12

Does Big Brother Exist?

Facial Recognition Technology in the United Kingdom

Giulia Gentile

12.1 INTRODUCTION

Facial recognition technology (FRT) functions by analysing key facial features to generate a mathematical representation of them, and then comparing these against the mathematical representation of known faces in a database to determine possible matches. This is based on digital images (still or from live camera feeds). In a policing context, FRT is used to help verify the identities of persons 'of interest' to police. State-operated surveillance involving FRT is hardly a novel phenomenon in the United Kingdom (UK). The UK has been the crib of the use of FRT. A technology that initially was used by public entities, it is now widespread also in the private sector.[1] According to a recent study, there are more than 6 million closed-circuit television (CCTV) cameras in the UK, more per citizen than in any country apart from China.[2] These cameras can take images of faces they film and compare them against a pre-defined database of images to determine if there is a match. That means they can be used to quickly identify individuals even in crowded areas such as shopping centres, airports, railway stations, and city streets. Even when a face is partially covered – by a cap or glasses, for example – they can still usually match it up with a stored image.[3]

The extensive presence of FRT in the UK raises concerns from the angle of democracy and individual freedoms: is the UK becoming an 'Orwellian' society where all individuals are monitored, identified, and potentially controlled? As observed in the literature, mass surveillance has immediate implications on privacy rights, but the knowledge gathered through monitoring can be used to compress

[1] See comments throughout this chapter.

[2] Silkie Carlo, 'Britain has more surveillance cameras per person than any country except China. That's a massive risk to our free society' (17 May 2019), *Time*, https://time.com/5590343/uk-facial-recognition-cameras-china/.

[3] Scutum, 'Facial recognition CCTV cameras' (n.d.), www.scutumlondon.co.uk/security-surveillance-systems/cctv-surveillance-cameras/cctv-products/facial-recognition-cctv-cameras/.

https://doi.org/10.1017/9781009321211.015 Published online by Cambridge University Press

other individual freedoms.[4] It follows that regulation on FRT should strive to minimise the interferences with privacy, and thus other individuals' rights, if democratic values of human dignity and pluralism are to be truly achieved.

Several non-governmental organisations (NGOs) protecting privacy rights established in the UK became the centre of important strategic litigation to protect privacy rights.[5] For instance, in the *Bridges* case,[6] supported by the NGO Liberty, the Court of Appeal has not only invalidated the use of facial recognition technology by South Wales Police (SWP), but also raised the attention to some unsolved issues regarding the use of FRT for law enforcement. As a matter of fact, notwithstanding the presence of multiple legal sources governing FRT, several legal and ethical issues are still unsolved. Clear legislation on FRT is missing.[7] In which circumstances should FRT not be used? What information duties should be discharged by those utilising FRT? What remedies should exist for individuals to address abuses of this technology? These are only some of the questions that should be addressed by legislators in order to prevent the emergence of an Orwellian society. What the future holds for FRT in the UK remains to be seen. Uncertainty is even higher in light of Brexit and the potential reforms to be introduced in the UK on the data protection framework.[8]

This chapter outlines the framework on FRT in the UK and offers reflections on the future of this technology in that jurisdiction. It is structured as follows. First, it discusses the uses of FRT in the UK and the public perceptions surrounding this technology. Second, it explores the UK relevant legal framework, and highlights its gaps. Third, the chapter discusses the *Bridges* saga and its implications. Fourth, the chapter highlights selected regulatory matters on FRT that are currently unsettled and on which legislative guidance appears necessary to prevent the establishment of an Orwellian society in the UK. Conclusions follow.

12.2 FRT IN THE UK: BETWEEN PUBLIC AND PRIVATE

To assess the impact of FRT in the UK, we need first to explore its use in this jurisdiction. The first observation is *the extensive use of this technology by both private*

[4] European Parliament, 'The US Surveillance programmes and their impact on EU citizens' fundamental rights' (2013), www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf; José R. Augustina and Gemma Galdon Clavell, 'The impact of CCTV on fundamental rights and crime prevention strategies: The case of the Catalan Control Commission of Video Surveillance Devices' (2011) 27(2) *Computer Law and Security Review* 168–174.

[5] See further references in this chapter.

[6] [2020] EWCA Civ 1058.

