here is the way the London study contradicts scientific orthodoxy on this issue, and that this minority study is the standard relied on by the police. In addition, the NPL report does not list details of any independent peer review of its findings, which would constitute a standard for scientific publications in this field. Analysing such research also reveals how narrowly conceived studies become recruited to justify politicised policing decisions.²³

To interrogate the issues, it is first necessary to articulate how LFR sensitivity is set. LFR operates by setting a threshold for which an alert is issued for a facial recognition match. This is broadly analogous to a 'correlation coefficient'. Statistically, this coefficient is a value somewhere between 0 and 1. A zero means no match at all (e.g. cats and dogs), a value of one denotes a complete match (dogs and dogs). If the sensitivity is set very high (for example, at 0.8), then the system will be more accurate but match fewer individuals. The opposite is true for lower sensitivity ratings. The NPL report identifies bias in the NEC algorithm until the threshold is set particularly high (0.64) before an alert is issued, and none above this range. However, such findings are a result of how statistics work, rather than how FRT operates. If the system sensitivity is set so high, very few matches occur. Therefore, very fewer matches are analysed for demographic bias. In fact, in the report used by the Metropolitan Police, no matches occurred at this level. The system simply was not tested at this level, and so the authors claimed there was no demographic bias. Important here is the way such flawed research adopts the appearance of scientific rigour and is used as evidence of such. By contrast, disputing such flimsy claims requires a detailed analysis of statistical method involving nuance that is not captured in public, political and media discourses of FRT.

The positive obligation that exists in many jurisdictions to prohibit discrimination also raises questions over the very generalized, utilitarian, notions of public support that are often used to justify the deployment of FRT.

Article 14 prohibition of discrimination is applicable.

²¹ NIST *Ongoing Face Recognition Vendor Test (FRVT) Part 3: Demographic effects*, Washington DC, US Department of Commerce, 2019.

²² In the UK, for example, this is set out in s24 of the Police and Criminal Evidence Act (PACE) 1984.

²³ See P. Fussey and D. Murray, cit., for an expansion of this argument, specifically with reference to how police necessity calculations become decorated with the language of science, statistics that hold little substantive meaning yet serve to legitimate the use - and deflect criticisms - of such tools.

Aggregated majority opinion is insufficient to address issues affecting minority rights and the prohibition of discrimination. This issue also raises questions over how knowledge is gained to evidence levels of public support. Existing research highlights how support for FRT can vary considerably in relation to dependent variables of demographics, social location and political beliefs. In the UK, for example, statistics illustrating overall majority support for FRT concealed significant opposition among the young and some (over policed) ethnic minorities.²⁴ An added complexity is the extent to which people are aware of the implications of FRT technology. Nevertheless, understanding levels of public acceptability and consent for FRT holds important relevance for considerations of policing legitimacy and public trust. When considering the impact of these technologies on the documented phenomena of surveillance chilling effects,²⁵ such impact extend to the core elements of democratic functioning itself.

4.1.3. Freedom of expression, and of assembly

The rights to freedom of expression, and of assembly, are protected under Articles 10 and 11 of the European Convention on Human Rights.²⁶ For the ECtHR, particular connection has been made between the rights to freedom of expression and freedom of assembly and democratic functioning. ECtHR case law has consistently held that, “[F]reedom of expression constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and for each individual’s self-fulfilment”,²⁷ and that “the right to freedom of assembly is a fundamental right in a democratic society and, like the right to freedom of expression, is one of the

foundations of such a society.”²⁸

FRT implicates the rights to freedom of expression and of assembly in multiple ways. Most directly is via the potential of the technology to assert chilling effects that deter individuals from exercising particular rights. The chilling effects of surveillance have been extensively documented through empirical research. This includes quantitative research focused on *measuring* changes in online behaviour²⁹ and surveys on government surveillance.³⁰ Peer reviewed qualitative research has also offered detail on first hand lived experience of surveillance chilling effects³¹ and includes studies of police surveillance in minority communities³² and the breakdown in trust among activists engaging in democratic processes.³³

Intrusive surveillance tools, including LFR therefore hold the potential to assert chilling effects and, by extension, deter individuals from exercising rights to expression and assembly. Of note is the wider recognition of the role digital technologies - including FRT – may have in implicating these rights in the context of protests, or other forms of political activity. For example, one 2022 study in London recorded that 38 percent of individuals under the age of 24 would be deterred from attending an event that was policed by facial recognition technologies.³⁴

²⁸ *Kudrevicius and Others v. Lithuania*, Grand Chamber, ECtHR, App. No. 15 October 2015, para. 91.

