University of New South Wales Law Research Series

BURNING BRIDGES: THE AUTOMATED FACIAL RECOGNITION TECHNOLOGY AND PUBLIC SPACE SURVEILLANCE IN THE MODERN STATE

MONIKA ZALNIERIUTE

Forthcoming (2021) Columbia Science and Technology
Law Review
[2021] *UNSWLRS* 39

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

BURNING *BRIDGES*: THE AUTOMATED FACIAL RECOGNITION TECHNOLOGY AND PUBLIC SPACE SURVEILLANCE IN THE MODERN STATE

MONIKA ZALNIERIUTE[*]

ABSTRACT

A live automated facial recognition technology, rolled out in public spaces and cities across the world, is transforming the nature of modern policing. In R *(on the application of Bridges) v Chief Constable of South Wales Police,* decided in August 2020 ('*Bridges*') – the first successful legal challenge to automated facial recognition technology worldwide - the Court of Appeal in the United Kingdom held that the use of automated facial recognition technology by the South Wales Police was unlawful. This landmark ruling can set a precedent and influence future policy on facial recognition in many countries. *Bridges* decision imposes some limits on the previously unconstrained police discretion on whom to target and where to deploy the technology. Yet, while the decision demands a clearer legal framework to limit the discretion of police

[*] Senior Lecturer, and Australian Research Council Discovery Early Career Research Award Fellow (project number DE210101183), Faculty of Law & Justice, UNSW Sydney), Leader of 'AI and Law' research stream, Allens Hub for Technology, Law and Innovation, m.zalnieriute@unsw.edu.au. I would like to thank Frank Pasquale at Brooklyn Law School, Thomas Streinz at NYU, Lee Bygrave at University of Oslo, Graham Greenleaf and Lyria Bennett Moses at UNSW Sydney, Christopher Kuner at Vrije Universiteit Brussel, Megan Richardson and Andrew Kenyon at University of Melbourne, Monique Mann at Deakin University, Angela Daly at University of Strathclyde, Nicolas Suzor at QUT, Alexander Trechsel at University of Lucerne and Giovanni Sartor at European University Institute for the invaluable input and feedback on the development of these ideas and earlier drafts. I also thank Jacob Silove and Inderpreet Kaugh Singh for their excellent research assistance.

who use such technology, it does not, in principle, oppose the use of facial recognition technology for mass-surveillance in public places, nor for monitoring political protests. To the contrary, the Court accepted that the use of automated facial recognition in public spaces to identify very large numbers of people and to track their movements is proportional to law enforcement goals. Thus, the Court dismissed the wider impact and significant risks posed by using facial recognition technology in public spaces; it underplayed the heavy burden placed on democratic participation and the rights to freedom of expression and association, which require collective action in public spaces. Neither did the Court demand transparency about the technologies used by the police force, which is often shielded behind the 'trade secrets' by the corporations who produce them, nor did the Court act to prevent fragmentation and inconsistency between local police forces' rules and regulations on automated facial recognition technology, which leaves the law less predictable. Thus, while the *Bridges* decision is reassuring and demands change in the discretionary approaches of UK police in the short term, its long-term impact in burning bridges between the expanding public space surveillance infrastructure and the modern state is less certain.

CONTENTS

M. Zalnieriute, 'Burning Bridges: Facial Recognition Technology and Public Space Surveillance in the Modern State', *Columbia Science and Technology Law Review,* 2021 Vol 22(2), pp. *forthcoming*

BURNING *BRIDGES*: THE AUTOMATED FACIAL RECOGNITION TECHNOLOGY AND PUBLIC SPACE SURVEILLANCE IN THE MODERN STATE

'[T]he Court has agreed that facial recognition clearly threatens our rights. This technology is an intrusive and discriminatory mass surveillance tool… We should all be able to use our public spaces without being subjected to oppressive surveillance'[1] – Edward Bridges, 2020

"We will continue our deployment and development of the technology when we have satisfied ourselves that we can meet the specific points identified in the conclusions of the Court of Appeal, and that work is underway as we now consider the comprehensive judgment."[2] – South Wales Police, 2020.

