Privacy, Crime Control and Police use of Automated Facial Recognition Technology (8831 words)

Joe Purshouse
Lecturer in Criminal Law, University of East Anglia
Liz Campbell
Professor and Francine McNiff Chair in Criminal Jurisprudence, Monash University

This paper discusses the police use of automated facial recognition technology (FRT) as a tool of crime control and public space surveillance. It considers the legality of the police use of FRT in England and Wales, with particular reference to the fundamental rights of those who have been subject to criminal process. Drawing on relevant privacy and criminal law scholarship, this paper argues that inadequate protection has been afforded to the privacy rights, and other human rights of those subject to police FRT surveillance in public space in England and Wales. We therefore suggest that, if FRT is to be deployed in future, a narrower and more prescribed legal framework is necessary.

Introduction

Over the last year, in England and Wales, FRT has been used at a number of crowded events to identify suspects and prevent crime. This technology is purportedly more valuable operationally than ordinary public Closed Circuit Television (CCTV) surveillance as it can identify individuals in real time and link them to other information stored on police databases. FRT involves the identification of an individual based on an analysis of the geometric features of his or her face, and a comparison between the algorithm created from the captured image and one already stored, such as from a custody image or social media account. It has numerous private and public sector applications.[1] Essentially, FRT deploys software to compare a collected image of an individual's face (as taken from a CCTV surveillance camera, for example) to facial images in a previously assembled database (henceforth, a "watch list") with the aim of

[1] Office of the Privacy Commissioner of Canada, *Automated Facial Recognition in the Public and Private Sectors* (Gatineau, QC, 2013), p.1.

gaining a match between a face on the database and the more recently collected image.[2] FRT's commercial applications range from enabling more effective photo sharing on social media sites by identifying faces on images uploaded to platforms such as Facebook and Instagram and linking these to user profiles, through to authenticating employees to access secure premises such as a power plant or prison.[3] Buolamwini and Gebru note that the capacity of FRT to move beyond mere face detection and towards the identification of emotions and personality characteristics is also increasing rapidly and becoming more precise (although such developments remain in their infancy).[4] FRT even holds the potential to ascertain a person's sexuality.[5]

Advances in FRT also have numerous criminal justice and policing applications, and this technology is becoming increasingly popular for police forces across the world. Where successful, such applications often have headline-grabbing effects.[6] FRT has been trialled by a handful of domestic police forces looking to position themselves at the leading edge of technology-led crime control practice. In England and Wales, FRT cameras have been used predominantly in the context of public surveillance operations at large gatherings such as outdoor festivals, sports events or public protests.[7] Though other applications of FRT may be utilised by the police in the future, which would undoubtedly raise significant practical and principled issues, these will not be considered here. In the interests of developing sharper focus, the following analysis is

[2] L.D. Introna and H. Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues* (Center for Catastrophe Preparedness and Response, 2009), p.11.
[3] A.P. Cackley, *Facial Recognition Technology: Commercial Uses, Privacy Issues, and Applicable Federal Law* (US Government Accountability Office, 2015), p.3.
[4] J. Buolamwini and T. Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (Conference on Fairness, Accountability, and Transparency, New York, NY, 2018), p.2.
[5] Y. Wang and M. Kosinski, "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images" (2018) 114 J. Pers. Soc. Psychol. 246.
[6] Recently, police in India suggested that the roll out of FRT across New Delhi enabled them to identify 3,000 missing children in just four days. See A. Cuthbertson, "Indian Police trace 3,000 Missing Children In Just Four Days Using Facial Recognition Technology" (April 24, 2018), *Independent.co.uk*, *https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missi ng-children-facial-recognition-tech-trace-find-reunite-a8320406.html*; "Chinese man caught by facial recognition at pop concert" (April 13, 2018), *BBC.co.uk*, *http://www.bbc.co.uk/news/world-asia-china-43751276* [Accessed August 7, 2018].
[7] "Three arrested using facial recognition technology during Wales' Six Nations opener" (February 6, 2018), *Walesonline.co.uk*, *https://www.walesonline.co.uk/news/wales-news/three-arrested-using-facial-recognition-14253344* [Accessed August 4, 2018]; V. Dodd, "Met police to use facial recognition software at Notting Hill carnival" (August 5, 2017), *Theguardian.co.uk*, *https://www.theguardian.com/uk-news/2017/aug/05/met-police-facial-recognition-software-notting-hill-carnival* [Accessed August 7, 2018].

limited to the police use of FRT at public gatherings. Additionally, ~~as a matter of path clearing,~~ to maintain the tight focus, the evidential value of FRT surveillance footage and fair trial rights will not be discussed.

Commented [LC1]: Not sure about this – what about just "to maintain focus" ?

Those police forces to have tri~~a~~led FRT claim of course that they are cognisant of human rights concerns, and of the need to ensure that the use of this technology is lawful and proportionate.[8] This article questions this claim. It provides a fuller understanding of how FRT interferes with human rights, with particular emphasis on the right to respect for private life under art.8 European Convention on Human Rights (ECHR). It then considers the extent to which the use of FRT in the context of public surveillance in England and Wales is lawful, and indeed the extent to which the law *should* permit the police to engage in this form of surveillance at public gatherings.

The FRT Surveillance Trials

Three domestic police forces have "tri~~a~~led" FRT to monitor public spaces: Leicestershire Police, South Wales Police (SWP) and the Metropolitan Police Service (MPS). The term "trial" in this context is a catchall term to describe various usages of FRT surveillance, and, as will be explored below, some trials are expansive with no defined end point or proposed measurement of success. Rather than pilots or tests, they seem to form part of an inevitable drive towards wider adoption of this technology. Leicestershire Police was the first force to begin using FRT to police public gatherings in the UK in April 2014, as part of a six-month trial of the 'Neoface' facial recognition system. Most famously, the force used the technology to identify "known offenders" among the 90,000 attendees at the Download festival in June 2015. The watch list comprised custody images held by the force, and images provided by Europol.[9] However, the results of the trial in terms of the accuracy of the technology and outcomes of any identifications remain unpublished.

[8] "Introduction of Facial Recognition into South Wales Police" (South Wales Police, 2018), *https://www.south-wales.police.uk/en/news-room/introduction-of-facial-recognition-into-south-wales-police/* [Accessed August 6, 2018].

