Pete Fussey

27 Facial recognition

Abstract: This chapter examines one of the most controversial law enforcement tools of recent years: facial recognition technology. The chapter first charts the growth and development of this technology—from niche curiosity to its current role as a powerful surveillance technology driven by advanced AI processing—before considering the complex human rights and social justice implications of its deployment. It concludes by highlighting how facial recognition, like other advanced digital policing tools, is exerting a profound impact on police–citizen encounters and on the nature of suspicion itself.

Keywords: surveillance, human rights, suspicion

Introduction

Facial recognition technology (FRT) has become one of the most controversial forms policing tools of the 2020s. Evangelists have described it as a 'precision crime fighting tool.' Critics have variously pointed to its overhyped effectiveness, bias across demographic groups, transformatory surveillance potential, and variety of human rights implications. Regarding the latter, members of the EU Parliament voted to ban public uses of live FRT (with notable exceptions) during 2023 and the technology has been prohibited in many parts of the US. Conversely, the UK has seen accelerated uses of FRT across public policing and private retail and leisure spaces. Other forms of FRT are less controversial and increasingly instituted into everyday life. For example, since 2017 Apple has incorporated the technology into its iPhone range. Uses of facial verification at e-borders has also grown and automated tagging of faces on social media platforms has become commonplace.

This contribution discusses the growth, impact, and meaning of FRT in the context of law enforcement. It begins by separating the complex range of technologies commonly considered together. The technological development and subsequent police adoption of FRT is then discussed. The paper then considers the wider implications of this technology, addressing the impact on policing, procedural justice, and the rights of those subjected to such surveillance.

FRT in context

'Facial recognition technology' (FRT) denotes a diverse range of tools and digital architectures. Such differences in FRT are important given their differential impact. The principle division is between 'one to one' ('*1:1*') and 'one to many' ('*1:n*') forms of image comparison. In simplest terms, *1:1* comparison involves photograph of a face

 https://doi.org/10.1515/9783111062037-028

being compared with an image of itself. For example, a smartphone will unlock if the computer judges sufficient resemblance between the presented face and the photograph(s) it holds of the owner. Such applications are less controversial because they do not require a large database of potential matches and matches are largely conducted with the consent of those involved. In some senses, *1:1* FRT may be considered as a form of 'verification,' rather than 'recognition.'

1:n forms are more controversial given they require a database of potential matches to function. This is the mode most typical in law enforcement applications, with databases ('watchlists') commonly including many thousands of enrolled images. For example, the 2023 London Metropolitan Police Service FRT operation at the coronation of King Charles III used a database of around 9,000 individuals, resulting in just one single arrest. *1:n* forms of FRT are further subdivided according to different forms of use. Often viewed as most controversial is 'live facial recognition' (LFR), where cameras scan the faces of passers-by while computers match these images to a police-compiled database of individuals they are interested in. Uses of LFR are limited (mostly to the UK in Europe) and this is the form of surveillance subject to EU and US bans outlined above. The second, similar, form of *1:n* FRT is often called 'Operator Initiated Facial Recognition' (OIFR) whereby software is installed on handheld devices (typically a smartphone) and street-based police officers can photograph faces to compare with a database. More widely used is 'retrospective facial recognition' (RFR), which takes an image from an event—for example, a robbery—and compares that to a database of thousands to find a match. While considered less controversial, RFR turns any recorded public gathering into a surveillance opportunity. Moreover, RFR databases usually implicate—and therefore engage the rights of—significantly more individuals than LFR. For example, US applications of RFR rely on public databases including the driving license register. This allows police to scan against the faces of 117 million American adults (The Perpetual Lineup, 2016). In the UK, during September 2023 the Policing Minister announced an intention to make two enormous databases available for police facial recognition systems. The first is the passport photograph database. 86 % of the UK population holds a passport. The second involves 16 million images held on the Police National Database. In 2012 the High Court of England and Wales ruled that many these images were held illegally by the state. This is because the retention of photographs of those arrested but not convicted was unlawful (*RMC and FJ v Commissioner of Police for the Metropolis [2012] EWHC 1681).* These images remain on the databases used by UK policing today.