1 Introduction

A live automated facial recognition technology, rolled out in public spaces and cities across the world, is transforming the nature of modern policing in liberal democracies and authoritarian regimes alike. The technology augments traditional surveillance methods by detecting and comparing person's eyes, nose, mouth, to skin textures, shadows to identify individuals.[3] The live automated facial

[1] Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech, LIBERTY (2020), https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech/ (last visited Sep 15, 2020).

[2] South Wales Police, *Facial Recognition* 4 (2020), https://afr.south-wales.police.uk/wp-content/uploads/2020/08/AFR-updated-briefing-and-QA-Aug20.docx (last visited Oct 16, 2020).

[3] Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, Forthcoming 2021 MINN. LAW REV., 6; Jagdish Chandra Joshi & K K Gupta,

recognition can instantaneously assess the facial biometric data in the captured images against a pre-existing 'watchlist' and flag it to the police officers.

Facial recognition technologies have been used by police, often in combination with the CCTV cameras, without a legal framework governing its discretion in the United Kingdom ('UK') and other countries for many years. Train stations, airports, and city squares are increasingly equipped with facial recognition technologies in the United States of America ('USA'), China, France and Hong Kong, among other nations. For example, in the UK, at least four police departments (Leicestershire Police, South Wales Police, the Metropolitan Police Service, and Humberside Police.[4]) have experimented with the technology by linking it to CCTV cameras.[5] Across the UK, there are an estimated 5.9 million CCTV cameras,[6] and the country ranks 3rd in the number of cameras per 100 people after the US and China.[7] Meanwhile, London ranks 8th in a list of the most surveilled cities in the world (ranks 1 to 7 are made of up

Face Recognition Technology: A Review, 1 IUP J. TELECOMMUN. 53, 53–54 (2016); Relly Victoria Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 J. MECHATRON. ROBOT. 237, 240 (2019); Mary Grace Galterio, Simi Angelic Shavit & Thaier Hayajneh, *A Review of Facial Biometrics Security for Smart Devices*, 7, 37 COMPUTERS, 3 (2018); IAN BERLE, FACE RECOGNITION TECHNOLOGY: COMPULSORY VISIBILITY AND ITS IMPACT ON PRIVACY AND THE CONFIDENTIALITY OF PERSONAL IDENTIFIABLE IMAGES (2020).

[4] Henriette Ruhrmann, *Facing the Future: Protecting Human Rights in Policy Strategies for Facial Recognition Technology in Law Enforcement* 35 (2019), https://citrispolicylab.org/wp-content/uploads/2019/09/Facing-the-Future_Ruhrmann_CITRIS-Policy-Lab.pdf (last visited Jun 1, 2020).

[5] INFORMATION COMMISSIONER'S OPINION: THE USE OF LIVE FACIAL RECOGNITION TECHNOLOGY BY LAW ENFORCEMENT IN PUBLIC PLACES, 6 (2019), https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf (last visited May 14, 2020).

[6] One surveillance camera for every 11 people in Britain, says CCTV survey - Telegraph, , https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html (last visited May 6, 2020).

[7] Source: PreciseSecurity.com & Comparitech, *Report finds the US has the largest number of surveillance cameras per person in the world*, TECHSPOT , https://www.techspot.com/news/83061-report-finds-us-has-largest-number-surveillance-cameras.html (last visited May 6, 2020).

of cities in China).[8] English capital was one of the first cities to link CCTV cameras to facial recognition technologies in the late 1990s;[9] and their use further intensified following the 9/11 to address the perceived new threat of terrorism.[10] Today, facial recognition technologies can identify a suspect in a city with population of over 3 million people within just 7 minutes.[11] Yet, despite the increasing use of facial recognition technology in modern policing, there is no comprehensive regulatory framework overseeing its use in the UK.[12]