[9] P. Gallagher, "Download Festival: Facial recognition technology used at event could be coming to festivals nationwide" (June 12, 2015), *Independent.co.uk*: *https://www.independent.co.uk/news/uk/crime/download-festival-facial-recognition-technology-used-at-event-could-be-coming-to-festivals-10316922.html* [Accessed July 30, 2018].

The MPS first used FRT at the Notting Hill Carnival in 2016, and aims to complete ten trials of its system by the end of 2018.[10] It has a bespoke facial recognition system. The trial in 2016 resulted in no successful identifications, and just one successful identification at the 2017 Notting Hill Carnival; in 2017 the system also misidentified five carnival goers as constituting wanted individuals, who were subject to a brief stop by police as a result of the "false positive" match.[11] These individuals were subject to stops despite the efforts of the MPS to reduce the risk of misidentification by adopting a two-step verification process, whereby any matches are checked by a human operator before being passed to patrolling officers in the vicinity of the monitored public space.[12] The MPS trialled their system for a third time on Remembrance Sunday 2017, again making one positive identification to a person on a watch list. This trial was particularly controversial as the MPS compiled and used a watch list of "fixated individuals", who were identified as having obsessive tendencies towards certain public figures but were not wanted in connection with any specific offence. According to *The Independent*, the MPS's use of the technology in 2018 in Stratford yielded no arrests.[13]

SWP is the national lead on FRT, having received a £2.6 million Government grant to test the technology.[14] SWP deployed Neoface's FRT system at 18 public gatherings between May 2017 and March 2018, and has no set end date for its trial of FRT. Big Brother Watch raised concerns about the accuracy of the technology during these trials, noting that a "staggering 91% of matches—2,451—incorrectly identified innocent members of the public."[15] SWP has defended its continued use of FRT, publishing

[10] Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing* (London, 2018), p.26.
[11] A false positive match occurs where a FRT system mistakenly matches a person passing under a facial recognition camera to an image on the watch list. Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing*, p.26.
[12] Facial identification is most accurate when both algorithms and so called "super-recognisers" (humans who are particularly adept at face identification) work in collaboration: see P. Phillips et al, "Face recognition accuracy of forensic examiners, super-recognizers, and face recognition algorithms" (2018) 115 Proc. Natl. Acad. Sci. USA. 6171. However, there is no legal prerequisite for the MPS to use super-recognisers when crosschecking FRT matches, and this is not common practice: see G. Edmond and N. Wortley, "Interpreting Image Evidence: Facial Mapping, Police Familiars and Super-recognisers in England and Australia" (2016) 3 J.I.C.L. 473.
[13] "Facial recognition trial in London results in zero arrests, Metropolitan Police confirm" (July 3, 2018) *Independent.co.uk*, *https://www.independent.co.uk/news/uk/crime/facial-recognition-police-uk-london-trials-stratford-no-arrests-privacy-human-rights-false-positives-a8429466.html* [Accessed August 1, 2018].
[14] *https://www.gov.uk/government/publications/police-transformation-fund-successful-bids-2016-to-2017* [Accessed August 1, 2018].
[15] Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing*, p.29.

information that 2,297 of these false positives occurred at a single event, the June 2017 Union of European Football Associations (UEFA) Champions League Final, where the technology was being trialled by the SWP for the first time and poor quality images provided by UEFA had been used to populate the watch list.[16] This might explain the high false positive rate at the Champions League Final, which was claimed to be an anomaly, but it raises further questions about the quality of the laws in place regulating the population of watch lists. A closer look at the data published by SWP reveals that, even when the Champions League Final is removed from the dataset, false positive matches still outnumber true positive matches by 154 to 106.

Although FRT is becoming more pervasive in the force areas that have trialled it, we still do not have much published data with which to evaluate its accuracy, and the positive contribution it can make towards the policing objectives. Each trialling police force claims to have made numerous arrests after successful identifications. However, these arrests appear to be far outweighed by the number of false positive matches, presenting a risk that any crime prevention successes will come at the expense of the rights of innocent people who may be subject to stops and other coercive policing measures. In July 2018, Big Brother Watch applied to the High Court for a judicial review of the MPS's use of FRT surveillance. The remaining sections of this analysis explore unsettled questions of principle and practice pertaining to the regulation of FRT surveillance. The aim of this exercise is not to speculate on the prospects of success for any legal challenges to the police use of FRT surveillance in public space, but to consider the extent to which human rights considerations *should* serve as a constraint on the police use of FRT at public gatherings.

Is the use of FRT Surveillance Convention Compliant?

In *Wood*,[17] the Court of Appeal attempted to set out the relevant tests underlying the scope of the powers of the police to subject individuals to overt public surveillance. The claimant, a campaigner against the arms trade who was photographed by the police at a protest outside the Annual General Meeting of a company connected to the arms

[16] "Facial Recognition" (South Wales Police, 2017), *https://www.south-wales.police.uk/en/advice/facial-recognition-technology/* [Accessed August 7, 2018].
[17] *R. (on the application of Wood) v Commissioner of Police of the Metropolis* [2010] 1 W.L.R. 123; [2010] E.M.L.R. 1; [2009] H.R.L.R. 25; [2009] A.C.D. 75.

trade, argued that the taking and retention of these photographs by the police violated his rights under arts 8, 10, 11 and 14 ECHR. The Court of Appeal held that the activities of the police had violated the claimant's art.8 rights, allowing the claimant's appeal. The Court dealt with the latter three articles briefly. On the rights to freedom of expression and freedom of assembly under arts 10 and 11, and without elaborating much on his reasoning, Laws LJ observed that it was "fanciful to suppose that in the events which happened there was any interference with the claimant's rights under arts 10 and 11."[18] Laws LJ further held that there was no discrimination contrary to art.14 as "the police had good reason, arising from their perception of events which was itself reasonable, to photograph the claimant."[19] The Court gave short shrift to any notion that these articles might be engaged through the surveillance, notwithstanding the claimant's assertions that this surveillance had a corrosive and chilling effect on his future involvement in political activism.

Turning to art.8, ~~T~~this case set out some of the main features of the domestic courts' approach to interpreting the scope of the human rights protection to be afforded to those subject to overt police surveillance in public spaces. It provides us with a useful reference point for assessing the extent to which the police's use of FRT surveillance is compatible with their obligations to respect fundamental human rights.