More controversial still is US tech company 'Clearview,' which has contracted its services to law enforcement agencies across the world in often opaque and unaccountable circumstances. Clearview operates by allowing faces to be scanned against a vast database of images scraped from the internet. A 2023 estimate placed Clearview's database at around four billion images (Hill, 2023). Such relationships between the number of suspects and the vast database of innocent individuals raise clear questions over proportionality, the right to privacy in public space, and fundamental protections against arbitrary state intervention (see Privacy and Data Protection by Bygrave).

The development of FRT for law enforcement

Facial recognition technology has a surprisingly long history. Gates (2011) credits the first public exhibition of the technology as a demonstration by Japanese technology company NEC (who also manufacture FRT systems currently used by police in London) at the 1970 Expo in Osaka. Law enforcement uses have since been sporadic, with short-lived deployments in Florida and London around the turn of the millennium. In a familiar tale, such uses were declared to have been an enormous success, yet the fact that such schemes were quietly dropped tells a different story. This is likely because, despite the enormous hype that regularly accompanies inaugurations of police technology (see Policing by Wilson), the systems simply failed to work to expectations, were expensive, and drained resources useful for other areas of policing. Things changed around 2015 with advancements in AI-driven computer vision image analytics brought by Convolutional Neural Network (CNN) processing. This step change in capability was further advanced by the integration of this technology into internet search engines and social media platforms that enabled reverse image searching and the automated 'tagging' of online friends.

This step change in digital image analytics translated into enhanced viability of FRT for law enforcement. Enthusiastic early adopters include the U.S. Customs and Border Protection (CBP) agency and UK policing. The former began trialing FRT to verify identifies of travelers between Atlanta and Japan before extending uses to Washington Dulles airport and, since, the processing of migrants arriving at US land borders from northern Mexico. In England, the London Metropolitan Police Service (MPS) began using NEC technology at the capital's 2016 Notting Hill Carnival, a celebration of Caribbean culture and among the largest street carnivals in the world outside Rio's Mardi Gras. Since then, the MPS have conducted an accelerating number of live facial recognition operations in London with many more conducted in the city's privatized spaces and in collaboration with commercial security operators.

Implications for public uses of facial recognition technology

FRT marks a significant shift in the capability of policing but, also, in the ways surveillance itself is conceptualized and critiqued. Proponents have sought to deemphasize the intrusiveness and impact of the technology in several ways. Among these, two justifications are particularly prominent: that FRT is similar to already accepted forms of public surveillance, such as 'CCTV' surveillance cameras, and/or that it is a "precision crime fighting tool" (Metropolitan Police Service, 2023) and, by implication, only intrudes on those 'wanted' individuals sought by the system. Both arguments are briefly analyzed in turn.

The world's first legal challenge to FRT was heard in during summer 2019 by the high court of England and Wales (*R (Bridges) v Chief Constable of South Wales Police and Others [2019] EWHC 2341 (Admin))*, brought jointly by the UK human rights organ-

ization, Liberty, and petitioner, Ed Bridges. The challenge turned on Mr. Bridges' complaint that South Wales Police illegally captured his facial biometric data on two occasions, the second at protest against an arms fair in Cardiff, Wales. The thrust of the complaint was Bridges' claim for judicial review on the assertion that police uses of FRT were not compliant with Article 8 of the European Convention on Human Rights (the right to private and family life), data protection law, and the UK's equalities legislation. The case was complex, and the court originally held many aspects of the police argument before being successfully challenged on appeal in 2020 (*R (on the application of Bridges) v Chief Constable of South Wales Police [2020 EWCA 1058]).* What is notable is that even though the original High Court ruling was excessively deferential to the police, it rejected the police argument that FRT was similar to existing surveillance camera capability. Instead, the court ruled, and thus established as legal fact, that the rights of everyone passing FRT cameras are engaged, rather than solely those individuals on watchlists. As such, FRT is different to open street surveillance cameras because, among other reasons, it engages the rights of *all* passers-by.

