Northern Ireland
Legal Quarterly
Vol. 75 No. 4 (2024) 806–817
Commentaries and Notes DOI: 10.53386/nilq.v75i4.1127

Bridges v South Wales Police and emerging privacy concerns

Te Li
Queen's University Belfast
Correspondence email: tli07@qub.ac.uk.

ABSTRACT

This article explores the landmark case of B*ridges v South Wales Police*, a pivotal legal challenge concerning the use of facial recognition technology by law enforcement. Edward Bridges, a civil liberties campaigner, contested the deployment of automated facial recognition (AFR) technology by the South Wales Police (SWP), arguing it infringed his privacy rights. The Court of Appeal of England and Wales ruled in favour of Bridges, finding that the SWP's use of AFR was unlawful and breached privacy rights under article 8 of the European Convention on Human Rights, data protection laws and equality laws. This analysis reviews the facts, legal issues and reasoning behind the court's decision, emphasising the broader implications for privacy law and the regulation of emerging technologies.

Keywords: facial recognition technology; automated facial recognition; law of privacy; article 8 of ECHR; misuse of private information; public authority.

INTRODUCTION

The case of *Bridges v South Wales Police* marks a significant moment in the legal examination of facial recognition technology (FRT) used by law enforcement.[1] Edward Bridges, a civil liberties campaigner, challenged the deployment of automated facial recognition (AFR) technology by the South Wales Police (SWP), alleging that its use in public spaces infringed on his privacy rights. On 11 August 2020, the Court of Appeal of England and Wales overturned a previous dismissal by the Divisional Court (DC), ruling that the use of AFR by the SWP was unlawful. The court found that the deployment breached privacy rights under article 8 of the European Convention on Human Rights (ECHR), violated data protection laws and failed to comply with equality laws. This note delves into the factual background of the *Bridges* case, the key legal issues raised and the detailed reasoning of the Court of Appeal. By analysing the court's decision and its implications, this

1 *R (on the Application of Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058, [2020] 1 WLR 5037.

article aims to provide a comprehensive understanding of the legal challenges associated with FRT. It also reflects on the broader impact of this judgment on the future regulation of emerging surveillance technologies and the balance between public safety and individual privacy rights.

REVIEW OF THE CASE

Factual backgrounds

Edward Bridges, the appellant, is a civil liberties campaigner residing in Cardiff. The Chief Constable of SWP, the respondent, leads the national trial of AFR technology, akin to FRT, designed for face identification and verification.[2] AFR involves six stages: 'compiling a watchlist, facial image acquisition, face detection, feature extraction, face comparison, and matching'.[3]

AFR Locate refers to a specific application or deployment of technology used by law enforcement agencies. In deployments of AFR Locate for crime prevention, digital facial images of members of the public are collected from live CCTV feeds and converted into real-time facial biometric information. This information is compared to police-uploaded watchlist data to determine if two facial images depict the same person. The SWP deployed AFR about 50 times between May 2017 and April 2019.

Two incidents were pertinent to Mr Bridges' claims. Firstly, on 21 December 2017, AFR was deployed in Cardiff with 10 possible matches, resulting in two false matches and two arrests. Mr Bridges, in close proximity, alleged the lack of obvious signage indicating that AFR was in operation.[4] Secondly, on 27 March 2018, AFR was used at the Motorpoint Arena during a defence exhibition. Although no arrests

2 AFR is an advanced technology designed for the automated identification and verification of individuals based on their facial features. It operates through a multi-stage process that includes compiling a watchlist of facial images, capturing images from live CCTV feeds, detecting faces within these images, extracting unique facial features, comparing them against a database of known individuals, and determining potential matches in real-time. AFR technology is used by law enforcement agencies and other entities for various purposes, including enhancing security, identifying suspects, and managing public safety. Its deployment has sparked significant legal and ethical debates regarding privacy rights, data protection and the regulation of surveillance technologies in public spaces.

3 *Bridges* (n 1 above) [8].