[7] Kay L. Ritchie, Charlotte Cartledge, Bethany Growns, An Yan, Yuqing Wang, Kun Guo, Robin S. S. Kramer, Gary Edmond, Kristy A. Martire, Mehera San Roque, and David White, 'Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world' 2021 16(10) *PLoS ONE*.

[8] UK Government, 'Data: A new direction' (23 June 2022), Department for Digital, Culture, Media & Sport, www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation.

and public entities. Starting from the public sector, the first CCTV system in the UK was set up in 1953 in London for the Queen's coronation.[9] By the 1960s, permanent CCTV began to cover certain London streets. Since then, the reach of CCTV surveillance has expanded in sporadic bursts, with many cameras installed in response to the 1990s IRA attacks and then again after 9/11 and the London Underground bombing.[10] Currently, CCTV cameras embed FRT that allows the identification of individuals against the information included in databases managed by law enforcement bodies. Policy documents produced by Metropolitan Police and the College of Policing indicate that FRT can be used to improve the fight against crime and make people's lives safer.[11] Moreover, the British government specifies that CCTV serves four purposes: the detection of crime and emergency incidents, the recording of events for investigations and evidence, direct surveillance of suspects, and the deterrence of crime.[12] In the past, critics argued there is little evidence to support the proposition that its use has reduced levels of crime. An internal report dated 2009 produced by London's Metropolitan Police revealed that only one camera out of every 1,000 had been involved in solving a crime.[13]

However, recent documents produced by the Metropolitan Police indicate that the main advantage of using FRT is that of making manhunts more effective. It was observed that many manhunts for offenders wanted for very serious offences such as murder involve hundreds of officer and staff hours. When aggregated together, manhunts cost many thousands of policing hours across London. By comparison, the four recent trial deployments of live facial recognition (LFR) resulted in eight arrests.[14] It was also reported that LFR deployments provide opportunities for police officers to engage with a person potentially wanted by the police and the courts. Another relevant comparative metric for LFR is the policing outcomes resulting from 'stop and search'. According to a report published in February 2020 by the Metropolitan Police,[15] 13.3 per cent of stops resulted in an arrest in 2019. By contrast, 30 per cent of engagements following an adjudicated alert from the LFR system

[9] Philipp Chertoff, 'Facial recognition has its eye on the U.K.' (7 February2020), Lawfare, www.lawfareblog.com/facial-recognition-has-its-eye-uk.

[10] Ibid.

[11] Metropolitan Police Service, 'Facial recognition' (2022), www.met.police.uk/advice/advice-and-information/fr/facial-recognition. College of Policing, 'Live facial recognition technology guidance published' (22 March 2022), www.college.police.uk/article/live-facial-recognition-technology-guidance-published.

[12] Parliamentary Office of Science and Technology, 'Postnote: CCTV', Number 175 (April 2022), www.parliament.uk/globalassets/documents/post/pn175.pdf.

[13] Christopher Hope, '1,000 CCTV cameras to solve just one crime, Met Police admits' (25 August 2009), *The Telegraph*, www.telegraph.co.uk/news/uknews/crime/6082530/1000-CCTV-cameras-to-solve-just-one-crime-Met-Police-admits.html.

[14] National Physical Laboratory and Metropolitan Police Service, 'Metropolitan Police Service live facial recognition trials' (February 2020), www.met.police.uk/SysSiteAssets/media/downloads/central/services/accessing-information/facial-recognition/met-evaluation-report.pdf.

[15] Ibid.

resulted in the arrest of a wanted person.[16] While the enhancement of public security and safety via FRT is a valuable goal, we should not lose sight of the significant implications of this technology on individual freedoms.

Such implications are amplified by the substantial employment of FRT by private entities in the UK. For instance, Clearview AI has collected more than 20 billion images of people's faces and data from publicly available information on the internet and social media platforms all over the world, including in the UK, to create an online database. The Information Commissioner's Office (ICO) has recently sanctioned this company for violation of data protection rules.[17] Further examples are supermarkets such as Tesco, Budgens, and Sainsbury, and start-ups such as Yoti and Facewatch. Such private entities utilise FRT in different fashions. For instance, Yoti, an FRT software, is used in UK cinemas to verify the age of customers,[18] while a growing number of businesses use Facewatch to share CCTV images with the police and identify suspected shoplifters entering their store.[19] Such widespread use of FRT by private entities is likely to cause invasive interferences with individual entitlements. Let us consider, for instance, the employment of FRT in supermarkets and in the workplace. The data gathered through FRT used in supermarkets might increase the potential for profiling consumers and thus limiting their choices based on selected biometric features.[20] Similarly, the use of FRT by employers could potentially facilitate profiling and monitoring employees' behaviours and even emotional states. As a result, employees may be controlled and ultimately prevented from exercising their fundamental rights, such as the freedom of expression. Constraining and regulating the use of this technology by private entities becomes essential to prevent indiscriminate restrictions of fundamental rights.