Furthermore, FRT technology does not passively observe like other forms of public surveillance. It captures biometric data from individuals, which is a form of data afforded special status under European data protection standards on the grounds it is of a more personal nature. Moreover, for FRT to work, it needs to both *capture* and *process* data. This distinction between data capture and processing—and recognition that the latter is more intrusive—has been recognized by the European Court of Human Rights (ECtHR) in a 2019 ruling against the UK addressing police surveillance practices during protests (*Catt v. the United Kingdom,* Judgment, ECtHR, App. No. 43514/15, 24 January 2019). A subsequent and more recent July 2023 ECtHR ruling (*Glukhin v. Russia* App no 11519/20 [ECtHR, 4 July 2023]) classified retrospective facial recognition and live facial recognition as intrusive and therefore necessitating a high level of justification for their use. Accordingly, the heightened intrusion brought by FRT has been established comprehensively as a legal fact. Such distinctions also hold implications for the ways in which FRT is conceptualized, and further underscore the difficulties of theorizing 'surveillance' as an undifferentiated set of tools and practices.

Regarding performance, it is common to hear impressive claims of FRT effectiveness. For example, Europe's heaviest users of live facial recognition, the London Metropolitan Police Service, claimed in 2023 that the technology as "a precision crime-fighting tactic" (MPS, 2023). They and have previously asserted a false positive rate of between 0.00 % and 0.13 % (MPS, 2020), thus implying the system was rarely wrong. However, closer analysis of these statistics reveals greater complexity and uncertainty over LFR performance. In circumstances where evidence is provided, most claims of positive technical performance are calculated by comparing the number of faces available for matching (e. g., the large number of passers-by) with the small number of actual matches. Therefore, if 100,000 people are estimated to pass a camera and the system incorrectly identifies 100 people, the standard evaluation methodology allows users to claim the systems are 99 % effective. The potential rights interferences of

those 100 individuals incorrectly stopped are concealed. Moreover, this approach allows system failures to be recast as successes. Using this methodology, FRT will always be presented as effective, *irrespective of how it actually performs.*

The impact of FRT

The surveillance potential of advanced facial recognition technologies has wide ranging implications for the rights of citizens, disrupts longstanding formulations of suspicion, and alters the operation of policing itself.

Facial recognition and human rights in the era of digital policing

As highlighted above, FRT has been legally recognized as an intrusive form of surveillance by both domestic and international courts. It is important to note how rights-based deliberations of FRT-related surveillance harms extend beyond notions of privacy (Article 8 of the European Convention of Human Rights (EHRC)). Given how such technologies may exert a chilling effect on individuals and groups (meaning that it inhibits them from exercising their rights; e.g., Stevens et al., 2023), FRT is implicated in the freedoms of expression (Article 10) and freedom assembly and association (Article 11) (Murray, 2023). It could be further argued that the differential performance of FRT across demographic groups, the impact on police suspicion, and the absence of effective oversight also engage the prohibition from discrimination (Article 14), right to liberty and security (Article 4), due process (Article 5), and right to effective remedy (Article 13). Recognizing the breadth of fundamental rights engaged by FRT also reveals the limitations of data protection-focused approaches for regulating this technology (such as that currently pursued by proposed UK legislation, the Data Protection and Digital Information Bill, and, prior to 2023's AI Act, a favoured approach in the EU).

Common to other forms of emerging technology, the ways in which 'necessity' is calculated are crucial to the rights implications of FRT. Typically, States commonly justify temporary limitations of many of the above rights (e.g., privacy or expression) on the basis of public security. Such rights modifications are often permissible if the three-part human rights test (an adequate legal basis, legitimacy, and whether the measure is necessary in a democratic society) is satisfied. While much misunderstood, the necessity calculation typically involves consideration of the utility of the measure and its potential harms. The more nascent a technology, the less is known about either variable.