4 Ibid [26]–[27].

occurred, Mr Bridges, protesting nearby, claimed unawareness of AFR in operation and that no information was provided by SWP officers.[5]

Issues

Mr Bridges contended that due to (1) the improper application of AFR Locate against him on the two occasions detailed above and (2) the continuous use of AFR Locate in his residential area, there was an inherent heightened risk of the technology being employed against him again.

Consequently, Mr Bridges initiated a legal challenge against SWP's adoption of AFR, citing three grounds: (1) infringement of the right to respect for private life as per article 8 of the ECHR; (2) violation of data protection laws, specifically the Data Protection Acts (DPAs) 1998 and 2018; and (3) breach of the public sector equality duty (PSED) provided for in section 149 of the Equality Act 2010. This note will primarily address the first two grounds of his challenge, as they are directly relevant to privacy law.

Procedural history

This case was initially heard in the DC in Cardiff by Haddon-Cave LJ and Swift J, who dismissed Mr Bridges' judicial review claim on all grounds. The DC, in addressing the article 8 ECHR right to respect for private life, recognised the complexity of defining 'private life'[6] but held that article 8 was engaged. AFR-derived biometric data is important personal information with 'intrinsically private character',[7] and it is sufficient if biometric data is captured, stored and processed even momentarily. However, the court rejected the argument that the use of AFR by the SWP lacked a sufficient legal framework, citing existing legislation, secondary regulations and SWP policies.

The DC applied the four-stage proportionality test from *Bank Mellat*,[8] finding that the use of AFR Locate on two occasions struck a fair balance and was not disproportionate.[9] Concerning data protection claims, the DC determined that the use of AFR on two occasions met the conditions of lawfulness and fairness under the DPA 1998.[10] It

5 Ibid [29].

6 *R (on the Application of Bridges) v Chief Constable of South Wales* [2019] EWHC 2341 (Admin), [2020] 1 WLR 672, [47].

7 See *S and Marper v the United Kingdom* (2009) 48 EHRR 50 (ECtHR, 2008); *Von Hannover v Germany* (2006) 43 EHRR 7 (ECtHR 2005).

8 *Bank Mellat v Her Majesty's Treasury (No 2)* [2013] UKSC 38, 39, [2014] AC 700.

9 *Bridges* (n 6 above) [100]–[101].

10 Ibid [127].

acknowledged the issue of sensitive processing under DPA 2018, but deferred judgment on the sufficiency of the SWP's policy document.[11]

Regarding section 64 of the DPA 2018, the DC rejected Bridges' claim that the SWP had failed to conduct an impact assessment, finding that relevant assessments were in place.[12] In relation to the PSED, the DC dismissed the claim, stating that the SWP could not have predicted indirect discriminatory effects of the licensed NeoFace Watch software. The court concluded that the equality impact assessment (EIA) demonstrated the SWP's due regard to the PSED criteria.[13]

THE REASONING OF THE COURT OF APPEAL

Bridges was granted permission to appeal on five grounds, Sir Terence Etherton MR, Dame Victoria Sharp PQBD and Lord Justice Singh delivered the leading judgment:

1. The DC erred in concluding that the interference with Mr Bridges' rights under article 8(1) of the ECHR was in accordance with the law for the purpose of article 8(2) (*sufficient legal framework*).
2. The DC erred in concluding that the interference with Bridges' right within article 8(2) was not disproportionate (*proportionality*).
3. The DC wrongly held that the SWP's data protection impact assessment (DPIA) was in accordance with the requirements of section 64 of the DPA 2018 (*section 64, DPA 2018 – DPIA*).
4. The DC should not have declined to deliver a conclusion as to whether SWP had in place an 'appropriate policy document' within the meaning of section 42 of the DPA 2018 (*appropriate policy document*).
5. The DC wrongly held that SWP complied with the PSED under section 149 of the Equality Act 2010, since SWP's EIA was 'obviously inadequate' and failed to recognise the potential risk of indirect discrimination (*PSED*).

