11

Lawfulness and Police Use of Facial Recognition in the United Kingdom

Article 8 ECHR and Bridges *v.* South Wales Police

Nora Ni Loideain

11.1 INTRODUCTION

Police use of facial recognition is on the rise across Europe and beyond.[1] Public authorities state that these powerful algorithmic systems could play a major role in assisting them to prevent terrorism, reduce crime, and to more quickly locate and safeguard vulnerable persons (online and offline).[2] There is also an international consensus among policymakers, industry, academia, and civil society, that these systems pose serious risks to the rule of law and several human rights integral to the existence of a democratic society.[3] These include the rights to private life, freedom of expression, freedom of assembly and association, and equality as guaranteed under the European Convention on Human Rights (ECHR).[4]

[1] Nessa Lynch et al., *Facial Recognition Technology in New Zealand* (The Law Foundation, 2020); European Digital Rights, *The Rise and Rise of Biometric Mass Surveillance in the EU* (EDRi, 2021); US Government Accountability Office, 'Facial recognition technology, GAO-21-526' (2021); House of Lords, 'Technology rules? The advent of new technologies in the justice system' (2022), HL Paper 180; Nicola Kelly, 'Facial recognition smartwatches to be used to monitor foreign offenders in UK' (5 August 2022), *The Guardian*; Laura Kayali, 'French privacy chief warns against using facial recognition for 2024 Olympics' (24 January 2023), *Politico*.

[2] World Economic Forum, 'A policy framework for responsible limits on facial recognition' (3 November 2022), pp. 15–18.

[3] Big Brother Watch, '*Face off: The lawless growth of facial recognition in the UK*' (May 2018), pp. 9–19; Pete Fussey and Daragh Murray, 'Independent report on the London metropolitan police's services trial of live facial recognition technology' (July), pp. 5–6; Information Commission's Office, 'The use of live facial recognition technology by law enforcement in public places' (2019), ICO Opinion; Kate Crawford, 'Regulate facial recognition technology' (2019) 572 *Nature* 565; European Digital Rights, *The Rise and Rise of Biometric Mass Surveillance*, pp. 12–13; Biometrics, Forensics and Ethics Group, 'Briefing note on the ethical issues arising from public–private collaboration in the use of live facial recognition technology' (2021), UK Government; Sarah Bird, 'Responsible AI investments and safeguards for facial recognition' (21 June 2022), Microsoft Azure AI; Matthew Ryder KC, *Independent Legal Review of the Governance of Biometric Data in England and Wales* (Ada Lovelace Institute, 2022); Information Commissioner's Office, 'ICO fines facial recognition company Clearview AI Inc more than £7.5 m' (May 2022); Clothilde Goujard, 'Europe edges closer to a ban on facial recognition' (20 September 2022), *Politico*.

[4] On the risks of unlawful discrimination from AI-based systems used for predictive policing, see EU Agency for Fundamental Rights (FRA), '*Bias in algorithms: AI and discrimination*' (2022), FRA

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

In response to these 'profound challenges', policymakers and researchers have called for law reform that would provide greater clarity on the limits, lawfulness, and proportionality of facial recognition and other emerging AI-based biometric systems (such as gait and emotion recognition).[5] Consequently, some local and state governments in the United States have placed legal restrictions or banned law enforcement use of facial recognition technologies.[6] During the pre-legislative stages of the proposed EU AI Act, the European Parliament has also issued calls for a ban on the use of private facial recognition databases in law enforcement.[7] The world's first case examining the legality of a facial recognition system deployed by police, *Bridges* v. *South Wales Police*, thus remains an important precedent for policymakers, courts, and scholars worldwide.[8]

This chapter focusses on the role and influence of the right to private life, as enshrined in Article 8 ECHR and the relevant case law of the European Court of Human Rights (ECtHR), in the 'lawfulness' assessment of the police use of live facial recognition (LFR) in *Bridges*. A framework that the Court of Appeal for England and Wales ultimately held was 'not in accordance with the law' for the purposes of Article 8(2) and therefore in breach of Article 8 ECHR.[9] The analysis also considers the emerging policy discourse prompted by *Bridges* in the United Kingdom (UK) surrounding the need for new legislation.[10] This marks a significant shift away from the current AI governance approach of combining new ethical standards with existing law.[11]

Report, pp. 36–48; FRA, 'Facial recognition technology: Fundamental rights considerations in law enforcement' (2019), FRA Paper, pp. 27–28.

[5] Bethan Davies, Martin Innes, and Andrew Dawson (2018), 'An evaluation of South Wales Police's use of automated facial recognition' (September 2018), Report, Crime & Security Research Institute, Cardiff University, p. 43; Crawford, 'Regulate facial recognition technology'; Information Commission's Office, 'The use of live facial recognition technology', pp. 21–22; House of Lords, 'Technology rules?', pp. 76–77. See generally European Data Protection Board and European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 5/2021' (18 June 2021).

[6] Kashmir Hill, 'How one state managed to actually write rules on facial recognition' (27 February 2021), *New York Times*.

[7] European Parliament, 'Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters' (2021), Report-A9-0232/2021.

[8] *R (Bridges) v. South Wales Police* [2019] EWHC 2341, High Court; [2020] EWCA Civ 1058, Court of Appeal.

[9] [2020] EWCA Civ 1058 [210]. Other legal issues addressed in *Bridges*, concerning proportionality, data protection, and equality law, are beyond the scope of this chapter. On these areas, see Lorna Woods, 'Automated facial recognition in the UK' (2020) 6 *European Data Protection Law Review* 455; Monika Zalnieriute, 'Burning bridges: The automated facial recognition technology and public space surveillance in the modern state' (2021) 22 *Columbia Science & Technology Law Review* 284; Joe Purshouse and Liz Campbell, 'Automated facial recognition and policing' (2022) 42 *Legal Studies* 209.

[10] Biometrics and Surveillance Camera Commissioner, 'Annual report 2022' (2023), UK Government, p. 6; House of Lords, 'Technology rules?', pp. 27–32; Ryder, *Independent Legal Review*, pp. 62–67.