The prohibition from discrimination

Beyond 'Article 8' rights to privacy, and deserving of its own category of discussion, is the prohibition on discrimination (Article 14 of the ECHR). Accordingly, one of the most animated areas of dispute over FRT is the issue of bias (see Bias by Oswald and Paul). Particularly acute are debates over the differential performance of algorithms in matching faces across visible ethnicities, gender, and age. One touchstone study in the debate is Buolamwini and Gebru's (2018) evaluation of related technology that evidenced (intersectional) poorer performance for females from ethnic minorities. While this research has been criticized on the grounds that Buolamwini and Gebru's (2018) work focuses on gender classification, a distinct and different technology to face recognition, the issue of ethnic, gender, and age-related bias is supported elsewhere. The most authoritative source is the US National Institute for Science and Technology (2019) evaluation of 189 commercially available face recognition algorithms that found them all to operate unequally across demographic groups. From an equality and human rights perspective this would mean someone from these populations is more likely to be incorrectly identified and thus suffer arbitrary rights infringement based on membership of a demographic group.

Subverting suspicion

Much of the complexity surrounding FRT arises because it superficially resembles other forms of more accepted surveillance. As such, any changes brought by the technology may subtle, yet are far reaching in their implications. One such subtle-yet-profound shift concerns how suspicion becomes formulated. These changes may be considered so fundamental that they challenge the basic principles and legal frameworks governing permissible state surveillance practices. Analyzing how FRT is deployed in practical operational settings reveals how the technology can impact suspicion formation in at least five ways:

i. *Subverting the sequence of surveillance.* Most legal frameworks (and all human rights tests) permitting police surveillance follow the core principle that a degree of suspicion needs to exist prior to the enactment of surveillance. This is largely how surveillance tools derive legal authorization and justify their necessity in temporarily modifying suspects' rights to privacy among others. As such, 'suspicion' needs to exist before 'surveillance.' FRT techniques, such as LFR, subvert this. All faces are scanned and deemed suspicious in the first instance, before being discounted by the computer or a human operator. In this way, FRT is much more *active* than other forms of overt surveillance.
ii. *Accountability and the origins of suspicion.* The origins of suspicion formation are complex and vary wildly in robustness and substantiation, from hunches through to criminal justice standards of evidence. Key here is that, however flawed it may be, suspicion traditionally arises from human or procedural activities that, at least

in theory, may be questioned. In the UK, a computational facial recognition match is regarded as reasonable suspicion for a street-based stop and search. Key here is the way suspicion originates outside of human discretion. Added to this is the fact that FRT processing is driven by complex AI architecture, which means the origins of such decisions are not scrutable to humans.

iii. *Technologically structured suspicion.* Relatedly, since the 1960s, sociologies of policing have revealed the complex ways suspicion is framed by myriad environmental and individual factors including organization culture and prejudice. Perhaps most notable among this literature is David Matza's (1969) concept of 'bureaucratic suspicion.' Ethnographic research on operational uses of FRT has argued that the technology brings a new component, the technological framing of bureaucratic suspicion, which can work to prime officers in reinforcing assumptions of guilt (Fussey et al., 2021).

iv. *Disrupting distinctions between covert and overt surveillance.* Many legal frameworks strive to separate covert targeted surveillance from more overt forms, with more legal restrictions and stringent authorization processes applying to the former. Users of FRT often classify the technology as overt. However, FRT relies on a hidden database of suspects. It also relies on the impossibility for individuals to know if they are enrolled onto it, regardless of how visible the cameras are. This means the system relies on covert processing to function.

v. *Individual and categorical suspicion.* That FRT performs differently across demographic categories is a scientific fact. This means the technology is more likely to screen in some demographic categories (e.g., visible ethnicity) for additional scrutiny while having a higher likelihood of incorrectly matching individuals from others (and therefore subjecting them to unnecessary police stops and arbitrary engagement of their rights). The existence of categorical suspicion—particularly on the basis of ethnicity, class, and age—is well established in the sociology of policing (e.g., Campbell, 1999). FRT adds another dimension by reinforcing such discrimination and investing it with a sense of scientific objectivity.