The majority held that held that the activities of the police constituted an interference with the claimant's art.8 rights, but that this interference was not "necessary in a democratic society" under art.8(2).[20] The majority expressed no conclusive view on whether the measures were "in accordance with the law" for the purposes of art.8(2). However, the majority held that the surveillance measures were disproportionate. In forming this conclusion, Dyson LJ emphasised that the police targeted the claimant in circumstances where he "had not been ejected from the meeting and … was not guilty of any misconduct" upon leaving.[21]

Commented [do2]: A couple of sentences summarizing the majority might help. It is odd to leap into the dissent

Commented [LC3]: This seems fine to me!

Commented [do4]: So how has Laws dissented – dissented from not holding because he has a firm view? I think this could be clearer

Commented [LC5]: I'll defer to you here, Joe

[18] *Wood* [2010] 1 WLR 123, 150.
[19] *Wood* [2010] 1 WLR 123, 150.
[20] *Wood* [2010] 1 WLR 123, 150.
[21] *Wood* [2010] 1 WLR 123, 152.

Laws LJ dissented~~,~~ holding that, whilst the surveillance activities of the police interfered with the claimant's art.8(1) rights, ~~on the point of whether~~ the interference was justified under art.8(2)~~, observing that it was~~. ~~However,~~ Laws LJ's dissent provided a considered breakdown of the tests that need to be applied to determine whether there has been an interference with art.8(1).

Laws LJ first described personal autonomy as the central value protected by art.8(1).[22] However, Laws LJ warned that there exist three safeguards for ensuring that the core values protected by art.8 are not interpreted so widely that its claims become unreal or unreasonable.[23] These are as follows: 1) a measure threatening or assaulting the individual's right must attain a "certain level of seriousness" for art.8 to be engaged; 2) the "touchstone" for art.8(1)'s engagement is whether the claimant enjoys on the facts a "reasonable expectation of privacy"; and 3) the breadth of art.8(1) may be curtailed by the scope of the justifications available to the state pursuant to art.8(2).[24]

In finding that there was in fact an interference with art.8(1), Laws LJ characterised the activities of the police in taking and retaining photographs as part of a surveillance operation as "a good deal more than the snapping of a shutter", as they involved the storing and processing of personal information, and were targeted specifically towards the claimant.[25] Dyson LJ, in the majority, agreed.

However, on the art.8(2) point, Laws LJ departed from the majority's position, observing that, as the taking of the claimant's image was not done in an aggressive manner, and the retention of his image was "tightly controlled", the activities of the police were proportionate and "necessary in a democratic society". ~~Dyson LJ determined that the activities of the police were disproportionate and in violation of~~

Commented [JP6]: In answer to your question, David, Laws LJ formed his own view on legality (which isn't really important for our analysis, so I've left it out), and dissented on the proportionality issue. Hopefully this is now clear.

[22] *Wood* [2010] 1 WLR 123, 135 at [21].
[23] *Wood* [2010] 1 WLR 123, 135.
[24] *Wood* [2010] 1 WLR 123, 135.
[25] *Wood* [2010] 1 WLR 123 at [45].

What rights are engaged by FRT surveillance?

At first glance, *Wood* might look like a victory for those concerned in the protection of the human rights of individuals subject to overt police surveillance. However, Laws LJ's pivotal interpretation of the scope of the human rights protection for those subject to public surveillance is unduly narrow. In elevating the "reasonable expectation of privacy" standard to a touchstone test of art.8 engagement, Laws LJ significantly restricted the availability of the art.8 protection for those subject to surveillance as they traverse public space. As has been discussed extensively in academic commentary,[28] the elevation of this test in English law—which has since been affirmed as the correct approach by the Supreme Court[29]—diverts focus away from whether or not the police use of chilling and intrusive surveillance measures is lawful and proportionate.

This interpretation of the scope of art.8(1) is also out of step with more recent European Court of Human Rights (ECtHR) case law, where the Strasbourg Court has found that art.8 is engaged without entering into a detailed analysis of whether the applicant held a reasonable expectation of privacy in the circumstances ~~mention of the reasonable expectation standard~~.[30] Rather, when developing the normative content of the right to respect for private life, the ECtHR's key focus has been on the degree to which a particular measure sets back the privacy related interests of the applicant.[31] Where the ECtHR does mention an applicant's reasonable expectations of privacy (or lack thereof) as part of its art.8(1) inquiry, it seems to ~~simply~~ declare simply that such expectations exist rather than use the reasonable expectation test as an empirically verifiable standard of art.8 engagement. The existence of a reasonable expectation of privacy is certainly not a mandatory precondition for art.8 engagement in the jurisprudence of the ECtHR.[32] Indeed, in *Barbulescu,* the ECtHR left open the question of whether the applicant held a reasonable expectation of privacy where his employer surreptitiously monitored his personal communications on a device which the employer had provided to him, but held that the applicant's art.8 rights were nonetheless engaged owing to the intrusive nature of the employer's activity.[33]

Even on Laws LJ's interpretation of the scope of art.8(1), however, the police use of FRT surveillance might interfere with art.8. Like the activities of the police in *Wood,*

Commented [do7]: So how has Laws dissented – dissented from not holding because he has a firm view? I think this could be clearer

Commented [LC8]: I'll defer to you here, Joe

FRT surveillance involves more than the "snapping of a shutter". When finding an interference in *Wood*, the Court of Appeal noted that photography by a state authority as part of a surveillance operation would have a "chilling effect" on an individual's activities in public space.[34] The Court also drew support for this view from *S and Marper*, where the ECtHR determined that "the mere storing of data relating to the private life of the individual amounts to an interference within the meaning of Article 8."[35]

Though there are contextual differences to note between the activities of the police in *Wood* and the FRT surveillance trials, the Court's findings in *Wood*, with regard to the chilling effect of overt police surveillance and the processing of personal information seem to support the notion that public FRT surveillance interferes with art.8. After all, this technology does collect personally identifiable information from each individual to pass under its gaze and momentarily compares this with other personal information data held on police records. This is to subject the individual to much more than a passing glance.