[11] See generally Julia Black and Andrew Murray, 'Regulating AI and machine learning' (2019) 10(3) *European Journal of Law and Technology*.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

11.2 FACIAL RECOGNITION SYSTEMS IN LAW ENFORCEMENT: LEGAL AND TECHNICAL ISSUES

Within a legal context, the use by public authorities of any preventive measures that will indiscriminately capture and analyse the biometric data of a vast number of innocent individuals raises significant questions. These include whether rule of law requirements developed for ensuring adequate limits, safeguards, and oversight for police surveillance systems in the pre-Internet era, such as closed-circuit television (CCTV), remain adequate and relevant to facial recognition systems and other modern internet-enabled and automated monitoring systems; furthermore, whether such novel and powerful AI-based technologies are strictly necessary in a democratic society and respect the presumption of innocence.[12] Privacy and data protection concerns have also been raised regarding the transparency and oversight challenges posed by the increasing role of the private sector within the areas of law enforcement and public security. These developments range from law enforcement use of data-driven tools and systems developed by industry, including commercial facial recognition software,[13] to tasking industry itself with law enforcement functions.[14]

11.2.1 *Facial Recognition Systems in Law Enforcement: Issues of Accountability and Bias*

The use of AI-based biometric systems for law enforcement purposes raises several legal and technical issues. First, there are transparency and accountability challenges that may hinder adequate independent auditing and oversight of their overall efficiency and societal impacts. These stem from the opaque design and operation of commercial facial recognition systems, including intellectual property issues, what training datasets are used, the risk of those datasets being unfairly biased, and how exactly these automated decisions and recommendations are being made (and fairly assessed) by public authorities.[15] The second concerns scientific evidence that facial

[12] Deryck Beyleveld and Roger Brownsword, 'Punitive and preventing justice in an era of profiling, smart prediction, and practical preclusion' (2019) 15 *International Journal of Law in Context* 198. See generally Andrew Ashworth and Lucia Zedner, *Preventive Justice* (Oxford University Press, 2014).

[13] For instance, multiple US public authorities have used Clearview commercial facial recognition software for law enforcement purposes since 2020: see US Government Accountability Office, 'Facial recognition technology', pp. 26–28.

[14] See Nora Ni Loideain, 'Cape Town as a smart and safe city: Implications for privacy and data protection' (2017) 4 *International Data Privacy Law* 314; Nadezhda Purtova, 'Between the GDPR and the police directive' (2018) 8 *International Data Privacy Law* 52; Orla Lynskey, 'Criminal justice profiling and EU data protection law' (2019) 15 *International Journal of Law in Context* 162; Sarah Brayne, *Predict and Surveil* (Oxford University Press, 2020); Helen Warrell and Nic Fildes, 'Amazon strikes deal with UK spy agencies to host top secret material' (25 October 2021), *Financial Times*; Litska Strikwerda, 'Predictive policing' (2020) 94 *The Police Journal* 259; Stanisław Tosza, 'Internet service providers as law enforcers and adjudicators' (2021) 43 *Computer Law & Security Review*.

[15] Linda Geddes, 'Digital forensics experts prone to bias, study shows' (31 May 2021), *The Guardian*; FRA, 'Bias in Algorithms', p. 19.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

recognition software currently designed and developed by industry, and subsequently used for law enforcement, is biased with a greater risk of false identifications ('false positives') for women and people from black, Asian, and other minority ethnic backgrounds.[16] There is then a risk that such groups may be disproportionately affected by this technology. This is particularly problematic given the need for public trust in police powers being used lawfully and responsibly and existing evidence of racial bias across the UK justice system (and indeed in other jurisdictions), with resulting harms including false arrests and over-policing of already vulnerable communities.[17]

11.2.2 *Facial Recognition Systems in Law Enforcement: 'Real-Time' and Historical*

Police trials of industry-developed facial recognition systems have been taking place in the UK since 2014.[18] Automated facial recognition (AFR) implies that a machine-based system is used for the recognition either for the entire process or assistance is provided by a human being. Live automated one-to-many matching involves near real-time video images of individuals with a curated watchlist of facial images. In a law enforcement context, this is typically used to *assist* the recognition of persons of interest on a watchlist, which means that police are required to verify or over-ride a possible match identified by the system (a system alert) and decide what actions to take (if any).[19] However, as regulators and scholars highlight, much uncertainty in UK law (and in laws across Europe) surrounds the complex legal framework governing police use of real-time access and historical (retrospective/post-event) of LFR and other biometric identification systems.[20]

In the case of historical (post-event) facial recognition systems, individual's facial data are compared and identified in searches by public authorities after the event

[16] Joy Buolamwini and Timnit Gebru, 'Gender shades: Intersectional accuracy disparities in commercial gender classification'(2018), *Proceedings of Machine Learning Research 81 Conference on Fairness, Accountability, and Transparency*, pp. 1–15; US National Institute of Standards and Technology (NIST), 'NIST study evaluates effects of race, age, sex on face recognition software' (19 December 2019).

[17] Dominic Casciani, 'Sarah Everard's murder and the questions the Met police now face' (2 October 2021), *BBC News*; UK Government, '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); Kashmir Hill, 'Wrongfully accused by an algorithm' (24 June 2021), *New York Times*; Jane Bradley, '"Troubling" race disparity is found in UK prosecution decisions' (8 February 2023), *New York Times*.

[18] *BBC News*, 'Leicestershire police trial facial recognition software' (15 July 2014); Fussey and Murray, 'Independent report'.

[19] Biometrics, Forensics and Ethics Group, 'Briefing note', p. 4.