Sufficient legal framework

The DC addressed the first ground by evaluating the adequacy of the legal framework for AFR use. It concluded that AFR's use is sufficiently foreseeable and accessible, meeting the 'in accordance with the law'

11 Ibid [139]–[141].
12 *Bridges* (n 1 above) 51.
13 *Bridges* (n 6 above) [157]–[158].

requirement.[14] However, the Court of Appeal disagreed, distinguishing AFR from conventional police practices like photography or CCTV use. They highlighted AFR's novelty, its mass collection of digital information on the public, the sensitive nature of facial biometric data and its automated processing.[15]

The Court of Appeal rejected the DC's view that the legal framework was sufficient,[16] identifying 'fundamental deficiencies' in the 'who' and 'where' aspects. They argued that individual police officers had excessive discretion in determining watchlist entries and deployment locations.[17]

Analysing the legal framework layers, the court found the DPA 2018 to be crucial but insufficient alone.[18] The Surveillance Camera Code of Practice[19] should specify watchlist inclusion criteria and deployment locations. Assessing the SWP's local policy,[20] the court expressed concern about its broad categories, allowing discretion in determining watchlist entries and deployment locations. Consequently, the court allowed the appeal on this ground.

Proportionality

The issue of proportionality did not need to be considered after it had been determined that the use of AFR was not in accordance with the law. Nonetheless, the Court of Appeal chose to evaluate whether the DC's assessment on proportionality was erroneous. The appellant did not address the first three stages of the *Bank Mellat* four-stage test but contended that the DC erred in assessing whether a fair balance had been struck.

---

14 General principles summarised by the DC are (1) the impugned measure in question must meet two requirements of 'accessibility' and 'foreseeability', namely it must have 'some legal basis in domestic law' and must be 'compatible with the rule of law'; (2) accessible means that it must be published and comprehensible, foreseeable means it must be possible for a person to foresee its consequences for them and the discretion cannot be so broad that its scope relies upon the will of those who apply it; (3) the law must afford adequate legal protection against arbitrariness and sufficiently indicate the scope of discretion; (4) discretionary power does not need an over-rigid regime which does not contain the flexibility to ensure the fundamental rights being protected, it just requires safeguards that could prevent overbroad discretion resulting in arbitrariness; (5) the rules governing the scope and application of measures do not need to be statutory; (6) the requirement for reasonable predictability does not mean the law should codify answers to every issue.

15 *Bridges* (n 1 above) 84.

16 Ibid [90].

17 Ibid [91].

18 Ibid [104].

19 Home Office, 'Surveillance Camera Code of Practice' (2013/2021).

20 Ibid [123].

Regarding the benefit side of proportionality, the appellant argued that anticipated benefits,[21] not just actual results, should be considered. On the cost side, the DC only considered the impact on Mr Bridges, whereas the appellant asserted that the interference with article 8 rights should be considered for all members of the public.[22] Citing *R (Tigere) v Secretary of State for Business, Innovation and Skills*,[23] the appellant argued for a broader consideration. However, the court emphasised that human rights questions should be addressed on legal principles rather than semantics,[24] pointing out that *Tigere* dealt with a general measure affecting a group,[25] unlike *Bridges*' case which focused on specific AFR deployments.[26] The court concluded that the impact on other members of the public in analogous situations to Bridges was as negligible as on Mr Bridges, stating that an impact with little weight does not gain significance simply because others were affected.[27]

Section 64 of the Data Protection Act 2018 – data protection impact assessment

The third aspect of this appeal centred on the adequacy of SWP's comprehensive DPIA. Mr Bridges argued that the DPIA had three key shortcomings. Firstly, it failed to acknowledge that AFR involves processing the personal data of individuals not on watchlists. Secondly, it failed to recognise the engagement of article 8 rights for such individuals. Thirdly, it remained silent on potential risks triggered by AFR, including the rights to freedom of expression and assembly under articles 10 and 11 of the ECHR.[28]

Counsel for the Information Commissioner's Office (ICO) criticised the DPIA for lacking assessments on privacy, personal data and safeguards. It also failed to acknowledge AFR's collection of data on a blanket and indiscriminate basis. The DPIA overlooked the risk of false-positive results leading to prolonged retention periods instead of immediate deletion. Additionally, it failed to identify potential gender and racial bias resulting from AFR.[29]

---

21 Ibid [135].
22 Ibid [136].
23 *R (Tigere) v Secretary of State for Business, Innovation and Skills* [2015] [2015] UKSC 57, [2015] 1 WLR 3820.
24 *Bridges* (n 1 above) [139].
25 *Tigere* (n 23 above) [6].
26 Ibid.
27 Ibid [143].
28 Ibid [147].
29 Ibid [149].