Another peculiarity of the use of FRT in the UK is that, especially in the field of law enforcement, the deployment of this technology has occurred *via partnerships between private entities providing digital services or infrastructures and public entities*. For instance, the Japanese technology company NEC provides cameras to the Metropolitan Police and SWP.[21] There is no transparency on how NEC was identified as supplier to SWP. The only publicly available information is contained in a series of statements published by NEC's and SWP's websites.[22] This example

[16] Ibid.

[17] ICO, 'ICO fines facial recognition database company Clearview AI Inc more than £7.5 m and orders UK data to be deleted' (23 May 2022), https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

[18] Sofi Summers, 'UK Cinema Association partners with digital identity provider Yoti to ease "proof of age" challenges at cinemas' (27 May 2022), www.yoti.com/blog/uk-cinema-association-partners-yoti-proof-of-age/.

[19] Chris Vallance. 'Facial recognition "watch-list" trial in UK stores', *BBC* (16 December 2005), www.bbc.co.uk/programmes/p03c7srr.

[20] Shoshana Zuboff, 'Big other: Surveillance capitalism and the prospects of an information civilization' (2015) 30 *Journal of Information Technology* 75–89.

[21] NEC, 'South Wales Police – Smarter recognition, safer community' (n.d.), www.necsws.com/case-studies/public-safety/facial-recognition/facial-recognition-south-wales-police.

[22] Ibid.

raises the question of how the selection of specific technologies provided by private entities may shape public services. As a subsequent matter, the issue arises as to what values, principles and rules should guide public–private partnerships in the field of law enforcement, especially when dealing with the processing of sensitive personal data.

The diffusion and evolution of FRT in the UK has led to the development of a system in which civil society has been crucial in casting light on the issues attached to FRT technology and its impact on individuals' rights. The *establishment of numerous privacy-related NGOs* appears to be a direct consequence of the spread in use of this technology on the UK territory. To name but a few, Privacy International, Liberty, Open Rights Group, and Big Brother Watch were all born out of the concerns surrounding mass surveillance in the UK.[23] These entities have contributed to many strategic litigation cases that have shaped the legal landscape of FRT regulation in the UK. The *Bridges* case, discussed in Section 12.4, is an instance of strategic litigation relating to FRT driven by the NGO Liberty. It is difficult to draw a clear connection between the work of civil society in the field of FRT and the impact of advocacy and strategic litigation on public awareness regarding the FRT challenges and risks. However, recent studies have highlighted that the UK public has a contradictory stance with reference to this technology.

In a study conducted by Steinacker and his colleagues involving more than 6,000 respondents, it was observed that while an overall of 43 per cent of respondents supported the use of surveillance, 26 per cent opposed it.[24] In the same study, 39 per cent of the interviewees expressed the view that FRT increases privacy violations and 53 per cent were of the opinion that FRT enhances surveillance.[25] These findings were confirmed by a study conducted by the Ada Lovelace Institute in 2019. The Institute commissioned YouGov to conduct an online survey with over 4,000 responses from adults aged sixteen and above. The survey asked respondents to express their views on a range of uses of FRTs in a number of settings including law enforcement, education, and in the private sector.[26] The report found that support for the use of FRT depends on the purpose. Notably, the study found that 49 per cent of the respondents supported its use in policing practices with the presence of appropriate safeguards, but 67 per cent opposed it in schools, 61 per cent on public transport, and a majority of 55 per cent wanted restrictions placed on its use by police.[27]

[23] See https://privacyinternational.org; www.libertyhumanrights.org.uk; www.openrightsgroup.org; https://bigbrotherwatch.org.uk.