[20] Woods, 'Automated facial recognition', p. 561; Zalnieriute, 'Burning bridges', p. 287; Nora Ni Loideain, 'A trustworthy framework that respects fundamental rights? The draft EU AI Act and police use of biometrics' (4 August 2021), Information Law & Policy Centre; European Data Protection Board and European Data Protection Supervisor, 'EDPB-EDPS Joint Opinion 5/2021'; Biometrics and Surveillance Camera Commissioner, 'Annual Report 2022', pp. 59–60.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

with images previously collected through various sources. These include custody photographs and video footage from CCTV, body-worn police cameras, or other private devices. Both the ECtHR and the Court of Justice of the EU (CJEU) view *real-time* access to these automated biometric systems, as opposed to searching through previously collected facial images, as inherently more invasive.[21] Yet these judgments do not explain why tracking a person's movements or attendance at certain events (such as public protests) over months or years should be viewed as less invasive of their privacy than one instance of real-time identification, particularly given the capacity of these automated systems to identify thousands of individuals using facial images in only a few hours.[22]

Such legal uncertainty would be less likely if these issues had already been addressed in a clear legislative framework regulating law enforcement use of facial recognition systems. As the UK House of Lords rightly points out, while they play 'an essential role in addressing breaches of the law, we cannot expect the Courts to set the framework for the deployment of new technologies'.[23] In other words, it is not the function of courts to provide a detailed and comprehensive legal framework for police powers, though they may provide careful scrutiny of the current law and its application in specific circumstances. This brings us to Article 8 ECHR and its relevance to the landmark case of *Bridges* where police use of LFR was (ultimately) held not to have met the legality requirements of Article 8(2).

11.3 JUSTIFYING AN INTERFERENCE WITH ARTICLE 8 ECHR

11.3.1 *Police Collection of Biometric Data: An Interference with Article 8(1)*

Th ECtHR has described the negative obligation to protect against arbitrary interference by a public authority with a person's private life 'as the essential object' of Article 8 ECHR.[24] It is also well-established case law that the mere storage of data 'relating to the private life of an individual' for the prevention of crime constitutes an interference with the right to respect for private life.[25] The ECtHR Grand Chamber has further held that it is irrelevant if this information collected by interception or other secret measures has not been subsequently accessed, used, or disclosed.[26]

[21] *Ben Faiza v. France* [2018] ECHR 153; Joined Cases C-511/18, C-512/18, C-520/18, *La Quadrature du Net and Others*, judgment of 6 October 2020 (ECLI:EU:C:2020:791) [187].

[22] Ni Loideain, 'A trustworthy framework'.

[23] House of Lords, 'Technology rules?', p. 50. See generally Robert Baldwin, Martin Cave, and Martin Lodge, *Understanding Regulation* (Oxford University Press, 2011).

[24] *M.D. and Others v. Spain* [2022] ECHR 527 [52].

[25] *Leander v. Sweden* (1987) 9 EHRR 433 [48]; *Catt v. United Kingdom* [2019] ECHR 76 [93].

[26] *Amann v. Switzerland* (2000) ECHR 87 [69].

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

Public information has also been held to fall within the scope of private life when it is systematically collected and stored by public authorities.[27]

In determining whether the retention of this personal data involves any 'private-life' aspects, the ECtHR will have due regard to the specific context in which the information has been recorded and retained, the nature of the records, the way in which these records are used and processed, and the results that may be obtained.[28] These standards all derive from the long-established principle in ECHR case law that 'private life' is 'a broad term *not* susceptible to exhaustive definition'.[29] As a result, this concept has been interpreted broadly by the Strasbourg Court in cases involving Article 8 ECHR and any data collection, retention, or use by public authorities in a law enforcement context. Even if no physical intrusion into a private place occurs, surveillance can still interfere with physical and psychological integrity and the right to respect for private life. For instance, in *Zakharov* v. *Russia*, the ECtHR Grand Chamber held Russia laws providing security agencies and police *remote* direct access to the databases of mobile phone providers to track users contained several 'defects' owing to a lack of adequate safeguards to ensure against abuse, thereby constituting a breach of Article 8 ECHR.[30]

The ECtHR has also shown itself to be particularly sensitive to the 'automated processing' of personal data and the unique level of intrusiveness on the right to private life posed by the retention and analysis of biometric data for law enforcement purposes, particularly DNA.[31] Biometric data (DNA, fingerprints, facial images) are a highly sensitive source of personal data because they are unique to identifying an individual and may also be used to reveal other sensitive information about an individual, their relatives, or related communities, including their health or ethnicity. Consequently, the ECtHR has held that even the capacity of DNA profiles to provide a means of 'identifying genetic relationships between individuals' for policing purposes thus amounts to a privacy interference of a 'highly sensitive nature' and requires 'very strict controls'.[32]

At the time of writing, there has been no judgment to date in which the ECtHR has been required to specifically review the compatibility of police use of a LFR system with Article 8 ECHR. This is surely, however, an important question on the horizon for the Strasbourg Court, particularly as the technology has already featured in the legal analysis of related case law. In *Gaughran* v. *United Kingdom*, the ECtHR highlighted as a factor the possibility that the police 'may also apply facial recognition and facial mapping techniques' to the taking and retention of a custody

[27] *M.M. v. United Kingdom* [2012] ECHR 1906 [187]

[28] *Gaughran v. United Kingdom* [2020] ECHR 144 [63]–[70]; *M.D. and Others v. Spain* [54].

[29] *S and Marper v. United Kingdom* (2009) 48 EHRR 50 [66] (emphasis added).

[30] *Zakharov v. Russia* (2016) 63 EHRR 17.

[31] *S and Marper v. United Kingdom* [66]–[86]; *Gaughran v. United Kingdom* [63]–[70].

[32] *Gaughran v. United Kingdom* [81]. On law enforcement use of this technique in the UK, see Biometrics and Forensics Ethics Group, *Should We Be Making Use of Genetic Genealogy to Assist in Solving Crime?* (UK Government, 2020).

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

photograph taken on the applicant's arrest in its determination that this clearly amounted an interference with Article 8(1).[33] Current jurisprudence therefore leaves little doubt that the collection, retention, or analysis of an individual's facial image for the prevention of crime (irrespective of where or how it was acquired) amounts to an interference with the right to private life, as guaranteed under Article 8 ECHR.