There is good reason for suggesting that individuals *should* be afforded the protection of art.8 when they are subject to FRT surveillance as they go about their business in public. Modern privacy scholarship generally acknowledges that individuals can retain an interest in privacy as they occupy public space.[36] Larsen suggested that public CCTV moves the goalposts insofar as privacy in public is concerned, as it allows authorities to subject the individual to quite intensive scrutiny, breaking traditional boundaries and social conventions regarding the extent to which individuals would usually be subject to scrutiny when traversing public space.[37]

[34] *Wood* [2010] 1 WLR 123 at [45] and [92] per Lord Collins.
[35] *S and Marper v United Kingdom* (2009) 48 E.H.R.R. 50; [2009] Crim. L.R. 355 at [67]. This interpretation has been embraced by the Supreme Court, where Lord Sumption ruled that the state's systematic collection and storage in retrievable form even of public information about an individual is an interference with private life. See *R. (on the application of Catt) v Commissioner of Police of the Metropolis* [2015] UKSC 9; [2015] A.C. 1065; [2015] 2 W.L.R. 664; [2015] H.R.L.R. 4 at [5].
[36] This is also a point that has been accepted by the ECtHR in *Amann v Switzerland* (2000) 30 E.H.R.R. 843 at [61], and, indeed, domestic courts: *Campbell v MGN Ltd* [2004] 2 A.C. 457; [2004] 2 W.L.R. 1232; [2004] E.M.L.R. 15; [2004] H.R.L.R. 24.
[37] B. vS-T. Larsen, *Setting the Watch: Privacy and the Ethics of CCTV Surveillance* (Oxford: Hart Publishing, 2011), pp.41-55.

FRT surveillance compounds the intrusive capacity of CCTV surveillance. Personally identifiable information is collected from the individual (namely, details of his or her facial geometry), and aggregated with other personally identifiable information (the image database) to create new information about the individual (that he or she is or is not a person of interest to the authorities). Thus, the technology allows the police to go further in transgressing social norms governing the flow of information about individuals as they occupy public space.

Brey suggests that the processing of the biometric features of the one's face in this way may violate an individual's legitimately held privacy rights. Firstly, this is because the process of functionally reducing one's face, which is a highly personal aspect of an individual's uniqueness, to an information structure is dehumanising; and, secondly, "this process of functional reduction involves the creation of informational equivalents of body parts that exist outside their owner and are used and controlled by others."[38] For Brey, through this process the individual loses full ownership of the geometric features of his or her face as these features acquire new meanings that the individual does not understand, and new uses realised outside of his or her own body.[39]

Any data protection concerns of the citizen may be mitigated by the fact that the police delete processed images 30 days after their collection (provided a positive or false positive match is not made). It is unclear if speculative searches are run in this period, and how to guarantee that the images and algorithms are in fact deleted at the end of the timeframe. However, the shift in the balance of power between the state and the individual occupying public space is normatively significant in yet another way. As Cohen suggests, the mere presence of a public surveillance tool with such intrusive capabilities as FRT can threaten privacy interests by moderating behaviour:

> "The experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behaviour. Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream. The result will be a subtle yet fundamental shift in the content of our character, a blunting and blurring of rough edges and sharp lines. But rough edges and sharp lines have intrinsic, archetypal value within our culture. Their philosophical differences aside, the coolly rational Enlightenment thinker, the unconventional Romantic dissenter, the skeptical pragmatist, and the iconoclastic postmodernist all share a deep-rooted

[38] P. Brey, "Ethical Aspects of Facial Recognition Systems in Public Places" (2004) 2 J.I.C.E.S. 97, 107.
[39] Brey, "Ethical Aspects of Facial Recognition Systems in Public Places" (2004) 2 J.I.C.E.S. 97, 107.

> antipathy toward unreflective conformism. The condition of no-privacy threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it."[40]

Cohen articulates how such monitoring can have a corrosive impact on personal autonomy. Where the police, as a state authority, u~~tili~~se technology to transcend social norms of acceptable observation and scrutiny in public it is not difficult to see how this might have a moderating effect on behaviour. As Benn puts it, sustained observation of an individual can be objectifying: "Finding oneself an object of scrutiny, as the focus of another's attention, brings one to a new consciousness of oneself, as something seen through another's eyes."[41] When "the other" is the state, such practices can be coercive. In short, the police use of FRT surveillance to monitor public spaces can be distinguished not only from being subject to the fleeting observations one might be subject to by a stranger in public space, but also from prolonged surveillance by police personnel, and the use of CCTV surveillance, which cannot limit the personal autonomy of the individual to the same extent. It is submitted that police FRT surveillance in public spaces has at least the potential to engage the art.8 rights of any member of the public to whom it is applied. Even if, contrary to the analysis above, individuals cannot be said to have a *reasonable expectation* that they ~~will not be subject~~be free from ~~to~~ FRT surveillance as they traverse public space, the balance of privacy scholarship and ECtHR jurisprudence suggests that—both legally and morally—the state should justify its ~~Thus FRT~~ deployments ~~must satisfy~~of FRT in compliance with ~~the criteria in~~ art.8(2).

The police use of FRT raises broader principled concerns than the impact that it will have on an individual's privacy. Cohen's observations about the moderating effect that public surveillance can have on behaviour hint at another drawback of the police use of FRT surveillance: this invasion of privacy may have a "chilling effect" on public assemblies, freedom of expression, and the general use of public space, by certain communities and demographics in particular. Drawing on empirical research, Aston develops this argument in the context of political protest movements, suggesting that

[40] J.E. Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 Stan. L. Rev. 1373, 1425-1426.
[41] S. Benn, "Privacy, Freedom, and Respect for Persons" in J. Pennock and J. Chapman (eds), *Privacy: Nomos XIII* (New York: Atherton Press, 1971), p.7.

overt surveillance can damage legitimate political mobilisations in public space by undermining the perceived legitimacy of protest groups and limiting their access to resources.[42] These findings, which are supported by empirical research from the United States,[43] suggest that the presence of visible surveillance at meetings and other political gatherings will reduce perceptions of legitimacy, and harm the efforts of such groups to be taken seriously and attract support from their target audiences.[44] The reputational hit that political groups may take when they are subject to surveillance can also have a knock-on effect on resources and networks.[45]