²⁹ J.W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, in *Berkeley Technology Law Journal*, vol. 31, Issue 1, 117-182, 2016.

³⁰ E. Stoycheff, *Under Surveillance: Examining Facebook’s Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, in *Journalism & Mass Communication Quarterly*, vol. 93, Issue 2, 2016, 296-311.

³¹ D. Murray, P. Fussey, K. Hove, W. Wakabi, P. Kimumwe, O. Saki and A. Stevens, *The Chilling Effects of Surveillance and Human Rights: Insights from qualitative research in Uganda and Zimbabwe*, in *Journal of Human Rights Practice*, vol. 16, Issue 1, 2023, 397-412; A. Stevens, P. Fussey, D. Murray, K. Hove and O. Saki, *I Started Seeing Shadows Everywhere’: The diverse chilling effects of surveillance in Zimbabwe*, in *Big Data and Society*, vol. 10, Issue 1, 2023.

³² A. Ali, *Citizens under Suspicion: Responsive Research with Community under Surveillance*, in *Anthropology & Education Quarterly*, vol. 47, Issue 1, 2016, 78-95.

³³ A. Starr, L.A. Fernandez and R. Amster, *The Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis*, in *Qualitative Sociology*, vol. 31, Issue 3, 2008, 251-270.

³⁴ London Police Ethics Panel, *Final Report on Live Facial Recognition*, London, Mayor’s Office for

²⁴ B. Bradford, J. Yesberg, J. Jackson and P. Dawson, *Live Facial Recognition: Trust and Legitimacy as Predictors of Public Support for Police Use of New Technology*, in *The British Journal of Criminology*, vol. 60, Issue 6, 2020, 1502-1522.

²⁵ D. Murray, P. Fussey, K. Hove, W. Wakabi, P. Kimumwe, O. Saki and A. Stevens, *The Chilling Effects of Surveillance and Human Rights: Insights from qualitative research in Uganda and Zimbabwe*, in *Journal of Human Rights Practice*, 2023, <https://doi.org/10.1093/jhuman/huad020>.

²⁶ These rights are also protected under Articles 19 and 21 of the International Covenant on Civil and Political Rights.

²⁷ *Axel Springer AG v. Germany*, Grand Chamber, ECtHR, App. No. 39954/08, 7 February 2012, para. 78.

The 2024 UN Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests recognises this potential harm to human rights, and imposes strict restrictions on the use of FRT. Key sections include:

32. Digital technologies should not be used to categorize, profile or remotely identify individuals, including by biometric means, during protests, given that they are discriminatory and inconsistent with the obligation of law enforcement officials to facilitate peaceful protests.

33. In the light of the pace of technological change, untested or unproven new technologies or technologies that have evolved should not be deployed during protests. Such technologies should be subject to full, independent human rights review and technical testing, in line with international human rights standards, that must also evaluate the likely impact on individuals and groups in situations of vulnerability.³⁵

4.2. Legal and procedural implications

4.2.1. Uses of facial recognition ‘in accordance with the law’

In human rights law, the purpose of the ‘in accordance with the law’ requirement is to ensure a legal framework capable of preventing the arbitrary exercise of State – or in this case police – powers. This is essential to ensure that any human rights interferences are appropriately limited. Specifically, human rights law requires that a legal basis for a rights interference exist,³⁶ and, crucially, that this legal basis be of sufficient *quality* to protect against arbitrary rights interferences. The quality component has two elements. First, the legal framework must be accessible, and second, its consequences must be foreseeable.³⁷ The requirement that the legal framework be accessible to the public is a core component of the rule of law: an individual should know the extent of the State’s powers, and the rules that they are bound by. The

Policing and Crime, 2019.

³⁵ UN Human Rights Council, Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, Geneva: UN HRC.

³⁶ This legal basis may arise as a result of dedicated legislation, or on the basis of common law powers.