11.3.2 *The Legality Requirements under Article 8(2): The Traditional Approach*

Under the traditional approach of the ECtHR in its assessment of whether an interference with Article 8(1) is justified, there is a two-stage test. First, as noted earlier, the ECtHR assesses whether the complaint falls within the scope of Article 8(1) and whether the alleged interference by the contracting state (such as the UK) has engaged Article 8(1). If so, the ECtHR will then examine whether the interference with one of the protected interests in Article 8(1) (in this instance, 'private life') meets the conditions of Article 8(2). The three conditions examined during this second stage concern whether the interference is 'in accordance with the law' (legality), pursues one of the broadly framed legitimate aims under Article 8(2) (including the prevention of crime), and whether it is 'necessary in a democratic society' (proportionality). If a measure is determined not to have satisfied the requirements of the legality condition, the ECtHR will not proceed to examine the proportionality condition.[34]

The traditional approach of the ECtHR, when determining if an interference meets the legality condition under Article 8(2), requires that the contested measure satisfy two principles. The measure must have 'some basis in domestic law' and, secondly, must also comply with the rule of law.[35] In its early jurisprudence, the ECtHR established that the principle of having some basis in domestic law comprises legislation and judgments.[36] The second principle focusses on the 'quality' of the domestic law, which involves meeting the tests of 'accessibility' and 'foreseeability'.[37] As police operation and use of surveillance measures by their very nature are not open to full scrutiny by those affected or the wider public, the ECtHR has stated that it would be 'contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power'.[38]

Thus, as part of the Article 8(2) foreseeability test, the ECtHR developed six 'minimum' safeguards the basis in domestic law should address to avoid abuses of power in the use of secret surveillance. These comprise: the nature of the offences where the measure may be applied; a definition of the categories of people that may be

[33] *Gaughran v. United Kingdom* [68]–[70].

[34] On the traditional approach of the ECtHR regarding the legality condition, see generally Geranne Lautenbach, *The Concept of the Rule of Law and the European Court of Human Rights* (Oxford University Press, 2013).

[35] *Malone v. United Kingdom* (1985) 7 EHRR 14 [67].

[36] *Huvig v. France* [1990] ECHR 9 [28].

[37] *Zakharov v. Russia* [228].

[38] *Weber and Saravia v. Germany* [2006] ECHR 1173 [94] (admissibility decision).

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

subjected to this measure; a limit on the duration of the measure; the procedures to be followed for the examination, use, storage of the obtained data; precautions to be taken if data is shared with other parties; and the circumstances in which obtained data should be erased or destroyed.[39] With regard to police use of emerging technologies, the ECtHR has consistently held that such measures 'must be based on a law that is *particularly precise* … especially as the technology available for use is continually becoming more sophisticated'.[40] The ECtHR has further stressed, in cases where biometrics have been retained for policing purposes, that the need for data protection safeguards is 'all the greater' where 'automatic processing' is concerned.[41]

This traditional approach, and the resulting legality standards developed and applied therein in landmark Article 8 ECHR judgments, have shaped and brought about notable legal reforms in domestic laws governing data retention and secret surveillance by public authorities across Europe.[42] Scholars have long recognised this impact by highlighting the major role played by this Article 8 ECHR jurisprudence in entrenching and ratcheting up data privacy standards in EU countries and within the legal system of the EU.[43] Based on these Article 8 ECHR standards, these minimum legality requirements seem no less than essential to ensuring adequate accountability and oversight of police surveillance powers. Indeed, as the ECtHR points out, this is an area 'where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole'.[44] However, more recent case law dealing with Article 8 ECHR and the legality of police powers has diverged from this lauded approach.

11.3.3 *The Legality Requirements under Article 8(2): The à la carte Approach*

Two key developments in its jurisprudence have contributed to the departure of the ECtHR from its previously lauded role for setting minimum standards in the review of laws governing government surveillance and police investigatory powers across Europe.

[39] *Huvig* v. *France* [1990] ECHR 9 [34]; *Big Brother Watch* v. *United Kingdom* [2021] ECHR 439 [335]. Although established in the 1990s, some scholars refer to the six foreseeability safeguards as the '*Weber* criteria' following *Weber and Saravia*.

[40] *Huvig v. France* (1990) 12 EHRR 547 [32]; *Zakharov v. Russia* [229] (emphasis added).

[41] *S and Marper v. United Kingdom* [103]; *M.K. v. France* [2013] ECHR 341 [35]; *Aycaguer v. France* [2017] ECHR 587 [38].

[42] See, for instance, Lorena Winter, 'Telephone tapping in the Spanish criminal procedure' (2007) 13 *Jura* 7; John Spencer, 'Telephone-tap evidence and administrative detention in the UK' in Marianne Wade and Almir Maljevic (eds.), *A War on Terror?* (Springer, 2010); T. J. McIntyre and Ian O'Donnell, 'Criminals, data protection, and the right to a second chance' (2017) 58 *The Irish Jurist* 27.

[43] David Feldman, 'Secrecy, dignity or autonomy? Views of privacy as a civil liberty' (1994) 47(4) *Public Law* 54–58; Aileen McHarg, 'Reconciling human rights and the public interest' (1999) 62 *Modern Law Review* 671; Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014), p. 86; see generally Nora Ni Loideain, *EU Data Privacy Law and Serious Crime* (Oxford University Press, 2024).

[44] *Klass v. Germany* [1978] ECHR 4 [56]; *Zakharov v. Russia* [233].

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

11.3.3.1 The Hierarchy of Intrusiveness

First, the ECtHR has established that the scope of the safeguards required to meet legality requirements under Article 8(2) will depend on the nature and extent of the interference with the right to private life.[45] This means that the ECtHR will not apply the same strict-scrutiny approach regarding what requirements must be met by interferences it considers to be less intrusive and thus affect an individual's rights under Article 8(1) less seriously.[46] Accordingly, the ECtHR may assess a measure to be justified interference with Article 8 ECHR even if the domestic legal basis does not incorporate the six minimum foreseeability safeguards.[47] Application of this 'hierarchy of intrusiveness' principle is clearly evident in the general legality assessments of the High Court and Court of Appeal in *Bridges* discussed in Section 11.4.