FRT surveillance has the potential to threaten an individual's right to be free from discrimination in two separate ways. The first is dependent on who the police choose to target using FRT surveillance. As we have seen, when FRT surveillance is deployed at public gatherings, faces in the crowd are checked against a watch list. One problem with public FRT surveillance is the lack of transparency regarding the selection process for images to go onto a watch list. This led to criticisms that the police are unjustifiably discriminating in their use of FRT surveillance when it was reported that the MPS used FRT at Remembrance Sunday in 2017 to identify and eject individuals based on criteria related to their mental ill health.[46]

Secondly, FRT might, through its relative inaccuracy as applied to different demographic groups, lead to members of some groups being misidentified and subject to coercive policing measures. One of the purported advantages of FRT surveillance is that it can bring objectivity to the exercise of identifying suspects or "persons of interest" in real time. Unlike the human eye, the software "does not see race, sex, orientation or age."[47] However, this truism masks the danger that this technology can reflect, produce and maintain biases in policing outcomes. In particular, the limited

[42] V. Aston, "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protestor perspectives" (2017) 8 E.J.L.T. 1, 10.
[43] A. Starr, L.A. Fernandez, R. Amster, L.J. Wood, and M.J. Caro, "Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis" (2008) 31 Qual. Sociol. 251, 261.
[44] Aston, "State surveillance of protest and the rights to privacy and freedom of assembly: a comparison of judicial and protestor perspectives" (2017) 8 E.J.L.T. 1, 10.
[45] Starr, Fernandez, Amster, Wood, and Caro, "Impacts of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis" (2008) 31 Qual. Sociol. 251, 258-259.
[46] Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing*, p.15.
[47] See C. Garvie, A. Bedoya, and J. Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America" (Georgetown Law, Center on Privacy & Technology, 2016), p.57.

independent testing and research into FRT technology indicates that numerous FRT systems misidentify ethnic minorities and women at higher rates than the rest of the population.[48]

Despite calls for rigorous testing on the performance of FRT systems from the scientific community,[49] the police have not even ~~recorded~~ published how the technology has performed relative to the gender, ethnicity or age of those subject to its use.[50] This risk of over-policing minority groups can be set in a context where black people are arrested at a rate three times higher than white people.[51] There appears to be a credible risk that FRT technology will undermine the legitimacy of the police in the eyes of already over-policed groups. This is not merely because the technology itself is more likely to wrongly identify those with darker skin, but also because—assuming custody images are to be routinely used to populate FRT databases—those with darker skin are likely to be disproportionately enrolled onto the comparator database. This will increase the probability that members of the public from black or other minority ethnic backgrounds will be mistakenly identified as "persons of interest" relative to their white counterparts. As David Lammy noted in his recent review into the treatment of black and minority ethnic individuals in the criminal justice system: "Grievances over policing tactics, particularly the disproportionate use of Stop and Search, drain trust in the CJS in BAME communities".[52]

In *Wood,* and then again in *Catt,* the domestic courts did not consider the broader human rights ramifications of overt surveillance for the individual and society.[53] This is hardly

Commented [do9]: Or is it not published findings?

Commented [LC10]: Fair question – I don't think gender etc is recorded, but can't find a source

Commented [JP11]: Admittedly, the source only refers to ethnicity figures. According to BBW, the Met confirmed that these have not been recorded. I've seen no published demographic breakdown of police FRT matches, so perhaps its safest to just sub 'recorded' for 'published'.

[48] These disparities of performance across different demographic groups are believed to be attributable to the way FRT algorithms are "trained", and the inherent difficulties in accurately recognising the facial features of some demographic groups. See B.F. Klare, M.J. Burge, J.C. Klontz, R.W. Vorder Bruegge, and A.K. Jain, "Face Recognition Performance: Role of demographic information" (2012) 7 T.I.F.S. 1789, 1797; Buolamwini and Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018), p.12.
[49] Buolamwini and Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018), pp.11-12.
[50] Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing,* p.17.
[51] Home Office, *Arrest statistics data tables: police powers and procedures year ending 31 March 2017* (London: OGL, 2017).
[52] The Lammy Review, *An independent review into the treatment of, and outcomes for, Black, Asian and Minority Ethnic individuals in the Criminal Justice System* (2017), p.17.
[53] *Wood* [2010] 1 WLR 123, 150; *Catt* [2015] UKSC 9 at [26]-[27].

surprising given the *Ullah* principle[54] and the fact that the ECtHR has been reluctant to consider whether overt surveillance activities have struck at the essence of arts 10 and 11.[55] Instead, when discerning the scope of these rights, Strasbourg and domestic courts tend to focus on more direct forms of restriction by a public authority[56] than on the broader, residual effects of surveillance measures. Neither domestic courts nor the ECtHR would be likely to indulge in an exhaustive analysis of the potential applicability of art.14 to those subject to FRT surveillance. Due to its relative inaccuracy, the technology may well fall within the scope of art.14 as a form of indirect discrimination, as it has a disproportionately adverse effect on certain demographic groups.[57] However, as was noted in the *'Belgian Linguistic' case (No 2),* art.14 "has no independent existence in the sense that under the terms of art.14 it relates solely to 'rights and freedoms set forth in the Convention'".[58] Art.14 plays a subordinate role: it is only applicable in circumstances that fall within the "ambit" of another Convention right.

As Goodwin has noted, the ECtHR's approach to non-discrimination issues has beenis hesitant: "the Strasbourg Court has continually placed itself and its jurisprudence behind developments in non-discrimination law at the Member State, international and European Community level."[59] It is often the case that when the principal Convention right is invoked almost any difference in treatment can be dealt with in that context, making an analysis of art.14 superfluous.[60] In *S and Marper*, the Strasbourg Court took this approach. In finding a violation of the applicants' art.8 rights, the ECtHR seemed, in its articulated reasoning, to attribute some weight to the suggestion from the applicants that the retention policies "led to the over-representation in the database of