[24] Léa Steinacker, Miriam Mechel, Genia Kostka, Damian Borth, 'Facial recognition: A cross-national survey on public acceptance, privacy and discrimination' (2020), https://arxiv.org/pdf/2008.07275.pdf.

[25] Ibid.

[26] Ada Lovelace Institute, 'Beyond face value: Public attitudes to facial recognition technology' (September 2019), www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL.pdf.

[27] Steinacker et al., 'Facial recognition'.

https://doi.org/10.1017/9781009321211.015 Published online by Cambridge University Press

In light of these findings, it appears that the public perception of FRT in the UK depends on the use of that technology. While this research illustrates that individuals appreciate the potential of FRT in the field of security and law enforcement, the general impression emerging from these surveys is that there is still a lack of awareness regarding the full consequences and impact of FRT on individual rights beyond privacy. This conclusion is further strengthened when one considers the significant gaps existing in the UK regulatory approach to FRT. It is argued that were the implications of FRT on individual rights' protection entirely appreciated, a stronger social resistance against FRT would emerge in light of the current limited framework. The attention on safety and security as one of the advantages of FRT would most likely be reassessed against the worrisome implications that mass surveillance, and ultimately a police state, would have on individual freedoms. The following paragraphs outline the UK legal framework on FRT and its limits.

12.3 THE LEGAL FRAMEWORK

Until 2019, the Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board oversaw the police use of automated facial recognition (AFR), LFR custody images, and new biometrics. The last meeting of the Board took place in September 2019 and alternative governance arrangements are now in place.[28] Currently, two bodies supervise the use of FRT: the ICO and the Biometric and Surveillance Camera Commissioner. The legal framework governing FRT in the UK is multi-layered. It is composed of human rights law, but also by data protection and law enforcement rules. As a result, the rights to privacy and data protection, being the most immediately entitlements affected by FRT, are to be balanced with public security and law enforcement objectives.

The starting point for analysing the UK FRT framework is the Human Rights Act, which gives effect to Article 8 ECHR, protecting the right to privacy, in the UK territory. In addition, the Data Protection Act (DPA) of 2018,[29] which transposed the EU's General Data Protection Regulation (GDPR) in the UK, plays a crucial role in governing FRT. This Act provides the duties for controllers and processors and rights for data subjects. It grants enhanced protection for sensitive personal data,[30] and imposes specific requirements for personal data used in the context of law enforcement.[31] While under EU law data protection is a fundamental right, in the post-Brexit era data protection has lost this status since the EU Charter of Fundamental

[28] UK Government, 'Law enforcement facial images and new biometrics oversight and advisory board' (n.d.), www.gov.uk/government/groups/law-enforcement-facial-images-and-new-biometrics-oversight-and-advisory-board.

[29] Data Protection Act 2018, www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

[30] See section 42.

[31] See part 3 of the DPA 2018.

https://doi.org/10.1017/9781009321211.015 Published online by Cambridge University Press

Rights is no longer binding in the UK.[32] Additionally, the UK GDPR framework may be subject to evolution in light of recent plans of the UK Government to depart from the EU legislation and case law.[33]

The Protection and Freedoms (PoFA) Act 2012 is also of relevance, since it regulates the use of evidential material, including biometric material that may be gathered through FRT. Furthermore, mention should be made of the Surveillance Camera Code of Practice, originally published in 2013 and amended in November 2021. This code is an implementation of Section 29(6) of PoFA and is to be taken into account by a relevant authority in the exercise of its functions when involving the operation or use of any surveillance camera systems, or the use or processing of images or other information obtained by virtue of such systems. The code sets out twelve guiding principles, such as that there should be effective review of audit mechanisms to ensure respect for legal requirements, policies, and standards. While this code applies to public authorities, private entities are not constrained by it. The ICO has issued guidance harmonising the Surveillance Camera Code of Practice with the GDPR requirements.[34] In this sense, the guidance has a broader scope than the code. In addition, we should mention that public authorities using FRT technology have produced policy and guidance documents. To name but one example, the Metropolitan Police have issued several LFR policy documents, including Data Protection Impact assessments and the 'Standard operating procedure'.[35] Similarly, SWP has produced multiple documents stating their approach to the deployment of FRT.[36] Finally, several guidance documents, such as those issued by the British Security Industry Association regarding the ethical and legal use of AFR,[37] or the Data Ethical Framework prepared by the UK Government, provide directives on the employment of FRT.[38] The effects and status of these guidance documents is unclear. While they may be used to guide the action of

[32] Marco Galimberti, 'Farewell to the EU Charter: Brexit and fundamental rights protection' (2021) (1) *Nordic Journal of European Law* 36–52.