11.3.3.2 The Joint Analysis of Legality and Proportionality

Secondly, and perhaps more importantly, scholars have raised concerns regarding a shift away from the traditional approach of the ECtHR in its Article 8 ECHR case law dealing with data retention and state surveillance. This often takes the form of an assessment that combines the legality and proportionality conditions under Article 8(2) and conflates separate principles and requirements under the distinct conditions of legality and proportionality.[48] From a rule of law perspective, this shift away from the traditional approach to the Article 8(2) stage of assessment is highly problematic as it makes less systematic and clear what is already a case-by-case analysis by the ECtHR. The resulting assessment of the domestic law is often ad hoc, patchy, and invariably less detailed regarding what specific standards contracting states should be satisfying if a contested measure is to be considered compatible with Article 8 ECHR.

Thus, as Murphy rightly notes, this joint analysis has resulted in the ECtHR applying less scrutiny of the accessibility and foreseeability legality tests, thereby serving to weaken the substantive protection of the right to respect for private life provided under Article 8 ECHR.[49] Indeed, the ECtHR may also determine (without

[45] *P.G. and J.H.* v. *United Kingdom* [2001] ECHR 550 [46].

[46] Janneke Gerards, *General Principles of the European Convention on Human Rights* (Cambridge University Press, 2019), p. 222.

[47] See, for instance, *Breyer v. Germany* [2020] ECHR 95. The CJEU has also followed the Art. 8 ECHR jurisprudence of the ECtHR and applies what this author describes as the 'hierarchy of intrusiveness' in its landmark data retention judgments: Ni Loideain, *EU Data Privacy Law*.

[48] Marie-Helen Murphy, 'A shift in the approach of the European Court of Human Rights in surveillance cases' (2014) *European Human Rights Law* 507; Kirsty Hughes, 'Mass surveillance and the European Court of Human Rights' (2018) *European Human Rights Law* 589; Nora Ni Loideain, 'Not so grand: The *Big Brother Watch* ECtHR Grand Chamber Judgment' (28 May 2021), Information Law & Policy Centre.

[49] Murphy, 'A shift in the approach', p. 513. See further Ni Loideain, *EU Data Privacy Law*.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

any detailed reasoning) that no rule of law assessment at all be undertaken and that the Article 8(2) stage assessment proceed directly to an examination of the proportionality condition. *Catt* v. *United Kingdom* illustrates the application of this à la carte approach to the requirements of Article 8(2), where the legality condition assessment is entirely omitted despite being the core issue before the ECtHR.

11.3.3.3 *Catt v. United Kingdom*: The Danger of Ambiguous Common Law Police Powers

The main facts in *Catt* involve the overt collection and subsequent retention of more than sixty records (including a photograph) on an 'Extremism database' concerning the applicant's attendance at protests between 2005 and 2009. The applicant was never charged or accused of any violent conduct as part of these protests.[50] An instrumental factor in *Catt* and *Bridges* is the broad scope of the 'common law' in England and Wales, which allowed for the police collection and storage of information in both cases.[51] Based on the undefined scope of these police powers, and the lack of clarity regarding what fell within the concept of 'domestic extremism', the ECtHR in *Catt* states that there was 'significant ambiguity over the *criteria* being used by the police to govern the collection of the data in question'.[52] A year later, in *Bridges*, the Court of Appeal would also criticise the same lack of clarity surrounding the criteria and limits underpinning the use of LFR by South Wales Police (SWP).

The Article 8(2) assessment in *Catt* then takes a curious turn. Following a bald statement that the question of whether the collection, retention, and use of the applicant's personal data is in accordance with the law is 'closely related to the broader issue of whether the interference was necessary in a democratic society', the ECtHR observes that it is not necessary for the legality condition to be examined.[53] The ECtHR proceeds to then hold that the retention of the applicant's personal data on this police database, and the fact that this retention occurred based on no 'particular inquiry', constituted a disproportionate interference with Article 8 ECHR.[54] The ECtHR was particularly critical that the applicant's personal data in *Catt* could potentially have been retained indefinitely owing to 'the absence of any rules setting a definitive maximum time limit on the retention of such data'.[55] The ECtHR further observes that the applicant was 'entirely reliant' on the application of 'highly flexible safeguards' in non-legally binding guidance to ensure the proportionate

[50] *Catt v. United Kingdom* [8]. The applicant was twice arrested for being part of demonstrations that blocked a public highway.

[51] Ibid., [34]. No specific case law is provided in *Catt v. United Kingdom* regarding the basis for these police powers.

[52] Ibid., [97] (emphasis added).

[53] Ibid., [106].

[54] Ibid., [33], [124]–[128].

[55] Ibid., [106] [124]–[128].

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

retention of his data.[56] In other words, as Woods rightly points out, this is 'hardly a ringing endorsement of broad common law powers'.[57]

However, despite its recognition of the 'danger' posed by the ambiguous approach to the scope of data collection under common law police powers,[58] the ECtHR sidesteps dealing with the lack of any clear legal basis or any assessment of the six minimum foreseeability safeguards. By departing from the traditional approach in its assessment of Article 8 ECHR, the ECtHR stops short of any detailed scrutiny of these requirements under the legality condition of Article 8(2). This allows the ECtHR to avoid addressing whether the 'common law' basis for police collection of personal data in the UK provides the 'minimum degree of legal protection' to which citizens are entitled under the rule of law in a democratic society.[59] Indeed, the curious decision of the ECtHR not to deal with these clear legality issues, and the resulting lax approach, is subject to strong criticism from members of the Strasbourg Court itself in *Catt*.[60] The latter stressed that the unresolved 'quality of law' questions posed by the contested common law police powers is actually 'where the crux of the case lies'.[61] This à la carte approach to the rule of law requirements in *Catt* is also clearly evident in the assessment of the LFR system by the national courts in *Bridges*, examined in Section 11.4.

11.4 *BRIDGES V. SOUTH WALES POLICE*: THE 'LAWFULNESS' OF AFR LOCATE

11.4.1 *Background and Claimant's Arguments*

This landmark case involves two rulings, the most significant being the Court of Appeal judgment delivered in 2020.[62] The claimant/appellant was Edward Bridges, a civil liberties campaigner who lived in Cardiff. His claim was supported by Liberty, an independent civil liberties organisation. The defendant was the Chief Constable of SWP. SWP is the national lead on the use of AFR in policing in the UK and has been conducting trials of the technology since 2017.[63] The software used by SWP for LFR in public places was developed by NEC (now North Gate Public Services (UK) Ltd).[64] In *Bridges*, AFR Locate was deployed by SWP via a live feed from

[56] Ibid., [119]. Since 2013, this guidance has been issued by the College of Policing.