[54] "The duty of national courts is to keep pace with the Strasbourg jurisprudence as it evolves over time: no more, but certainly no less." *R. (on the application of Ullah) v Special Adjudicator* [2004] UKHL 26; [2004] 2 A.C. 323; [2004] 3 W.L.R. 23; [2004] H.R.L.R. 33; [2004] I.N.L.R. 381 at [20].
[55] In *Shimovolos*, where the ECtHR did not consider the corrosive impact that data retention might have on the applicant's art.11 rights, notwithstanding that the surveillance was directly related to his participation in a political rally. See *Shimovolos v Russia* (2014) 58 E.H.R.R. 26; 31 B.H.R.C. 506.
[56] Such as the criminalisation for certain forms of expression and assembly (*Müller v Switzerland* (1988) 13 E.H.R.R. 212 at [28]; *Ezelin v France* (1991) 14 E.H.R.R. 362 at [37]); and the exertion of pressure to compel someone to join an association contrary to his or her convictions (*Young, James and Webster v United Kingdom* (1981) 4 E.H.R.R. 38 at [57]).
[57] See *DH v Czech Republic* (2008) 47 E.H.R.R. 3.
[58] *'Belgian Linguistic' case (No 2)* (1968) 1 E.H.R.R. 252 at [9].
[59] M.E.A. Goodwin, "Taking on Racial Segregation: The European Court of Human Rights at a *Brown v. Board of Education* moment?" (2009) 170 *Rechtsgeleerd Magazijn Themis* 93, 94.
[60] J. Gerards, "The Discrimination Grounds of Article 14 of the European Convention on Human Rights" [2013] 13 H.R.L. Rev. 99, 100.

young persons and ethnic minorities, who have not been convicted of any crime."[61] In light of this reasoning, the ECtHR considered that it was not necessary to examine separately the applicants' complaint that the DNA and fingerprint retention policies, which disproportionately affected young persons and ethnic minorities, violated art.14.[62]

This exercise of considering under the art.8 heading broader human rights considerations than would typically fall under the scope of art.8~~, under the art.8 heading~~ does little to advance legal certainty. However, a full discussion of whether or not it would be principled or practically sustainable to broaden the scope of arts 10, 11 and 14 to include protection from the use of surveillance measures, which might chill their exercise, falls beyond the scope of this analysis. This does not mean that the chilling or discriminatory effects of FRT surveillance are irrelevant when assessing its impact from a fundamental human rights perspective. At the least, any such effects conceivably serve to exacerbate the art.8 interference arising from FRT surveillance.

Is FRT surveillance "in accordance with the law"?

One criticism of the FRT trials is that they have been operating in a legal vacuum. FRT is said to have no legal basis regulating its proper operational limits.[63] The Home Office has responded to such concerns, claiming that three legal regimes have regulated the trials: the Data Protection Act 2018; the Surveillance Camera Code of Practice; and, relevant human rights principles. However, none of these regimes provide guidelines or rules *specifically* regulating the police use of FRT. Moreover, in its recent Biometrics Strategy, the Home Office acknowledged that the governance and oversight of FRT surveillance could be "strengthened further".[64] It seems that the question of whether this legal basis meets the Convention's legality requirements would be a particular flashpoint in any judicial review of FRT surveillance.

[61] *S and Marper* (2009) 48 E.H.R.R. 50 at [124].
[62] *S and Marper* (2009) 48 E.H.R.R. 50 at [129].
[63] Big Brother Watch, *Face Off: The lawless growth of facial recognition in UK policing*, p.3.
[64] Home Office, *Biometrics Strategy: Better public services, maintaining public trust* (London: OGL, 2018) 12.

In *Catt*,[65] Lord Sumption summarised relevant ECtHR principles concerning what is required of the "in accordance with the law" requirement for Convention compliance. In different circumstances the two applicants had personal information about their activities noted down and retained by the police as they occupied publicly accessible space. The Supreme Court ruled that whilst the retention practices in each case engaged art.8(1), they satisfied the criteria in art.8(2) (with Lord Toulson dissenting on this point in the case of the first applicant). Lord Sumption concluded that the measures were "in accordance with the law", observing that the exercise of common law powers to collect and store information is subject to an "intensive regime of statutory and administrative regulation" under the Data Protection Act 1998, and various guidance documents on the management of police information.[66]

Lord Sumption drew support for this conclusion from *MM*[67] and *T,*[68] which concerned the disclosure of criminal records information to potential employers. In each case, it was held that the storage of criminal record information cannot be "in accordance with the law" if the provisions for the storage had no clear scope; contained no safeguards against abuse or arbitrary treatment of individuals; or if the provisions lacked minimum safeguards governing the storage, usage, procedures for preserving integrity, and confidentiality of data.[69]

Lord Sumption observed that the application of rules regulating the use of an interfering measure should be reasonably predictable:

> "The rules need not be statutory, provided that they operate within a framework of law and that there are effective means of enforcing them. Their application, including the manner in which any discretion will be exercised, should be reasonably predictable, if necessary with the assistance of expert advice. But except perhaps in the simplest cases, this does not mean that the law has to codify the answers to every possible issue which may arise. It is enough that it lays down principles which are capable of being predictably applied to any situation."[70]

---

[65] *Catt* [2015] UKSC 9.
[66] Lord Sumption cited principles 1, 2, 3, 5, and 7 listed in Schedule 1 of the Data Protection Act 1998 along with the *Guidance on the Management of Police Information* (2010), which is superseded by a 2014 edition.
[67] *MM v United Kingdom* [2013] April 29, 2013.
[68] *R. (on the application of T) v Chief Constable of Greater Manchester Police* [2014] UKSC 35; [2015] A.C. 49; [2014] 3 W.L.R. 96; [2014] 4 All E.R. 159; [2014] 2 Cr. App. R. 24.
[69] *MM* [2013] April 29, 2013 at [195].
[70] *Catt* [2015] UKSC 9 at [11].

Lord Sumption paid close attention to how the activities of the police accorded with the 1998 Act, and how these provisions met the demands of art.8 more generally, concluding that English law's combination of these elements met the requirements of the legality test under art.8.[71] Police FRT surveillance then, like the retention practices at issue in *Catt,* should accord with current data protection regulations. Following the enactment of the 2018 Act, this means that a trialling police force should follow the Data Protection Principles to ensure that data cannot be obtained, retained or used by the police unless it is necessary for them to do so for a law enforcement purpose (i.e. to prevent, detect, investigate, or prosecute criminal offences).[72] Additionally, as FRT involves the systematic monitoring of public spaces on a large scale, and the processing of biometric data, the police should undertake a Data Protection Impact Assessment (DPIA) before undertaking this form of information processing. DPIAs must describe the nature, scope, and purpose of the processing, but there is no requirement upon a police force to publish their DPIA.[73] The original PIA for the MPS trial was reviewed by the Information Commissioner's Office.[74] The Code of Practice on the Management of Police Information provides guidance to ensure consistent procedures throughout the police service for obtaining, storing and sharing personal information.[75]