³⁷ *Roman Zakharov v. Russia*, Grand Chamber, ECtHR, App. No. 47143/06, 4 December 2015, para. 228; *Gillan and Quinton v. the United Kingdom*, Judgment, ECtHR, App. No. 4158/05, 12 January 2010, para. 76.

foreseeability requirement relates to the precision with which the legal framework is formulated.³⁸ In *Catt*, the European Court of Human Rights stated that ‘[f]or domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope and discretion conferred on the competent authorities and the manner of its exercise’.³⁹ It is likely that a high degree of precision will be required of any legal framework regulating police use of FRT, given the level of intrusiveness linked to the technology, the number of people affected, and the consequences for those implicated by its use.⁴⁰ The term legal framework is used here, rather than law, as it is possible that common law⁴¹ powers coupled with a publicly accessible policy framework may be sufficient to satisfy the in accordance with the law test. This issue is currently unsettled before the UK courts, although we argue that this common law/policy framework combination is insufficient and that a legislative framework is required for FRT to be ‘in accordance with the law’.⁴²

Four legal risks are linked to many public uses of FRT. First, in the absence of either an explicit legal basis,⁴³ or a publicly accessible policy framework, it is highly unlikely that police uses of FRT could be considered ‘in accordance with the law’. Second, any limitation on a human right must be accessible. In many jurisdictions, the public currently has no means of obtaining any information on police uses of FRT. Third, any limitation must be foreseeable. This is intended to limit officer discretion, and to

³⁸ *Perincek v. Switzerland*, Grand Chamber, ECtHR, App. No. 27510/08, 15 October 2015, para. 131.

³⁹ *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 94.

⁴⁰ *Gillan and Quinton v. the United Kingdom*, Judgment, ECtHR, App. No. 4158/05, 12 January 2010, para. 77.

⁴¹ Common law jurisdictions include Australia, Bahamas, Barbados, Belize, Bermuda, Canada (excl. Quebec), Cayman Islands, Fiji, Ghana, India, Ireland, Jamaica, Kenya, New Zealand, Nigeria, Pakistan, Singapore, Tanzania, Trinidad and Tobago, Uganda, United States.

⁴² See P. Fussey and D. Murray, *Facial Recognition Surveillance*, cit.

⁴³ It is noted that in *Catt* the European Court of Human Rights expressed concern regarding reliance on the use of common law powers for invasive surveillance measures, in this case the ... The Court did not, however, rule on this point. *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 105.

protect against arbitrariness. For example, in *Glukhin*, the Court expressed concern that the law did not appear to place any limits on officer discretion, stating that: ‘[t]he domestic law does not contain any limitations on the nature of situations which may give rise to the use of facial recognition technology, the intended purposes [or] the categories of people who may be targeted’.⁴⁴ Fourth, in our research in the UK, for example, we have seen no examples of guidance setting out factors such as: the limitations of facial recognition technology itself, risks linked with its use (such as automation bias), or examples illustrating how officers can approach the necessity and proportionality test.⁴⁵ Such guidance can play a key role in ensuring that officers are equipped to grapple with the complex and novel issues raised by FRT use.

4.2.2. FRT and the ‘necessary in a democratic society’ test

The necessity test is intended to ensure the overall human rights compliance of a measure; i.e. can that measure be considered necessary in a democratic society, bearing in mind the values associated with such a society.⁴⁶ A core objective of the necessity test is the resolution of the ‘competing interests’ at play in a specific context.⁴⁷ In the context of FRT this relates to, on the one hand, the potential benefit to human rights linked to the use of the technology (such as protection of public order or the prevention of crime), and on the other hand, the potential harm linked to that tool (such as to the rights to privacy, freedom of expression, the prohibition of discrimination, etc.). This means that to conduct the necessity test effectively clear articulation of both the potential utility, and the potential harm, associated with a particular surveillance measure must exist.

Evaluating competing interests is not equivalent to a straightforward balancing

exercise. It is not the case that, if the utility outweighs the harm, then the measure may be considered necessary, and therefore lawful. The necessity test must engage with the overall rights impact of a measure, and be consistent with democratic values. In a surveillance context this will often involve a three stage process: A measure may be considered necessary in a democratic society ‘if it answers to a “pressing social need”, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient’.⁴⁸ A pressing social need is not regarded as synonymous with ‘indispensable’, but neither does it have the flexibility of ‘ordinary’, ‘reasonable’, ‘desirable’, or ‘useful’.⁴⁹ Proportionality refers to the relationship ‘between the means used and the aim sought to be achieved’.⁵⁰ This test also requires an examination of alternative, less rights-intrusive means.⁵¹ In *Glukhin*, the European Court of Human Rights classified FRT as a ‘highly intrusive’ technology, the use of which would require a ‘high level of justification’.⁵² This suggests that an appropriate evidence base justifying the use of FRT, in terms of both benefit and harm, should be developed, and that ‘necessity’ threshold will be set high.