[57] Woods, 'Automated facial recognition', p. 460.

[58] *Catt v. United Kingdom*, [123].

[59] As held in the leading case law on Art. 8 ECHR, lawfulness, and police powers: *Malone v. United Kingdom* (1985) 7 EHRR 14; *Huvig v. France* (1990) 12 EHRR 528; *Valenzuela v. Spain* (1999) 28 EHRR 483.

[60] *Catt v. United Kingdom*. See Separate Opinion of Judge Koskelo joined by Judge Felici [12]–[15].

[61] Ibid.

[62] [2019] EWHC 2341; [2020] EWCA Civ 1058.

[63] [2020] EWCA Civ 1058, paras 10–26. The Metropolitan Police also conducted ten trials of LFR technology between 2016 and 2019: Fussey and Murray, 'Independent report'.

[64] [2020] EWCA Civ 1058, para. 10. NEC has been awarded contracts for providing facial recognition systems to other police services since 2014, including the Metropolitan Police and Leicestershire Police.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

CCTV cameras to match any facial images and biometrics with watchlists compiled from existing custody photographs. SWP would be alerted to a possible match by the software (subject to meeting a threshold level set by SWP) and the police would verify the match, determining whether any further action was required, such as making an arrest, if the match was confirmed.[65]

Mr Bridges challenged the lawfulness of SWP's use of the AFR Locate system in general, and made a specific complaint regarding two occasions when his image (he argued) was captured by the system. The first occasion was in a busy shopping area in December 2017, the second at a protest attended by the claimant in March 2018.[66] Regarding the legality requirements of Article 8 ECHR and use of this LFR system by SWP, the claimant submitted two main arguments. First, there is 'no legal basis' for the use of AFR Locate and thus SWP did not, as a matter of law, have power to deploy it (or any other use of AFR technology). Secondly, even if it was determined that some domestic basis in law existed, it was not 'sufficient' to be capable of constituting a justified interference under Article 8(2).[67] This contrasts with legal provisions under the Police and Criminal Evidence Act 1984 and its related Code of Practice, which specifically state the circumstances that apply to police collection and use of DNA and fingerprints.[68]

The claimant submitted that to satisfy the legality condition of Article 8(2) there must be a legal framework that specifies the following five safeguards. First, the law should specify the circumstances and limits by which AFR Locate may be deployed, such as only when there is 'reasonable suspicion' or a 'real possibility' that persons who are sought may be in the location where AFR Locate is deployed. Secondly, the law should place limits on where AFR Locate may be deployed. Thirdly, the law should specify the 'classes of people' that may be placed on a watchlist, further arguing that this be limited to 'serious criminals at large'. Fourthly, the law should state the sources from where images included in watchlists may be obtained. Finally, the law should provide 'clear rules relating to biometric data obtained through use of AFR Locate'. This should include how long it may be retained and the purposes for which such information may (or may not) be used.[69]

The claimant thus challenged the absence of any accessible or foreseeable legal framework (in legislation or any related Code of Practice) that explicitly and clearly regulates the obtaining and use of AFR technology by SWP (or any police force) in England and Wales. In her role as an intervener before the High Court in *Bridges*, the then Information Commissioner (the statutory regulator of UK data protection law) made similar arguments. While she did not seek to limit the categories of persons who might be included on watchlists, her submission was that the 'categories

[65] Davies, Innes, and Dawson, 'An evaluation of South Wales Police's use', p. 13.
[66] [2020] EWCA Civ 1058, paras 27–30.
[67] [2019] EWHC 2341 [63].
[68] Ibid., [64].
[69] Ibid.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

of who could be included on a watchlist needed to be specified by law'. She also submitted that the purposes for which AFR Locate could be used should be specified in law. Finally, she argued that any use of AFR Locate, and any decision as to who should be included on a watchlist, needed to be the subject of 'independent authorisation'.[70]

11.4.2 *Police Collection, Use, Retention of a Facial Image: An Interference with Article 8(1)*

Both the High Court and the Court of Appeal engage in detail, and at length, with the Article 8 ECHR case law of the ECtHR in their assessments that SWP use of AFR Locate amounted to an infringement with the Article 8(1) rights of the applicant. As the High Court states: 'Like fingerprints and DNA, AFR technology enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances. Taken alone or together with other recorded metadata, AFR-derived biometric data is an important source of personal information.'[71] This determination is unsurprising for two reasons.

First, as noted earlier, the ECtHR has consistently held that the collection and use of biometric data using automated processing for police purposes constitutes an interference with Article 8(1). Secondly (and perhaps more importantly), none of the parties contested that use of the AFR Locate system by SWP constitutes an interference with Article 8(1).[72] Nevertheless, as the first judgment worldwide to hold that a police force's use of LFR constituted an interference with Article 8 ECHR, this assessment in *Bridges* represents an important legal precedent in European human rights law and international human rights law.

11.4.3 WAS SWP DEPLOYMENT OF AFR LOCATE 'IN ACCORDANCE WITH THE LAW' UNDER ARTICLE 8(2)?

11.4.3.1 *High Court Finds Common Law Powers 'Amply Sufficient': No Breach of Article 8 ECHR*

With respect to there being a lack of a specific statutory legal basis for SWP's use of LFR, SWP and the Secretary of State submitted to the High Court that the police's common law powers constituted 'sufficient authority for use of this equipment'.[73] The High Court accepted this argument. In its reasoning, the High Court cited

[70] Ibid.

[71] Ibid., [62].

[72] Ibid., [57].

[73] Ibid., [68].