In R *(on the application of Bridges) v Chief Constable of South Wales Police* ([2020] EWCA Civ 1058) *('Bridges')* the Court of Appeal held that the use of automated facial recognition technology by the South Wales Police Force was unlawful because it was not "in accordance with law" for the purposes of Article 8 of the European Convention on Human Rights ('ECHR').[13] In addition, the South Wales Police had failed to carry out a proper Data Protection

[8] Paul Bischoff, *Surveillance camera statistics: which cities have the most CCTV cameras?*, COMPARITECH (2019), https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

[9] REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS, 79 (2020).

[10] James Meek, *Robo cop*, THE GUARDIAN, June 13, 2002, https://www.theguardian.com/uk/2002/jun/13/ukcrime.jamesmeek (last visited May 12, 2020); RHODRI JEFFREYS-JONES, WE KNOW ALL ABOUT YOU: THE STORY OF SURVEILLANCE IN BRITAIN AND AMERICA 183 (1st edition OUP ed. 2017).

[11] Jon Russell, *China's CCTV surveillance network took just 7 minutes to capture BBC reporter*, TECHCRUNCH (2017), https://social.techcrunch.com/2017/12/13/china-cctv-bbc-reporter/ (last visited Jul 31, 2020).

[12] See, eg, PAUL WILES, *Commissioner for the Retention and Use of Biometric Material - Annual Report* 2 (2020) noting that no "second-generation" biometrics (such as facial images, live facial matching, voice recognition, and gait analysis) are covered by legislation governing the police use of biometrics (the Protection of Freedom Act 2012, also known as PoFA); See also INDEPENDENT ADVISORY GROUP ON THE USE OF BIOMETRIC DATA IN SCOTLAND, 10–12 (2018) which recommends the establishment of a Scottish Biometrics Commissioner, as well as a Code of Practice to govern the use of biometrics.

[13] *R (on the application of Edward Bridges) v The Chief Constable of South Wales Police, , 210 (2020).*

Impact Assessment and had not complied with the public sector equality duty.[14]

Bridges is the first successful legal challenge to police use of automated facial recognition technology in the UK and worldwide. Fresh lawsuits brought by NGOs in the USA[15] and France[16] are still pending, and they might provide different judicial responses to regulation of police use of facial recognition technology. Some US cities, such as of San Francisco, and Berkeley have banned the use of facial recognition technology by local agencies, including transport authority and law enforcement,[17] some municipalities in Massachusetts banned government use of facial recognition data in their communities,[18] while some US States (California, New Hampshire, and Oregon) have instituted bans on facial-recognition

[14] *Id.* at 210.

[15] American Civil Liberties Union v United States Department of Justice, (2019); In October 2019 the American Civil Liberties Union (ACLU) brought an action against the US Department of Justice, the FBI, and the Drug Enforcement Agency, claiming that the public had a right to know when facial recognition software was being utilised under the Freedom of Information Act. The case was filed after the ACLU made a freedom of information request in January of 2019. The DoJ, FBI, and DEA failed to produce any responsive documents ACLU Challenges FBI Face Recognition Secrecy, , AMERICAN CIVIL LIBERTIES UNION , https://www.aclu.org/press-releases/aclu-challenges-fbi-face-recognition-secrecy (last visited Jun 1, 2020).

[16] Conseil D'état, , https://www.laquadrature.net/wp-content/uploads/sites/8/2020/08/LQDN-REQ-TAJ-02082020.pdf (last visited Oct 20, 2020).