The Court of Appeal recognised certain issues raised, including the DPIA's acknowledgment of article 8's relevance, but dismissed these concerns.[30] Its decision was rooted in the determination that the use of AFR was inherently unlawful as per the first ground, highlighting that the DPIA's shortcomings hindered a thorough evaluation of risks to data subjects' rights and freedoms and lacked adequate measures to mitigate these risks.[31] Therefore, the appeal on this specific ground was upheld.

Appropriate policy document

To fulfil the requirement of the first data principle, the data controller needs to satisfy the conditions outlined in section 35(5) of the DPA 2018. Specifically, the SWP was required to have an appropriate document in place when carrying out the processing. Section 42(2) of the DPA 2018 specifies the necessary contents of this document. The appellant argued that the DC was obligated to determine whether SWP's November 2018 Policy Document[32] complied with section 42, and also argued that the DC should have found that it did not.[33] The court rejected this argument, stating that the two instances of AFR deployment took place before the official enforcement of the DPA 2018, and there was no alleged failure to comply with the DPA 1998.[34] Moreover, the policy document is considered to be an evolving document, and controllers are duty-bound to periodically review and update it in accordance with section 42(3) of the DPA 2018. At the time of the DC hearing, the ICO had not issued guidance on the contents of the section 42 document. The ICO considered that the November 2018 Policy Document ideally should be more detailed but satisfied section 42(2).[35] The court deemed it appropriate for the DC not to make a final judgment, allowing the SWP the opportunity to revise its document in light of future guidance from the ICO.

The public sector equality duty

The Court of Appeal held that no satisfactory response to the challenge based on the PSED had been provided. There had been no analysis of 'the racial or gender profiles of the total number of people who were captured by the AFR but whose data was then almost immediately

30 Ibid [151].
31 Ibid [153].
32 Cited in *Bridges* (n 1 above) [50] and see the SWP's Policy on Sensitive Processing for Law Enforcement Purposes, under Part 3 Data Protection Act 2018 (September 2022).
33 *Tigere* (n 23 above) [157].
34 Ibid [159].
35 Ibid [161].

deleted'.[36] Dr Anil Jain, in his witness statement, highlighted the impact of various variables, including 'training datasets', on the performance of AFR technology. He underscored that 'the accuracy of an AFR system depends to a considerable extent on the training dataset'.[37] Concerning the NeoFace Algorithm used by the SWP, Dr Jain stated that:

> he cannot comment on whether AFR Locate has a discriminatory impact, simply because he did not have access to the datasets on which the system is trained. A thorough evaluation needs to be done of the demographic composition of the NeoFace algorithm training dataset to determine whether the training dataset is biased or may be.[38]

The court concluded that as the SWP did not take reasonable steps to check if the software has an unacceptable level of bias, the PSED was not satisfactorily fulfilled.

The Court of Appeal allowed the appeal on grounds (1), (3) and (5) but dismissed grounds (2) and (4). The SWP has confirmed it will not appeal the decision, making the Court of Appeal's judgment final.

COMMENTARY

Bridges marks the world's first legal challenge related to FRT. The significance of this judgment can be assessed from three key perspectives. Firstly, *Bridges* transcends the mere examination of FRT's legality; it introduces a constructive legal strategy. This strategy aims not only to establish the lawfulness of FRT but also to propose a framework aligning it with article 8 rights and DPA law. Consequently, public authorities are prompted to reconsider the existing legal framework for AFR, revisiting policies, reassessing DPIA adequacy and retesting the inherent biases of AFR software. The deficiencies in the current legal framework may necessitate parliamentary intervention.