When engaging with the necessity test, and assessing utility/harm, a distinction should be made between different FRT use cases. For example, FRT searches made against public databases may raise issues around necessity related to:

- a) What purpose FRT can be used for (i.e. to identify specific individuals linked to a crime, to build an intelligence profile, etc.).
- b) The nature of the offence warranting the use of FRT (i.e. all crime, serious crime, etc.).⁵³
- c) Who it can be used against (i.e. the

⁴⁴ *Glukhin v Russia*, Judgment, ECtHR, App No. 11519/20, 4 July 2023, para. 83.

⁴⁵ This is of particular importance in light of the novel nature of facial recognition technology, and the new human rights considerations it raises. Moreover, as the discussion on discrimination above highlights, a common response of FRT users is to merely state that such risks do not exist.

⁴⁶ *Klass and Others v. Germany*, Judgment, ECtHR, App. No. 5029/71, 6 September 1978, para. 55.

⁴⁷ *S. and Marper v. the United Kingdom*, Judgment, ECtHR, App. Nos. 30562/04 & 30566/04, 4 December 2008, para. 112.

⁴⁸ *Catt v. the United Kingdom*, Judgment, ECtHR, App. No. 43514/15, 24 January 2019, para. 109.

⁴⁹ *Handyside v. the United Kingdom*, Judgment, ECtHR, App. No. 549/72, 7 December 1976, para. 48.

⁵⁰ *Perincek v. Switzerland*, Grand Chamber, ECtHR, App. No. 27510/08, 15 October 2015, para. 228.

⁵¹ *Nada v. Switzerland*, Grand Chamber, ECtHR, App. No. 10593/08, 12 September 2012, para. 183.

⁵² *Glukhin v Russia*, Judgment, ECtHR, App No. 11519/20, 4 July 2023, paras. 86, 88.

⁵³ For instance, *Glukhin* states that: ‘In the assessment of the “necessity in a democratic society” of the processing of personal data in the context of investigations, the nature and gravity of the offences in question is one of the elements to be taken into account”, para. 87.

degree of suspicion, persons of interest).

d) Context specific considerations (*i.e.* is FRT used in the context of a peaceful assembly, or at a religious or cultural event).

Any evaluation of potential harm should also consider the chilling effects of surveillance, noting that these effects are likely to be exacerbated in situations where there is uncertainty as to how the technology is used.

In the absence of a legal or publicly accessible policy framework, it is typically difficult, if not impossible, to evaluate how police uses of FRT engage with the necessity test in order to justify FRT deployments. A principal concern is that no indication exists as to which uses of FRT may be considered ‘necessary in a democratic society’, and on what basis any decision in this regard is made. It is rare that justifications for FRT are provided at more than a general level. An appropriate evidence base setting out this justification has been absent in all FRT policies we have reviewed. Indeed, this lack of clarity over how necessity tests are addressed, and their instrumentalization for the purposes of extending surveillance has been a persistent issue affecting other forms of police surveillance.⁵⁴

5. Conclusion

This paper has set out some of the key human rights considerations that arise in relation to police use of FRT. Whether FRT, in and of itself, can be deployed by the police in a human rights compliant manner is a difficult question to answer. Human rights compliance is invariably context dependent. However, two considerations are clear. First, to be considered ‘in accordance with the law’, a legal basis authorising the use of FRT must exist, and this must meet quality requirements established in case law. Second, any use of FRT must be ‘necessary in a democratic society’. This requires that police forces evidence the utility linked to particular FRT uses, and that the associated harm be evaluated. Essential to this calculation are the chilling effects of surveillance. Our analysis has seen no examples of how these complex

issues have been addressed by those using the technology. Until both the utility and harm associated with specific FRT deployments can be understood and effectively incorporated into a necessity analysis, it is difficult to see how the technology can be considered in accordance with the law and a moratorium on use seems the only appropriate response.

⁵⁴ See P. Fussey and A. Sandhu, *Surveillance Arbitration in the Era of Digital Policing*, in *Theoretical Criminology*, 2022, 26; K. Bullock and P. Johnson, *The Impact of the Human Rights Act on the Police Service in England and Wales*, in *British Journal of Criminology*, vol. 52, Issue 3, 2012.