[17] San Francisco Bans Facial Recognition Technology - The New York Times, , https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html (last visited Oct 8, 2019); The decision was made by the Board of Supervisors, who stated that the responsibility to regulate facial recognition technology will lie first with local legislators who have the capacity to move more quickly than the Federal government Kate Conger, Richard Fausset & Serge Kovaleski, *San Francisco Bans Facial Recognition Technology*, N. Y. TIMES (2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

[18] Christopher Jackson et al., *Regulation of Facial Recognition Systems at the Municipal Level* 3 (2020), https://escholarship.org/uc/item/7qp0w9rn.

technology used in conjunction with police body cameras.[19] UK also has an *Automated Facial Recognition Technology (Moratorium and Review) Bill*,[20] proposing to ban the use of technologies in the UK, yet its future remains uncertain.

In such climate, the *Bridges* decision by the Court of Appeal imposed limits on the relatively unrestrained expansion of police use facial recognition technologies in the UK.[21] Up to *Bridges,* the automated facial recognition in the UK had been used without any constraints on police discretion on who to target and where to deploy such technology. In light of absence of judicial precedent on this point in many jurisdictions,[22] and the implicit approval by superior courts in others,[23] this judgment is an important turning point in legal discourse on the presumptive use of sophisticated technologies for biometric analysis in modern policing.

[19] Max Read, *Why We Should Ban Facial Recognition Technology*, INTELLIGENCER (2020), https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html (last visited Jun 1, 2020); California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams | ACLU of Northern CA, , https://www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams (last visited Jun 1, 2020).

[20] Lord Clement-Jones. 2019. Automated Facial Recognition Technology (Moratorium and Review) Bill [HL] 2019-20. <https://services.parliament.uk/bills/2019-20/automatedfacialrecognitiontechnologymoratoriumandreview.html/>accessed 23 October 2020.

[21] Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech, *supra* note 1.

[22] For an analysis of whether the US Constitution would find impermissible the police use of FRT, in the absence of actual caselaw on this point, see Julian Murphy, *Chilling: The Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests*, 75 WASH. LEE LAW REV. ONLINE 1–32 (2018).

[23] See, eg, Supreme Court of India, Justice K.S. Puttaswamy (Retd.) v Union of India (2018) where the Supreme Court of India held that the Indian government could make compulsory the use of the "Aadhaar" authentication system, which incorporates facial recognition technology, in accessing government schemes and benefits. while the case is not about police of technology, but the government bodies more generally.

Yet, despite the civil society hype around the decision's far reaching impact,[24] the Court accepted that deploying automated facial recognition in public spaces to identify very large numbers of people and to track their movements is *in principle* proportional to the law enforcement goals. While the judgment insists on a clearer articulation of limits on police discretion while using such technology, the decision does not, *in principle,* oppose the use of automated facial recognition technology for mass-surveillance in public places. The Court dismissed the wider impact and significant risks posed by automated facial recognition technology use in public spaces as 'hypothetical'; it underplayed the heavy burden the public place surveillance has on population as a whole, democratic participation and the rights to protest, which require collective action in public spaces. Nor did the Court demand transparency about the technologies used by the police, which are often shielded behind the 'trade secrets' of the corporations who produce them. Thus, while the *Bridges* decision insists on a change in the discretionary approaches by the police in the UK in the short term, its long-term impact on constraining the expanding public space surveillance infrastructure of the modern state is less certain.

The remainder of this article is structured as follows. Part II of this note provides the factual and legal background of the case, while Part III focuses on the Court of Appeal's *Bridges* decision, and explains its reasoning. Part IV outlines at the impact of mass surveillance in cities across the world, facilitated by the use of facial recognition technology, on political participation, which emphasises the rather formalistic nature of the Court's pronouncement. Part V then looks at the Court's limited pronouncement on the potential for discrimination and the actual operation of automated facial recognition technologies veiled behind trade secrets, arguing that in practice, the judgment will have little impact. Part VI zooms to the potential fragmentation and *ad hoc* regulation of automated facial recognition technologies in the future.

[24] Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech, *supra* note 1.