Conclusion

Driven by advancements in AI, current forms of FRT represent a dramatic shift in police surveillance capability. Added to this is the reliance the technology has on extracting biometric data, information categorized with a higher level of sensitivity, to function. One critical feature of debates over FRT, and over advanced AI-driven policing technologies more generally, is their deployment into conditions of legal ambiguity, and of insufficient oversight. This absence of regulatory imagination holds manifold implications.

Most obviously it means the rights of those subjected to such technologies are placed at risk of arbitrary interference. Moreover, many existing legal frameworks lack the quality and reach to offer the necessary protections needed against nascent

technologies. The different cadences of rapid technological innovations that drive such technologies, and the ponderous development of frameworks to regulate them, is a much-admired problem. One uninspired form of solutionism is to assert the primacy of humans—the 'human-in-the-loop'—as a panacea. Neither can human–technological interrelationships be separated so trivially, but human action is not shorn of context, and humans rarely have the capability or motivation to objectively scrutinize complex AI-driven processes. Human adjudication is important, but its capabilities are easily overstated. Worse, it can be offered as a synonym for digital accountability, a Potemkin façade of regulation: seemingly substantial while concealing the nothingness that lies behind. Another approach has been the establishment of AI ethics standards. Frequently normative, and often legally irrelevant, such ethical frameworks have become sufficiently numerous for surveillance users to cherry pick elements that licence and legitimate their actions. Human rights standards are exposed to sustained assault in the current era of populism. Yet they currently provide the most comprehensive means to capture and mitigate the complexity of harms and remedies brought by advanced and intrusive surveillance technologies such as FRT.

Suggested reading

Andrejevic, M., & Selwyn, N. (2022). *Facial Recognition.* New York: Wiley

Fussey, P., Davies, B., & Innes, M. (2021). "Assisted" facial recognition and the reinvention of suspicion and discretion in digital policing. *British Journal of Criminology*, 61(2), 325 – 344. https://doi.org/10.1093/bjc/azaa068

Murray, D. (2023). Police use of retrospective facial recognition technology: A step change in surveillance capability necessitating an evolution of the human rights law framework. *Modern Law Review.* DOI: 10.1111/1468 – 2230.12862

References

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1 – 15

Campbell, E. (1999). Towards a sociological theory of discretion. *International Journal of the Sociology of Law*, 27, 79 – 101.

Fussey, P., Davies, B., & Innes, M. (2021). "Assisted" facial recognition and the reinvention of suspicion and discretion in digital policing. *British Journal of Criminology*, 61(2), 325 – 344. https://doi.org/10.1093/bjc/azaa068

Gates, K. (2011) *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance.* New York: NYU Press

Hill, K. (2023) *Your Face Belongs to Us: The Secretive Startup Dismantling Your Privacy.* New York: Simon & Schuster

Matza, D. (1969) *Becoming Deviant.* Englewood Cliffs, NJ: Prentice-Hall

MPS. (2020). *Metropolitan Police Service Live Facial Recognition Trials.* https://www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf

MPS. (2023). *MPS LFR Policy Document.* https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf

Murray, D. (2023). Police use of retrospective facial recognition technology: A step change in surveillance capability necessitating an evolution of the human rights law framework. *Modern Law Review.* DOI: 10.1111/1468 – 2230.12862

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

Stevens, A., Fussey, P., Murray, D., Hove, K., & Saki, O. (2023) 'I started seeing shadows everywhere': The diverse chilling effects of surveillance in Zimbabwe. *Big Data & Society*, 10(1).

The Perpetual Lineup. (2016) *The Perpetual Lineup: Unregulated Police Face Recognition in America.* https://www.perpetuallineup.org/