[33] UK Government, 'Data: A new direction', Department for Digital, Culture, Media & Sport (10 September 2021), www.gov.uk/government/consultations/data-a-new-direction.

[34] ICO, 'Checklist for limited CCTV systems' (n.d.), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/checklist-for-limited-cctv-systems/.

[35] Metropolitan Police, 'Data protection impact assessment' (n.d.), www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/impact-assessments/lfr-dpia.pdf; Metropolitan Police, 'Standard Operating Procedure (SOP) for the overt deployment of Live Facial Recognition (LFR) technology' (29 November 2022), www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-sop.pdf.

[36] See South Wales Police, 'Facial recognition technology', www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/.

[37] See BSIA, 'Automated facial recognition: A guide to ethical use' (1 January 2021), BSIA Artificial Intelligence Series, www.bsia.co.uk/zappfiles/bsia-front/public-guides/form_347_automated_facial%20recognition_a_guide_to_ethical_and_legal_use-compressed.pdf.

[38] UK Government, 'Data ethics framework' (16 September 2020), Central Digital and Data Office, www.gov.uk/government/publications/data-ethics-framework/data-ethics-framework-2020.

public authorities, whether or not they are binding is allegedly different from the law.[39]

Overall, the private use of FRT appears less regulated than the public enforcement. However, the presence of a more developed legislative framework for the public sphere does not equate to effective FRT regulation in that sector. In 2019, the London Policing Ethics Panel advanced several recommendations concerning LFR, such as that there should be enhanced ethical governance of policing technology field research trials, and that regulation of new identification technologies should be simpler.[40] The ICO also issued an opinion on the use of LFR technology by law enforcement authorities in public places, which concluded that the use of that technology should meet the threshold of strict necessity.[41] For example, it was suggested that FRT could be used to locate a known terrorist but not indiscriminately in order to identify suspects of minor crimes.[42] The 2022 report of the Minderoo Centre for Technology and Democracy found that the use of FRT by the UK police did not meet fundamental rights standards.[43] Yet, as mentioned, private parties may also be extremely intrusive when utilising FRT. One may wonder whether this different treatment for private bodies, which are subject to less cumbersome duties when utilising FRT, is at all justified.

In the UK, the ICO, former Biometrics Commissioner, and former Surveillance Camera Commissioner have all argued that the law relating to biometric technologies is no longer fit for purpose.[44] The same point was advanced by the Court of Appeal of England and Wales in August 2020 in its judgment on the *Bridges* case, concluding that there were 'fundamental deficiencies' in the legal framework surrounding the police use of facial recognition.[45] The next paragraphs offer an overview of this case, which is pivotal in identifying existing regulatory gaps concerning FRT in the UK.

[39] Giulia Gentile, '"Verba volant, quoque (soft law) scripta?" An analysis of the legal effects of national soft law implementing EU soft law in France and the UK' in M. Eliantonio, E. Korkea-Aho, and O. Stefan (eds.), *EU Soft Law in the Member States: Theoretical Findings and Empirical Evidence* (Hart Publishing, 2021), pp. 79–98.

[40] Ritchie et al., 'Public attitudes'.

[41] ICO, 'The use of live facial recognition technology by law enforcement in public places' (31 October 2019), https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

[42] Ritchie et al., 'Public attitudes'.

[43] See Evani Radiya-Dixit, 'A sociotechnical audit: Assessing police use of facial recognition' (October 2022), Minderoo Centre for Technology and Democracy, www.mctd.ac.uk/wp-content/uploads/2022/10/MCTD-FacialRecognition-Report-WEB-1.pdf; Vikram Dodd, 'UK police use of live facial recognition unlawful and unethical, report finds' (27 October 2022), *The Guardian*, www.theguardian.com/technology/2022/oct/27/live-facial-recognition-police-study-uk?CMP=share_btn_tw.