PART I SETTING THE SCENE

2 Factual and Legal Background

The *Bridges* case concerned a live automated facial recognition technology, called 'AFR Locate' which establishes a live feed by using a facial recognition-enabled camera in a certain location, and instantly assesses the facial biometric data in the captured images against a pre-existing database (or 'watchlist') of photographs.[25] If no match registers, the data is deleted immediately.[26] If a match is registered, then a police officer reviews the match, before determining whether to stage an intervention.[27] Facial recognition technology relies on a machine learning software, which 'learns' to recognise facial features and match biometrics from training datasets, which are large databases containing facial photographs of people who have been arrested. Arrest rates in the UK are 3.2 times higher for people of African origin than Caucasians, as Home Office published data shows.[28] Therefore, facial recognition databases often over-represent ethnic minorities.[29]

Between 2016 and 2018, the South Wales Police was awarded 2.6 million pounds for an automated facial recognition technology pilot programme.[30] The South Wales Police overtly deployed the 'AFR Locate' in a pilot scheme on about 50 occasions between May 2017 and April 2019 at a variety of public events, such as protests, royal visits, and music concerts and sporting events to identify

[25] BRIDGES (APPEAL), *supra* note 13 at [8]–[9].

[26] *Id.* at [17].

[27] *Id.* at [15].

[28] Arrests, , https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/number-of-arrests/latest (last visited Jun 11, 2020).

[29] Ruhrmann, *supra* note 4 at 41.

[30] Big Brother Watch, *Face Off: The Lawless Growth of facial recognition in UK policing* 28 (2018), https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf (last visited Jun 11, 2020).

individuals who were "wanted on suspicion for an offence, wanted on warrant, vulnerable persons and other persons where intelligence [was] required".[31] It is estimated that around 500,000 faces may have been scanned.[32] Despite being programmed to identify a pre-specified list of people, the technology collected biometric data indiscriminately. Therefore, the vast majority of faces scanned were not of persons flagged on a watchlist, and the images were automatically deleted.

In October 2018, with the support of the UK non-governmental organisation Liberty, civil society activist Edward Bridges filed a claim for judicial review, arguing that the use of automated facial recognition by the South Wales Police violated his right to privacy and private life under Article 8 of the ECHR, and breached both the UK data protection law[33] and the public sector equality duty.[34] Edward Bridges claimed to have been in the proximity of the automated facial recognition technology on two occasions: in the automated facial recognition-equipped van in the city centre of Cardiff on the 21st December 2017,[35] and on 27 March 2018, where he attended a protest against the UK Defence Exhibition of arms at Motorpoint Arena, where automated facial recognition was deployed at the entrance.[36] The initial legal challenge also included an explicit claim that the 'AFR Locate' deployment infringed

[31] South Wales Police, *Deployments | What is AFR? | AFR | South Wales Police*, WHAT IS AFR? | AFR | SOUTH WALES POLICE , http://afr.south-wales.police.uk/#deployments (last visited May 16, 2020); South Wales Police, *All Deployments*, http://afr.south-wales.police.uk/cms-assets/deployments/uploads/All-Deployments.pdf (last visited May 16, 2020).

[32] BRIDGES (APPEAL), *supra* note 13 at [16].

[33] Breaches of sections 4(4), 35(1) (requirement to comply with data protection principles) and 64 (requirement to carry out a data protection impact assessment) of the Data Protection Act 2018 *Id.* at [32].

[34] *Id.* at [32].; Bridges, R (On application of) v The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), , [18]-[21] (2019), https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf (last visited Jun 10, 2020).

[35] BRIDGES (APPEAL), *supra* note 13 at [26]-[27]; BRIDGES, *supra* note 34 at [11]-[12].

[36] BRIDGES (APPEAL), *supra* note 13 at [28]-[30]; BRIDGES, *supra* note 34 at [13]-[16].