Any use of FRT surveillance must also be considered against the Surveillance Camera Code of Practice, to which police must have regard under Protection of Freedoms Act 2012 s.33. This Code of Practice contains 12 guiding principles, which require surveillance camera system operators to ensure that their use of a camera system has a legitimate purpose. Operators must put in place safeguards to ensure that such systems are used transparently, and that information is only collected, processed or retained in so far as this is necessary for the legitimate purpose.[76]

It is not clear that this piecemeal regulatory framework would satisfy the foreseeability and accessibility requirements in art.8(2). Whilst the general principles governing the

[71] *Catt* [2015] UKSC 9 at [12].
[72] Data Protection Act 2018 s.31
[73] Information Commissioner's Office, *Data protection impact assessments* (London: OGL, 2018).
[74] *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/731641/BFEG_minutes_-_05_June_2018.pdf* [Accessed September 21, 2018], para.2.6.
[75] Home Office, Code of Practice on the Management of Police Information (NCPE, 2014), p.8.
[76] Home Office, *Surveillance Camera Code of Practice* (London: The Stationary Office, 2013), pp.10-11.

use of surveillance camera systems and the protection of personal data are accessible to the public, they do not seem to pass the test set out by Lord Sumption in *Catt*: they are not capable of being predictably applied to the use of the interfering measure. That is to say that, whilst the domestic legal framework, which covers surveillance camera systems and data protection generally, does require the police to consider points that are relevant to the regulation of FRT surveillance, it is doubtful that this framework sets out a clear scope specifically for the use of FRT surveillance. This is because none of these regulatory mechanisms seem to have been drafted with the police's current or future use of FRT surveillance in mind.

Consequently, the regulatory framework gives little indication or guidance as to the proper threshold at which inclusion on a watch list is lawful.[77] Practices between trialling police forces have diverged, and the Information Commissioner has expressed concern about the absence of national-level coordination and a comprehensive governance framework to oversee FRT deployment.[78] Most images used to populate watch lists are gathered from custody image databases. Though forces trialling public FRT surveillance have been keen to emphasise that these databases are populated with images that they are legally entitled to collect or retain, they have the discretion to include as many images on the watch list as they see fit. For example, in their trial of FRT surveillance, SWP have included not only the images of wanted suspects and missing persons, but also other "persons of interest"—a conspicuously indefinite phrase.[79] There is also no legal prohibition on police forces taking images from the internet or public facing social media accounts for this purpose.

There is a particular risk, here, that people with old and minor convictions, or even those with no convictions at all, may find themselves stigmatised through the deployment of FRT surveillance, which targets them. This risk is compounded by the lack of effective safeguards governing the collection and continued retention of custody images taken from people who come into contact with the police, but are not

[77] London Policing Ethics Panel, *Interim Report on Live Facial Recognition* (2018), p.14
[78] E. Denham, "facial recognition technology and law enforcement" (Information Commissioner's Office, May 14, 2018), *Ico.org.uk*, *https://ico.org.uk/about-the-ico/news-and-events/blog-facial-recognition-technology-and-law-enforcement/*.
[79] "Introduction of Facial Recognition into South Wales Police" (South Wales Police, 2018), *https://www.south-wales.police.uk/en/news-room/introduction-of-facial-recognition-into-south-wales-police/* [Accessed August 6, 2018].

subsequently convicted of an offence. In *RMC*,[80] the High Court ruled that the legal framework regulating the retention of custody images taken from such non-convicted persons under the Police and Criminal Evidence Act 1984 s.64 was not compatible with art.8 ECHR. The Science and Technology Committee recently expressed concerns that a Home Office review[81] of the framework—which recommended that such images only be considered for deletion upon request (and not subject to any automatic deletion)—did not seem to go far enough to satisfy the requirements of art.8.[82]

Added to this, as discussed above, forces have used other images provided by third parties such as Europol and UEFA. The SWP admitted that the low quality of some such images resulted in a high rate of false positives at the 2017 Champions League Final. This raises the question: what constitutes an acceptable standard of image quality for a police facial recognition system? The regulatory framework, as currently formulated, provides no answer.

Is FRT surveillance "in pursuit of a legitimate aim" and "necessary in a democratic society"?

FRT surveillance conducted in accordance with the new DPA 2018 principles will be done "in pursuit of a legitimate aim" for the purposes of art.8(2). Police FRT surveillance, which pursues a "law enforcement purpose" under the DPA 2018, is, if not by default then to a virtual certainty, for the "prevention of disorder or crime" or "in the interests of public safety" for art.8(2) purposes. For an interference to satisfy the final criterion in art.8(2) it must be "necessary in a democratic society", meaning the interfering measure must respond to a "pressing social need" and be "proportionate to the legitimate aim pursued".[83] Ultimately, the final limb requires a consideration of whether the degree of the interference with the rights of those subject to FRT surveillance is greater than justifiable in achieving the aims of the trialling police forces. Put another way, when the detrimental impact of carrying out FRT surveillance is

Commented [do12]: Not very clear sentence

Commented [LC13]: What about:

Police FRT surveillance with a "law enforcement purpose" under the DPA 2018 can be regarded/deemed to be pursued for the "prevention of disorder or crime" or "in the interests of public safety" under art.8(2).

[80] *R. (on the application of RMC and FJ) v Commissioner of Police of the Metropolis* [2012] 1 W.L.R. 3007; [2012] H.R.L.R. 26; [2012] A.C.D. 103 at [55].
[81] Home Office, *Review of the Use and retention of Custody Images* (London: OGL, 2017).
[82] "Police unlawfully retaining custody images, claims Norman Lamb" (February 6, 2018), *BBC.co.uk*, *http://www.bbc.co.uk/news/uk-politics-42961025*; House of Commons. Select Committee on Science and Technology, *Biometrics strategy and forensic services*: Fifth Report of Session 2017-19 (The Stationary Office, 2018) HC Paper No.800, pp.18-19.
[83] *Olsson v Sweden* (1989) 11 E.H.R.R. 259 at [67].

weighed against the crime prevention and public safety benefits that are accrued from carrying it out, is there a net gain in favour of using FRT surveillance?