[44] See Ada Lovelace Institute, 'The Citizens' Biometrics Council' (March 2021), www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Citizens_Biometrics_Council_final_report.pdf.

[45] [2020] EWCA Civ 1058 (*Bridges*) para. 91.

https://doi.org/10.1017/9781009321211.015 Published online by Cambridge University Press

12.4 THE *BRIDGES* CASE

The case concerned the deployment of AFR Locate, a technology that involves the capturing of digital images of members of the public, which were then processed and compared with digital images of persons on a watchlist compiled by SWP. The claimant in the case, Edward Bridges, supported in his action by the NGO Liberty, raised complaints against the use of this technology against him on two occasions and against the use of AFR Locate in general. The watchlists used in the deployments contested by Mr Bridges included, among others, persons wanted on warrants, individuals who were unlawfully at large having escaped from lawful custody or persons simply of possible interest to SWP for intelligence purposes.

At first instance, the Divisional Court declared that Article 8 ECHR was not violated. This was because of 'the common law powers of the police to obtain and store information for policing purposes, and [the fact] that the compilation of the watchlists is both authorised under the Police and Criminal Evidence Act 1984 and within the powers of the police at common law'.[46] The court also found that DPA 2018 and the Code of Practice on the Management of Police information provided a legal basis for the use of AFR Locate. Overall, the 'accordance with the law' requirement laid down in Article 8(2) ECHR was satisfied. Furthermore, the Divisional Court rejected the pleas based on data protection law. Of interest is the way in which the court delineated the scope of the margin of appreciation enjoyed by the ICO. Notably, it concluded that it was for the ICO to assess whether the documents adopted by the SWP complied with Section 42(2) of the DPA 2018, requiring the adoption of a policy document by public entities processing personal data for law enforcement purposes. The court also rejected the claim that SWP had failed to comply with the Equality Act 2010.

Mr Bridges challenged the Divisional Court's judgment and was granted leave to appeal. In its judgement, the Court of Appeal began by considering whether the interference of privacy rights caused by the SWP was in accordance with the law, as demanded by Article 8(2) ECHR. While it found that the action of the SWP was carried out pursuant to a legal basis, it embraced a relativist approach: it advanced the view that 'the more intrusive the act complained of, the more precise and specific must be the law said to justify it'.[47] After acknowledging that the technology involved in the case was different from that considered in previous judgments,[48] the court held that 'the legal framework that the Divisional Court regarded as being sufficient to constitute the "law" for the purposes of Article 8(2) is on further analysis insufficient'.[49] In particular, the Court of Appeal argued that two issues remained

[46] Ibid., para. 38.
[47] Ibid., para. 82, citing *R (Wood) v Metropolitan Police Commissioner* [2009] EWCA Civ 414.
[48] *S v UK* Apps nos. 30562/04 and 30566/04 (ECHR, 4 December 2008) and R *(Catt) v Association of Chief Police Officers* [2015] UKSC 9.
[49] EWCA Civ 1058 (*Bridges*) para. 90.

https://doi.org/10.1017/9781009321211.015 Published online by Cambridge University Press

open under the framework in place, the 'who' and the 'where' questions. As a matter of fact, the applicable law did not clarify who could be placed on the watchlist, nor was it clear that there were any criteria for determining where AFR Locate could be deployed. On this issue, the court advanced the view that the legislator should provide clearer guidance on the erasure of data of individuals who are captured by FRT but do not match the identity of any person included in the watchlist. Subsequently, the judgment moved on to the analysis of the Surveillance Camera Code of Practice. The court noted that 'the guidance does not contain any requirements as to the content of local police policies as to who can be put on a watchlist. Nor does it contain any guidance as to what local policies should contain as to where AFR can be deployed.'[50] The court also assessed the documents issued by the SWP, and concluded that they too left unsolved the 'who' and 'where' questions. As a result, the first ground submitted by Mr Bridges concerning the violation of the legal basis requirement under Article 8 ECHR was well founded.

The court then tackled the second ground raised by Mr Bridges; that is, whether the SWP complied with principle of proportionality in the deployment of AFR Locate. The judgment found that the Divisional Court did not err in the assessment of proportionality. While the appellant had suggested that the balancing under proportionality should consider not only the FRT's impact on a single individual, but also on the public as a whole, the Court of Appeal held that the assessment of proportionality should occur as a matter of legal principle,[51] and therefore not in abstract terms. The second ground was thus dismissed.