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

at length previous caselaw where the extent of the police's common law powers has generally been expressed in very broad terms. In particular, the High Court relied heavily on the controversial majority verdict in the UK Supreme Court case of *Catt*.[74] The High Court gave considerable weight to a specific passage by Lord Sumption JSC who states in *Catt* that at 'common law the police have the power to obtain and store information for policing purposes … [provided such] powers do not authorise intrusive methods of obtaining information, such as entry onto private property or acts … which would constitute an assault'.[75]

The High Court then observed that the 'only issue' for it then to consider is whether using CCTV cameras fitted with AFR technology to obtain the biometric data of members of the public in public amounts to an 'intrusive method' of obtaining information as described by Lord Sumption JSC in *Catt*. Observing that the AFR Locate system method of obtaining an image 'is no more intrusive than the use of CCTV in the streets', the High Court held that such data collection did not fall outside the scope of police powers available to them at common law.[76] Regarding the use of watchlists within the AFR Locate system, the High Court swiftly concluded that as the relevant images were acquired by way of police photography of arrested persons in custody, the police already have explicit statutory powers to acquire, retain, and use such imagery under the Police and Criminal Evidence Act 1984.[77] The High Court also took no issue with the ambiguity of the broadly-framed scope for watchlists that may cover any 'persons of interest' to the police. The grounds for such reasoning being that the compilation of any watchlists 'is well within the common law powers of the police … namely "all steps necessary for keeping the peace, for preventing crime or for protecting property"'.[78]

The High Court briefly refers to the general requirements of accessibility and foreseeability, but there is no mention (or any engagement with) the six minimum safeguards implicitly raised in the claimant's submission on legality. Instead, the court distinguishes the need for AFR Locate to have 'detailed rules' or any independent oversight to govern the scope and application of police retention and use of biometrics (as set out in the ECtHR jurisprudence) on two grounds. First, that facial recognition is 'qualitatively different' from the police retention of DNA that provides access to a very wide range of information about a person and, secondly, it is not a form of covert (or secret) surveillance akin to communications interception.[79] In addition to the common law, the High Court stresses that the legal framework comprises three layers, namely existing primary legislation, codes of practice,

[74] This judgment was subsequently reviewed by the ECtHR (see Section 11.3.3.3).

[75] [2019] EWHC 2341 [71].

[76] Ibid., [75].

[77] Ibid., [76].

[78] Ibid., [77].

[79] Ibid., [82]–[83].

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

and SWP's own local policies, which it considered to be 'sufficiently foreseeable and accessible'.[80]

In dismissing the claimant's judicial review on all grounds, the High Court held the legal regime was adequate 'to ensure the appropriate and non-arbitrary use of AFR Locate', and that SWP's use to date of AFR Locate satisfied the requirements of the UK Human Rights Act 1998 and data protection legislation.[81]

11.4.3.2 *'Fundamental Deficiencies' in the Law: Court of Appeal Holds Breach of Article 8 ECHR*

In stark contrast to the High Court judgment, the Court of Appeal held the use of the AFR Locate system by SWP to have breached the right to respect for private life, as protected under Article 8 ECHR of the UK Human Rights Act 1998, because of 'two critical defects' in the legal framework that leave too much discretion to individual officers.[82] The Court of Appeal highlights that the guidance (not legally binding) in the Surveillance Camera Code of Practice 2013 did 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'.[83]

The Court of Appeal further criticised the fact that SWP's local policies did 'not govern who could be put on a watchlist in the first place … [and] leave the question of the location simply to the discretion of individual police officers'.[84] Thus, the Court of Appeal took issue with 'fundamental deficiencies' of the legal framework relating to two areas of concern, namely two safeguards from the established ECtHR Article 8 ECHR case law on the six minimum foreseeability safeguards: 'The first is what was called the "who question" at the hearing before us. The second is the "where question" … In relation to both of those questions too much discretion is currently left to individual police officers.'[85]

11.4.4 *Beyond* Bridges*: Moves towards Regulating Police Use of Facial Recognition?*

The Court of Appeal judgment represents a clear departure from the legality assessment of the High Court, particularly its determination that SWP's use of LFR does not satisfy the requirement of Article 8 ECHR (via the UK Human Rights Act 1998)

[80] Ibid., [84]. The primary legislation is the Data Protection Act 2018, which does not specifically refer to facial recognition technology.

[81] [2020] EWCA Civ 1058 [61].

[82] Ibid., [120].

[83] Ibid.

[84] Ibid., [129]–[130].

[85] Ibid., [91].

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

of being ‘in accordance with the law’. This assessment was long-awaited by civil society and scholars who had consistently raised concerns that police deployment in England and Wales of LFR trials risked being assessed as unlawful if challenged before the courts. Two key issues were the lack of a specific legal basis authorising police use of AFR and a lack of clarity regarding the foreseeability of the applicable circumstances and safeguards by which police services across England and Wales are lawfully permitted to use these automated systems.[86] Indeed, the former Biometrics Commissioner observed in his 2017 Annual Report that the development and deployment of automated biometric systems in use by police at that time was already ‘running ahead of legislation’.[87]

The Court of Appeal judgment in *Bridges* thus provides some clarity regarding the ‘deficiencies’ to be addressed by the current legal framework applied specifically by SWP and its deployment of a specific LFR system. Critically, however, the Court of Appeal also states that *Bridges* is ‘not concerned with possible use of AFR in the future on a national basis’, only the local deployment of AFR within the area of SWP.[88] Thus, the legality of police use of facial recognition systems (real-time and post-event) across the UK remains a subject of intense debate. Over 80,000 people have signed a petition (organised by UK-based non-governmental organisation Liberty) calling on the UK Government to ban all use of facial recognition in public spaces.[89] In 2022, a House of Lords report and a review on the governance of biometrics in England and Wales (commissioned by the Ada Lovelace Institute) both called for legislation that would provide greater clarity on the use, limits, and safeguards governing facial recognition and other AI-based biometric systems.[90]

In the wake of the *Bridges* case, the Biometrics and Surveillance Camera Commissioner (BSCC) for England and Wales and civil society has also highlighted concerns regarding wide-ranging guidance from the College of Policing,[91] which gives police services considerable discretion regarding the criteria of persons who may be placed on a watchlist for LFR use. The Commissioner has noted that the broad and general scope of such guidance means LFR is not limited to the identification of suspects but may even include potential victims on such watchlists, providing police with a level of discretion that has ‘profound’ implications for constitutional freedoms.[92] A Data Protection Impact Assessment (DPIA) published by

[86] See, for instance, Fussey and Murray, ‘Independent report’, pp. 8–9. The former Biometrics Commissioner also raised issues regarding the lack of any specific legal basis for the use of LFR systems: Office of the Biometrics Commissioner, ‘Annual Report 2017’ (2018), UK Government, p. 86.