Bridges' rights to freedom of expression, assembly and association under Articles 10 and 11 of the ECHR, but it was not pursued before the High Court.[37]

In September 2019, the High Court dismissed Bridges' claim, determining that the use of automated facial recognition was both in "accordance with the law", as well as necessary and proportionate to achieve South Wales Police's statutory obligations.[38] The High Court also dismissed Bridges' claims under the *UK Data Protection Act 2018* for the same reason, and rejected Bridges' assertion that the South Wales Police had not complied with its obligations to foster non-discrimination and equality of opportunity, as prescribed by the *Equality Act 2010*.[39] The Court thus concluded that "the current legal regime is adequate to ensure the appropriate and non-arbitrary use of AFR Locate, and that SWP's use to date of AFR Locate has been consistent with the requirements of the *Human Rights Act*, and the data protection legislation".[40]

In June 2020, the Court of Appeal heard Ed Bridges' appeal against the decision on five grounds: first, that the High Court erred in concluding that the appellant's right to privacy under Article 8(1) of the ECHR interfered with by the use of automated facial recognition was 'in accordance with the law' for the purposes of Article 8(2); second, that the High Court erred in assessing whether the use of 'AFR Locate' was a proportionate interference with Article 8 rights by reference to only the two occasions on which the appellant was profiled, as opposed to considering the cumulative interference occasioned on *all* people who were profiled on those occasions; third, that the High Court was wrong to hold that the South Wales Police's Data Protection Impact Assessment complied with statutory requirements; fourth, that the High Court erred in declining to opine on whether the South Wales Police had an appropriate policy document to comply with its data

[37] BRIDGES (APPEAL), *supra* note 13 at [32]–[33].

[38] BRIDGES, *supra* note 34.

[39] EQUALITY ACT, 149 (2010); BRIDGES, *supra* note 34 at [149]-[158].

[40] BRIDGES, *supra* note 34 at [159].

protection duties; and fifth, that the High Court was wrong to hold that the South Wales Police complied with its public sector equality duty, particularly in light of the possible indirect discrimination arising from using 'AFR Locate'. [41]

3 The Decision of the Court of the Appeal

On the 11th of August 2020, the Court of Appeal overturned the High Court's determination, finding in favour of the appellant on three grounds, by holding that the South Wales Police's use of automated facial recognition was not in accordance with law for the purpose of Article 8(2) of the ECHR (ground 1), that the Data Protection Impact Assessment did not comply with the *Data Protection Act 2018* (ground 3), and that the South Wales Police failed to satisfy its public service duty under section 149 of the Equality Act 2010 in not recognising the risk of a disproportionate impact upon women and minorities of the AFR technology (ground 5).[42]

First, the Court found "fundamental deficiencies" in the legal framework governing the use of automated facial recognition, declaring its use *not* in accordance with law. The Court remarked that automated facial recognition was a novel technology involving the automated processing of sensitive personal data, which distinguished it from other cases, such as *S and Marper vs UK* (on blanket retention of fingerprints and DNA records),[43] and *Catt* (the collection, retention and use of personal data about an individual on a secret 'extremism database').[44] The Court found that the existing framework gave too much discretion to individual police officers to determine which individuals were placed on watchlists and where AFR Locate could be deployed.[45] *The Surveillance Camera*

[41] BRIDGES (APPEAL), *supra* note 13 at [53].

[42] *Id.* at [209]-[210].

[43] *S and Marper v United Kingdom ECHR 1581, (2008).*

[44] R (Catt) v Association of Chief Police Officers, , AC 1065 (2015); BRIDGES (APPEAL), *supra* note 13 at [65]–[81], [86]–[90].

[45] BRIDGES (APPEAL), *supra* note 13 at [91].