However, the court allowed the appeal on the third ground submitted by Mr Bridges, notably that the data protection impact assessment (DPIA) carried out by the SWP did not comply with the DPA 2018 requirements. On this issue, the Court of Appeal ruled that, since SWP had failed to comply with Article 8 ECHR, and especially the 'in accordance with the law' requirement, the DPIA was not compliant with the DPA 2018.

Subsequently, the Court of Appeal evaluated whether the SWP had failed to respect Section 35 of the DAP 2018, detailing the first data protection principle. The combined reading of Sections 35, 42 and Schedule 8 DPA 2018 requires public entities processing personal data for law enforcement purposes to have appropriate policy documents in place. The Court of Appeal held that, since the ICO had found that the SWP documents contained sufficient information in compliance with Section 42(2) DPA, the Divisional Court did not err in law. The fact that the ICO had later revised the guidance on FRT and law enforcement could not change the validity of the ICO's opinion on the policy documents. Putting it differently, the updated guidance of the ICO could not have retroactive effects and invalidate the policy documents adopted by SWP.

[50] Ibid., para. 120.
[51] Ibid., para. 139.

Finally, the court considered whether SWP had breached the Equality Act 2010. To address this plea, the court evaluated the robustness of the verifications carried by SWP with reference to the potential biases entailed by the FRT. The court observed that 'SWP have never sought to satisfy themselves, either directly or by way of independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex. There is evidence [...] that programs for AFR can sometimes have such a bias.'[52] As a result, the court concluded that the safeguards employed by the SWP were insufficient, and therefore this ground of appeal was allowed.

The *Bridges* saga prompts several observations. First, it demonstrates that the central provision in the reasoning of the parties as well as the court in drawing the boundaries for the use of FRT was the fundamental right to privacy protected under the ECHR. By contrast, the data protection framework was employed to 'compensate' and strengthen the fundamental right to privacy. Through the prism of Strasbourg case law, Article 8 ECHR appears to offer ample guidance to courts on how to achieve the protection of privacy even in the face of technological advancements such as FRT.[53] Second, the *Bridges* case showcases the intersectionality of FRT. This technology does not only impact privacy and data protection rights, but also other fundamental entitlements, such as the right not to be discriminated against. Yet additional fundamental rights could be found to intersect with the use of FRT, such as the freedom of expression or the right to liberty. Third, the case suggests that different understanding of the principle of proportionality and its interplay with fundamental rights can allow for stricter or laxer scrutiny over the employment of FRT. In *Bridges*, the Court of Appeal did not consider the 'necessity' requirement or the 'stricto sensu' proportionality; rather, it carried a soft scrutiny over the choices of the SWP. Hence, owing to the malleability of proportionality, one may wonder whether this is an effective principle to carry a precise scrutiny over the deployment of this technology and its implications. The answer to this matter depends on personal views on the very principle of proportionality. Fourth, one may wonder how much 'law' is needed to regulate FRT. While the Court of Appeal considers that it is not the place of the judges to dictate what the law should look like, at the same time it cast light on selected drawbacks and limitations emerging from the current framework. The Court of Appeal invited the legislator to clarify the 'who' and 'where' questions and to detail rules on the deletion of personal data for individuals captured by FRT. One could think of additional questions and issues that require legislative action. Indeed, the *Bridges* saga highlighted only selected open questions concerning the use of FRT in the UK. The future of FRT regulation in the UK will depend on how the uncertainty surrounding these issues is tackled.

[52] Ibid., para. 199.
[53] Ibid.

https://doi.org/10.1017/9781009321211.015 Published online by Cambridge University Press

12.5 THE FUTURE OF FRT IN THE UK

While the *Bridges* case has powerfully illustrated some of the crucial gaps in the current framework on FRT, there are further unsletted matters. To name but a few: For what purposes and in what contexts is it acceptable to use FRT to capture an individual's image? What checks and balances should be in place to ensure fairness and transparency in the use of FRT? What accountability mechanisms should be established for different usages? The list could continue. Several NGOs have produced reports partially addressing these matters. Interestingly, there seems to be convergence towards the (at least partial) halting of FRT under the current rules. For instance, the Ada Lovelace Institute commissioned the Ryder Review,[54] published in June 2022, which recommended that the use of live FRT should be suspended until the adoption of a legally binding code of practice governing its use. The presence of binding rules identifying accountable entities and means of redress for individuals are considered as crucial to enhance the protection of individuals against FRT technology.[55] The report specified that the code should not only address the public use of the technology, but also its deployment by private parties. Furthermore, the Mideroo report on the use of FRT,[56] published in October 2022, went as far as calling for a ban of FRT in the context of police activities. The report justified this recommendation in light of the blatant violations of fundamental rights by way of deployment of FRT by the police.