Secondly, the judgment identifies two crucial legal shortcomings – the 'who question' and the 'where question'. These deficiencies, by expanding police discretion, can have detrimental effects on society, adversely impacting law-abiding citizens and potentially eroding public support, leading to the 'de-legitimisation of police'.[39] The recognition that legal predictability does not require codified answers to every conceivable situation acknowledges the broad and varied nature of

36 Ibid [191].

37 Ibid [193].

38 Ibid [197]–[198].

39 Ben Bowling and Coretta Phillips, 'Disproportionate and discriminatory: reviewing the evidence on police stop and search' (2007) 70(6) Modern Law Review 936–961.

policing.[40] Excessive legal constraints might alter the essence of policing, diminishing its effectiveness, particularly in responding to serious crimes and terrorism.

Thirdly, post-*Bridges*, the SWP affirmed its intention to continue using FRT after addressing specific defects highlighted by the Court of Appeal.[41] The Surveillance Camera Commissioner (SCC), disputing the Court of Appeal's judgment's fatal impact on FRT, suggested ministers refrain from any 'self-generated' plan to merge the roles of SCC and the Biometric Commissioner into a single commission.[42] The Court of Appeal's decision marks the commencement, rather than the conclusion, of legal standards challenging AFR. Commissioners should conduct an independent review of the legal framework governing overt surveillance.

The focal point of *Bridges* revolves around determining whether the existing legal framework in the United Kingdom (UK) effectively prevents the arbitrary use of AFR through police discretionary authority. The Court of Appeal's judgment, influenced by certain objective factors, did not encompass all facets of FRT. Consequently, this note highlights specific issues that merit additional scrutiny and consideration.

The uniqueness of the facial recognition technology and the reasonable expectation of privacy

Firstly, as the court noted, 'bias has been found to be a feature of common AFR systems'.[43] Without a specific dataset, the Court of Appeal emphasised the SWP's failure to fulfil the PSED to assess whether the demographic composition of the training dataset is biased. However, the judgment did not discuss whether the AFR technology itself is intrusive or biased, and to what extent the manufacturers can eliminate such inbuilt bias. Indeed, this raises interesting questions about new technologies and administrative law – do supposedly impartial systems incorporate biases?[44]

---

40 *R (on the Application of Catt and Others) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] UKSC 9, [2015] AC 1065, [11].

41 'Response to the Court of Appeal Judgment on the Use of Facial Recognition Technology' (11 August 2021).

42 'Surveillance Camera Commissioner's Statement: Court of Appeal Judgment (R) Bridges v South Wales Police – Automated Facial Recognition' (*Gov.UK* 11 August 2020).

43 *Bridges* (n 1 above) [197].

44 See Jennifer Cobbe, 'Administrative law and the machines of government: judicial review of automated public-sector decision-making' (2019) 39 Legal Studies 636–655.

Regarding the use of FRT, in *Bridges*, the court's reasoning was mainly based upon the authority of *S v UK*,[45] that article 8 will be engaged once an individual's personal data has been stored by the police. The court did not assess in the context of the deployment of the FRT, whether Bridges had a reasonable expectation that his facial biometrics would be stored, processed and further discarded. An anonymised person in a public place may still have a reasonable expectation of privacy in respect of information like name, home address and so on. Likewise, even though Bridges knowingly and intentionally involved himself in activities that might be recorded by the surveillance technology, he should have foreseen that his facial appearance would be observed by passers-by, the police and even CCTV, but Bridges still enjoyed a reasonable expectation that his biometric information behind the face would not be stored and processed, especially in the context that: a) he was of good character and was not engaged in any reprehensible or criminal activities; b) the intrusive nature of the FRT; and c) the sensitivity of biometric data.

Proportionality issue

Mr Bridges' core argument on the proportionality issue is the DC's failure to consider the cumulative interference with the privacy rights of all those whose facial biometrics were captured as part of the deployment of FRT. The Court of Appeal separated *Bridges* from challenges to 'a general measure, for example a policy or a piece of legislation', such as in *Tigere*, where the Supreme Court considered the criteria for eligibility for student loans.[46] A case concerned with 'general measure' will require the court to balance 'the impact on every person who is affected by the measure and the interest of the community'.[47] However, the Court of Appeal did not accept the use of FRT as a general measure, but chose merely to assess the impact of FRT on Mr Bridges himself, especially two deployments of FRT on two specific occasions. The Court of Appeal's conclusion was based on the specific facts and grounded in the infringement of Mr Bridges' article 8 rights. Thus, as Purshouse and Campbell have stated, 'it is regrettable that the ground on proportionality was not framed in more general terms'.[48] And the courts did not really come close to the core debate over the use of FRT and consider the wider societal impact it brings.