Code of Practice,[46] and South Wales Police local policies, did not contain limitations as to who can be put on a watchlist, or where the AFR can be deployed.[47] The Court commented that "the current policies do not sufficiently set out the terms on which discretionary powers can be exercised by the police and for that reason do not have the necessary quality of law."[48] The Court further described the discretion as "impermissibly wide",[49] because, for example, the deployment of the technology was not limited to areas in which it could reasonably be thought that individuals on a watchlist might be present.[50] The Court implied that this should be a significant factor in determining where AFR Locate should be deployed, stating, "it will often, perhaps always, be the case that the location will be determined by whether the police have reason to believe that people on the watchlist are going to be at that location."[51] Therefore, the appeal succeeded on the first ground that the use of AFR was not in accordance with the law for the purposes of Article 8(2) of the ECHR.[52]

Given that the use of automated facial recognition was ruled unlawful, it was not necessary for the Court to decide the second ground of appeal, regarding the proportionality of the automated facial recognition use. Yet, in an unexpected move, the Court went beyond its strict mandate to address this ground. It held that the High Court had correctly weighted the balance between the actual and anticipated benefits of AFR Locate on the one hand, and the impact of deploying automated facial recognition on Mr Bridges, on the other hand. Mr Bridges specifically argued that the balancing test between the rights of the individual and the interests of the community, which forms part of the proportionality analysis,

[46] Home Office, *Surveillance Camera Code of Practice* (2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf (last visited Oct 20, 2020).

[47] BRIDGES (APPEAL), *supra* note 13 at [109]-[130].

[48] *Id.* at [94].

[49] *Id.* at [152].

[50] *Id.* at [130].

[51] *Id.* at [96].

[52] *Id.* at [210].

should not only consider the impact on Mr. Bridges, but also the impact on all other individuals whose biometric data was processed by the technology on the relevant occasions.[53] The Court of Appeal disagreed, noting that Mr. Bridges had only articulated the impact on himself, not the wider public, in his original complaint.[54] Further, according to the Court, the impact on Mr Bridges was 'negligible' and "an impact that has very little weight cannot become weightier simply because other people were also affected".[55] The balancing exercise, according to the Court, "is not a mathematical one; it is an exercise which calls for judgement."[56] The benefits were potentially great, and the impact on Mr Bridges was minor, and so the use of AFR was proportionate under Article 8(2).[57] For the Court it was also important that the police "did all that could reasonably be done to bring to the public's attention that AFR Locate was being deployed at a particular place at a particular time".[58] The ground of proportionality, should it have been necessary to decide, would thus have failed in the appeal.

The Court then moved on to address the third ground of appeal, relating to South Wales Police's failure to carry out a sufficient data protection impact assessment. The Court rejected the bulk of the applicant's arguments on the assessment's deficiency – namely, that the assessment did not acknowledge that personal data which was deleted was still 'processed' within the meaning of data protection law, that the assessment did not acknowledge the rights of individuals under Article 8 of the European Convention on Human Rights were engaged, nor the risks to freedom of expression and assembly.[59] Nonetheless, the Court agreed with Mr Bridges that the South Wales Police's data protection impact assessment was deficient because of their failure in establishing the correct legal framework for using automated facial recognition.

[53] *Id.* at [136]–[137].

[54] *Id.* at [142].

[55] *Id.* at [143].

[56] *Id.* at [143].

[57] *Id.* at [143].

[58] *Id.* at [70].

[59] *Id.* at [147]-[151].

The Court noted that the assessment "proceed[ed] on the basis that Article 8… is not infringed", and therefore, failed to properly address the need to be "in accordance with the law".[60] The Court concluded that "the inevitable consequence of those deficiencies is that… the DPIA failed properly to assess the risks to the rights and freedoms of the data subjects" and consequently breached section 64 of the Data Protection Act 2018.[61]

The Court next addressed the fourth ground of appeal, quickly dismissing it. The issue related to Section 42 of the *Data Protection Act 2018*, which sets out what an appropriate policy document relating to data protection matters must contain. However, this provision had not been enacted at the time of the two occasions on which the appellant was captured by 'AFR Locate',[62]and the ground was rejected.