[87] Ibid.

[88] [2020] EWHC 2341, para. 159.

[89] Liberty, ‘Resist facial recognition’ (n.d.), Online petition, https://action.libertyhumanrights.org.uk/page/50456/petition/1.

[90] House of Lords, ‘Technology rules?’, p. 31; Ryder, *Independent Legal Review*, pp. 62–67.

[91] College of Policing, ‘Authorised Profession Practice (APP) on live facial recognition’ (last updated 21 March 2022), www.college.police.uk/app/live-facial-recognition/live-facial-recognition.

[92] Alexander Martin, ‘Police warned against “sinister” use of facial recognition to find potential witnesses and not just suspects’ (4 April 2022), Sky News.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

SWP concerning their use of LFR confirms the broad criteria for those persons that may be placed on a watchlist, including witnesses and persons 'who are or *may be* victims of a criminal offence'.[93]

It is also important to stress that the standards set out by the College of Policing APP are not legally binding. They also do not constitute a statutory code of practice. In direct reference to its legal context, the APP states that its function is to provide 'direction to [police] forces that will *enable them* to ensure that their deployment of overt LFR [complies] with applicable legal requirements'.[94] An important caveat, however, for police services across England and Wales immediately follows. The APP implicitly acknowledges that such guidance is insufficient in of itself to ensure the lawfulness of LFR and proceeds to specifically advise police that they should obtain 'expert legal advice' to support their use of these systems.[95]

In terms of developing the foreseeability safeguards as part of the legality requirements of Article 8(2) ECHR, it is submitted that legislation should require law enforcement authorities using facial recognition systems to make publicly available the 'threshold value' being applied by public authorities when using these systems. Where the system has been acquired from the private sector, this information should also explain if (and why) public authorities have chosen to depart from the default threshold value set by the company that has provided any facial recognition system(s) to public authorities. Independent scientific research examining the facial recognition systems being used by SWP, and the Metropolitan Police Service,[96] has specifically stated that false positive identifications 'increase at lower face-match thresholds and start to show a statistically significant imbalance between demographics with more Black subjects having a false positive than Asian or White subjects'.[97] Thus, using a system with a lower threshold value increases the number of matching results but also increases the risk of unfair bias against certain societal groups by law enforcement, and should consequently be accompanied by the necessary justification and safeguards. Such information should also be shared in Data Protection Impact Assessments in order to alert regulators (and other independent oversight bodies) of the increased risk of bias posed towards

[93] SWP DPIA, 4–5 (emphasis added). The DPIA further states that: 'It is possible that the personal data of individuals aged under 18 years, those under 13 years, a person with a disability or vulnerable adults will be processed where there is a policing need and it is deemed to be necessary and proportionate to locate and/or safeguard these individuals.' See further www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/live-facial-recognition-documents/.

[94] College of Policing, 'Authorised profession practice', p. 5.

[95] Ibid.

[96] The largest police force in England and Wales.

[97] National Physical Laboratory, 'Facial recognition technology in law enforcement equitability study' (March 2023), NPL Report MS 43, para. 1.4.5. https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf. See further Davies, Innes, and Dawson, 'An evaluation of South Wales Police's use' and their findings and recommendations regarding false positives and threshold value settings by SWP in their trials of FRT in 2019.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press

certain groups and the safeguards being adopted by public authorities to address and mitigate these risks.

11.5 CONCLUSIONS

While some valuable guidance has been provided by the Court of Appeal in *Bridges*, which draws (albeit in a limited way) on the lauded legality case law of the ECtHR dealing with Article 8 ECHR and police investigatory powers, the current patchwork of law governing police use of facial recognition in the UK falls short of lawful and trustworthy public policy.

As the UK House of Lords rightly points out, it is not for the courts to set the framework for the deployment of new technologies. This chapter argues that the reasoning for this is threefold. First, court judgments are not systematic, comprehensive, or evidence based. Secondly, they represent ad hoc reviews of problematic public policymaking that only occur when (and if) a legal challenge is brought before them. Thirdly, the courts will assess only a narrow scope of issues relevant to that specific case. The implications posed by the lack of an accessible and foreseeable framework for police use of AFR in the UK are significant. This gap represents a source of confusion and legal uncertainty for policymakers, police, industry, courts, and citizens, thereby giving rise to gaps and patchy protection of affected rights and safeguards, including but not limited to the right to private life. These all serve to undermine adequate and effective compliance, oversight, evaluation, and thus public trust in the use of these novel and increasingly sophisticated police powers.

There is, however, a post-*Bridges* discourse on lawfulness that has moved towards enacting a law specifically tailored to regulating use of facial recognition. Such reform could address the current obscurity and uncertainty in the current patchwork of legal rules in England and Wales governing the limits and safeguards underpinning police use of facial recognition, particularly the compilation and application of watchlists. This legislation could then meet the accessibility and foreseeability tests under the legality condition of Article 8 ECHR, the 'minimum degree of legal protection' to which citizens are entitled under the rule of law in a democratic society.[98] Such reform would also enable 'greater certainty and accountability' around police use of AI-based biometric surveillance systems and other emerging technologies.[99]

[98] As held by the ECtHR in its leading case law dealing with Art. 8 ECHR, lawfulness, and police powers: *Malone v. United Kingdom* (1985) 7 EHRR 14; *Huvig v. France* (1990) 12 EHRR 528; *Valenzuela v. Spain* (1999) 28 EHRR 483.

[99] Biometrics and Surveillance Camera Commissioner, 'Annual Report'.

https://doi.org/10.1017/9781009321211.014 Published online by Cambridge University Press