It would have been very interesting if the Court of Appeal had considered the use of FRT as a general measure to further assess its

45 *S v UK* (n 7 above) [50].

46 *Tigere* (n 23 above) [1].

47 *Bridges* (n 1 above) [140].

48 Joe Purshouse and Liz Campbell, 'Automated facial recognition and policing: a bridge too far?' (2022) 42(2) Legal Studies 209–277, 223.

general impact as, firstly, its use affected not only Mr Bridges but also anyone who was present in particular places in Cardiff during particular times. Although FRT identifies targeted people based upon the specified watchlist, its way of collecting public biometric data *en masse* is still general and unselected. According to Strasbourg jurisprudence, 'a wide margin of appreciation is usually allowed to the state under the Convention when it comes to general measures of political, economic or social strategy, and the court generally respects the legislature's policy choice unless it is "manifestly without reasonable foundation"'.[49] Thus, if the use of FRT as a general measure had been considered, the likelihood is not high that the court would have found a breach of the Convention.

The Court of Appeal stated that 'this was not a question of simple multiplication, but rather an exercise of judgment'.[50] However, the controversial aspect lies in the court's omission to expound on the nature of such judgment and why considering others affected by the measure is not characterised as 'simple multiplication'. Alternatively, one could argue that Parliament might be better positioned to assess the broader impact of FRT than the court.[51] It is pertinent to note that a Bill seeking to prohibit the use of automated FRT in public spaces is currently undergoing its second reading in the House of Lords. The existing scenario places significant discretion in the hands of public authorities, who may not be the most suitable entities to determine whether the use of FRT strikes a fair balance.

Moreover, irrespective of the court's evaluation of Mr Bridges' personal experience, a crucial inquiry remains regarding the extent to which the proportionality of future FRT use can be adequately assessed solely by referencing its impact on a single individual.

Bridges draws clear parameters as to use, regulation and scrutiny of AFR. From a wider perspective, we may consider how the algorithm of law can catch up with new emerging technologies promptly, namely, whether there should be a specific legal framework for the police (or the other data controllers) to routinely deploy novel biometrics including AFR but also voice recognition, gait analysis, iris analysis or other new biometric technologies as they emerge.[52] The European Union Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) has already published detailed guidelines on using

49 See *Stec v UK* [2006] 43 EHRR 47, [52].

50 *Bridges* (n 1 above) [143].

51 Purshouse and Campbell (n 48 above) 224.

52 Biometrics Commissioner, 'Automated facial recognition' (*Gov.UK* 10 September 2019).

FRT,[53] and the European Commission similarly issued a White Paper on 'Artificial intelligence: a European approach to excellence and trust', which situated FRT in a broader context of technological change.[54] We may also wonder if it is true that, when laws and regulations develop constraints for each aspect of new emerging technologies, those technologies can then be used absolutely safely.

CONCLUSION

In conclusion, the *Bridges* case signifies a critical juncture in the legal scrutiny of emerging technologies, particularly in the realm of civil liberties and privacy. The judgment's multifaceted implications extend beyond the immediate concerns of the appellant, Edward Bridges, to broader considerations of societal impact, legal frameworks and the evolving landscape of technological surveillance. While the Court of Appeal has offered clarity on certain legal deficiencies, fundamental questions persist regarding the intrusive nature of FRT, the adequacy of regulatory frameworks, and the need for comprehensive legislative guidance in governing novel biometric technologies. As technology continues to advance, this case sets a precedent for ongoing debates surrounding the intersection of individual rights, law enforcement practices, and the regulatory response to rapidly evolving technologies.

53 'Guidelines on facial recognition' (*Council of Europe* 28 January 2021).

54 See 'Artificial intelligence: a European approach to excellence and trust' (European Commission COM(2020)65 final 19 February 2020) and the European Data Protection Supervisor response at Opinion 4/20 (29 June 2020).