As we have established above, FRT surveillance in public gatherings has the potential to set back privacy related interests to a significant degree. This surveillance subjects members of the public to uninvited scrutiny and has the potential to chill the exercise of other fundamental human rights. It constitutes a serious interference with art.8(1) compared to other forms of overt surveillance. One problem with the recent FRT trials is that it is not easy to discern their purpose. SWP have suggested that their trials enabled them to validate the technology and build confidence amongst their officers in using the technology.[84] Running trials of the technology with simulated natural conditions could, at least partially, enhance these objectives. Similarly, the London Policing Ethics Panel criticised the MPS for citing the need to test the technology in natural conditions as a reason for undertaking their trials:

> "If the argument is that [FRT] must be tested in natural conditions, a better justification for trial~~l~~ing it on the public at large would have been that all options for testing and refining it in simulated natural conditions had been exhausted. The MPS has not presented this claim to the public."[85]

Where the police are trial~~l~~ing the technology on the general public in live policing operations as a means of testing whether the technology works, without exhausting less intrusive options for testing the technology in a simulated environment, this use does not respond to a "pressing social need".

Another aim of the trials has been to use the technology ~~to~~ effectively to prevent crime and ensure public safety. In *Bank Mellat*, Lord Reed explained that the proportionality test requires a public authority to show that the legitimate aims of the legislature are logically furthered by the means it has chosen to adopt.[86] Thus, to justify any continued use of FRT surveillance, the trials should enable the police to successfully gauge that this surveillance can contribute to its crime prevention objectives.

Commented [do14]: Repetitive

Commented [LC15]: Happy to omit

[84] "Facial Recognition" (South Wales Police, 2017), *https://www.south-wales.police.uk/en/advice/facial-recognition-technology/* [Accessed August 7, 2018].
[85] London Policing Ethics Panel, *Interim Report on Live Facial Recognition* (2018), p.9.
[86] *Bank Mellat v HM Treasury (No. 2)* [2013] UKSC 39 at [92]; [2014] A.C. 700; [2013] 3 W.L.R. 179; [2013] H.R.L.R. 30.

Success is not easy to measure in this context, particularly when relying on the limited statistical information about the trials that has been made publicly available. A low number of positive matches, which taken at face value might indicate that the technology is not very useful, could in fact represent an indication of success as the technology is effectively deterring those who might pose a threat to the public from attending gatherings where FRT surveillance is known to be in use. Notwithstanding this difficulty, both the SWP and MPS have defended, and appear committed to, their use of FRT surveillance. The former force suggested that the technology has led to numerous arrests and helped the force identify vulnerable people at times of crisis.[87] From the limited statistical data that has been published by the police, it is at least plausible to suggest that the use of FRT surveillance can make some contribution to crime control. The police have, after all, successfully identified people who are wanted in connection with criminal offences using FRT surveillance. However, in the face of the weighty impact that FRT surveillance will have on fundamental human rights, including the privacy interests people maintain as they occupy public space, the published results of the trials undertaken so far are insufficiently detailed to support the argument that its current use has been proportionate. They also raise troubling questions about the accuracy of the technology and its potential to undermine police legitimacy.

Even *if* the technology is accurate enough to produce significant crime prevention benefits, there is good reason for restricting the use of FRT surveillance in public spaces. The preceding analysis suggests that any regulatory framework for the police use of overt FRT surveillance in public space should proceed on the basis that this surveillance interferes with the fundamental human rights of all who are subject to it, and that such interferences must be strictly necessary in response to a strong crime prevention or public safety based justification. This necessity principle suggests that a selective approach to the use of FRT surveillance in public space is required. Rather than gradually becoming a pervasive and chilling feature of public life, FRT surveillance should only be used in response to documented, credible and serious threats to public safety.

[87] "Police defend facial recognition technology that wrongly identified 2,000 people as potential criminals" (The Telegraph, May 5, 2018), *Telegraph.co.uk*, *https://www.telegraph.co.uk/news/2018/05/05/police-defend-facial-recognition-technology-wrongly-identified/* [Accessed July 15, 2018].

Without the enactment of statutory rules governing the deployment of FRT surveillance, assessments of proportionality will remain in the hands of individual police forces. Parliament should set out rules governing the scope of the powers of the police to deploy FRT surveillance in public space to ensure consistency across police forces. The regulatory framework, as it is currently formulated, is insufficiently calibrated, permitting the trialling police forces to come up with divergent, and sometimes troubling, policies and practices for the execution of their FRT operations. The unique human rights based challenges posed by FRT surveillance require specific rules governing the scope of the powers of the police to use FRT surveillance, including minimum safeguards governing the composition of watch lists; the collection, processing and storage of personal information in this context; and the quality requirements of FRT systems and images for watch lists.

We propose that particular care should be taken with the population of watch lists. Inclusion on a watch list involves further processing of personal information and, of course, the potential for additional risk of stigmatisation following a positive match. As a baseline standard, watch list inclusion should be reserved only for those individuals who are *either*:

1) wanted in connection with a criminal offence; *or*
2) otherwise reasonably believed to pose a serious risk to public safety (including the individual's own safety); *and*
3) in addition to 1 or 2, reasonably likely to be in the vicinity of the public space being monitored by FRT surveillance.

Any regulatory framework should also ensure transparency and accountability in the police use of overt FRT surveillance by requiring any initiating police force to publicise its use of the surveillance during operations, and periodically publish information pertaining to the performance of the technology, including numbers of false positive matches and interventions based on false positive matches.

Conclusion

The use of FRT surveillance is on the rise without sufficient reflection on its aims, and consequences. The ways in which FRT surveillance has the potential to interfere with

citizens' privacy related rights are multifaceted and complex, and without a full understanding of this potential, we cannot hope to adequately regulate this form of policing technology. This paper has considered the impact of FRT surveillance from a fundamental human rights perspective, and has shown that the legal framework regulating these trials is piecemeal and fails to provide satisfactory rules and minimum safeguards governing the police use of FRT in public spaces. The extent to which police FRT surveillance can make a useful contribution to crime prevention and public safety objectives in England and Wales has yet to be ascertained. Like all surveillance technologies, it has the capacity to improve state oversight of individuals and populations, and like many other technologies, the drive for its wider use seems ineluctable, despite questionable reliability and inadequate reflection on its purposes. Aside from any crime control potential, and as this paper has demonstrated, human rights considerations should serve as a significant constraint on police FRT surveillance in public spaces.