Interestingly, these proposals are to a certain extent in line with the position of EU institutions. For instance, the European Data Protection Board called for a general ban on any use of AI for an automated recognition of human features in publicly available spaces, as well as for AI systems categorising individuals from biometrics into clusters.[57] Moreover, in the European Parliament there is growing consensus on banning the use of this technology.[58] Whether the UK legislator and authorities involved in the regulation of FRT will reach a similar conclusion requiring the suspension, if not the banning, of FRT remains to be seen. In July 2022, Liberty published a tweet indicating that the Metropolitan Police used FRT at Oxford Circus. As a result, thousands of people walking in that area were monitored and captured

[54] See Ada Lovelace Institute, 'The Ryder Review' (June 2022), www.adalovelaceinstitute.org/wp-content/uploads/2022/06/The-Ryder-Review-Independent-legal-review-of-the-governance-of-biometric-data-in-England-and-Wales-Ada-Lovelace-Institute-June-2022.pdf.

[55] See Julia Black and Andrew D. Murray, 'Regulating AI and machine learning: Setting the regulatory agenda' (2019) 10(3) *European Journal of Law and Technology*, https://eprints.lse.ac.uk/102953/4/722_3282_1_PB.pdf.

[56] See Radiya-Dixit, 'A sociotechnical audit'.

[57] See EDPB, 'Joint opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence' (18 June 2021), EDPB and EDPS, https://edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

[58] See Clothilde Goujard, 'Europe edges closer to a ban on facial recognition' (20 September 2022), *Politico*, www.politico.eu/article/europe-edges-closer-to-a-ban-on-facial-recognition/.

by cameras. Such overt and extensive use of FRT in the UK might signify that this jurisdiction is still far away from undergoing a serious reconsideration of FRT's limited benefits and high risks. However, several crucial changes to the current rules seem necessary. These reforms should involve increasing public awareness of the implications of FRT as well as enhancing transparency on the deployment of that technology. Another point that future legislation should tackle is how to ensure that public–private partnerships involving the digitisation of public services respect public goods and values. The opaque co-operation between NEC and SWP suggests that the public is unable to scrutinise how public entities build their co-operation with private digital providers, and therefore how much power private parties have in shaping the public sphere. Until the day such legislation is in place, it is legitimate to ask: 'Does Big Brother exist in the UK?'

12.6 CONCLUSION

The UK has been a crib for the development and deployment of FRT. Since the 1950s, this technology has been largely used in the public sphere, and especially for law enforcement purposes. However, FRT has rapidly expanded, and it is now omnipresent, having landed also in the private sector. As a result, the UK legal order offers a remarkable case study to reflect on the future of FRT regulation. The existing FRT framework in the UK is multi-layered but also fragmented and incomplete. The loopholes of the rules currently in place became evident in the *Bridges* saga. While the first instance court considered the use of FRT by SWP lawful, the Court of Appeal identified violations of Article 8 ECHR, data protection rules, and the Equality Act 2010. Accordingly, the UK judicature has revealed the power of fundamental rights in regulating FRT and cast light on the limits of existing rules. In particular, the Court of Appeal observed that the legislator should clarify who can be placed on watchlists and where the FRT can be employed. Yet additional questions remain open, beyond those identified by the *Bridges* case: For what purposes and in what contexts is it acceptable to use FRT to capture an individual's image? What checks and balances should be in place to ensure fairness and transparency in the use of FRT? What accountability mechanisms should be established for different usages? The list could continue. Several NGOs have called for halting or even banning FRT in the UK. There is general consensus that the current UK framework is insufficient. Until the point when the UK legislator takes charge of enhancing regulation relating to FRT, it is legitimate to ask: 'Does Big Brother exist?'