Finally, the Court addressed Bridges' complaint that the South Wales Police breached their positive duty to have 'due regard' to eliminating potential bias and indirect discrimination associated with automated facial recognition technology.[63] The South Wales Police were also deficient in fulfilling their public sector equality duty, by not recognising the risk of a disproportionate impact upon women and minorities profiled by automated facial recognition technology.[64] The Court agreed that the breach of the public sector equality duty was a "serious issue of public concern".[65] The duty's importance lies in the requirement that "a public authority give thought to the potential impact of a new policy which may appear to it to be neutral but which may turn out in fact to have a disproportionate impact on certain sections of the population".[66] Here, the Court reasoned, the South Wales Police had :never sought to satisfy themselves, either directly or by way of

[60] *Id.* at [152].

[61] *Id.* at [152]-[153].

[62] *Id.* at [159].

[63] *Id.* at [165].

[64] *Id.* at [164].

[65] *Id.* at [173].

[66] *Id.* at [179].

independent verification, that the software program in this case does not have an unacceptable bias on grounds of race or sex".[67] The Court noted evidence from computer expert Dr Anil Jain that automated facial recognition can sometimes have such bias and could generate a greater risk of "false positives" relating to persons from ethnic minorities and women because of the way in which the "training datasets" had been configured.[68] Consequently, the automated facial recognition technology would be better at identifying with greater accuracy persons of a demographic it has been given a bigger data set on. Faced with opposing expert evidence on whether on not such algorithms could give rise to bias, the Court did not comment nor adjudicate on whether the South Wales Police's technology was producing bias.[69] However, that the South Wales Police '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' meant it did not fulfil its public sector equality duty.[70] Consequently, the Court allowed the fifth and final ground of appeal.[71]

PART II ANALYSIS AND IMPLICATIONS

This is the first case to consider police use of automated facial recognition technology in public spaces, and has important implications not only for the rights to privacy and data protection, but also on the right to political protest and democratic participation more generally. While the case concerned the deployment of the technology and specific legislation in the UK, it is emblematic of wider concerns worldwide around the *ad hoc* and

[67] *Id.* at [199].

[68] *Id.* at [193].; ANIL JAIN, *Expert Report of Dr Anil Jain* 47–51 (2018), http://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/First-Expert-Report-from-Dr-Anil-Jain.pdf (last visited Oct 16, 2020).

[69] BRIDGES (APPEAL), *supra* note 13 at [199].

[70] *Id.* at [199]–[201].

[71] *Id.* at [201]-[202].

discretionary use of automated facial recognition technology by police, without appropriate legal frameworks to govern their use nor sufficient oversight or public awareness, where the discriminatory nature of algorithmic and biometric technologies remains a significant threat. Thus, while *Bridges* is a landmark ruling about the limits of police discretion and for the future regulation of facial recognition technology and automated facial recognition, the long-term impact of the Court's pronouncement on the future expansion and deployment of automated surveillance technologies in public spaces is less clear. In particular, the Court did not find that deploying facial recognition technology for mass surveillance in public spaces is disproportional, and nor did it demand that the automated facial recognition technologies used by police authorities be more transparent, with clear information about its operation be accessible in the public domain, nor did it consider how regulatory guidance may fragment and make the law less predictable and certain. Instead, the Court imposed minimal formalistic requirements on the police to comply with their public sector equality duty and rights to privacy. I discuss these limitations in turn.

4 Surveillance, Protests in Public Spaces: The Acceptance of the FRT as 'Proportional'

> 'There is nothing in the Court of Appeal judgement that fundamentally undermines the use of facial recognition to protect the public. This judgement will only strengthen the work which is already underway to ensure that the operational policies we have in place can withstand robust legal challenge and public scrutiny.*'*[72] *–South Wales Police, 2020*

[72] Response to the Court of Appeal judgment on the use of facial recognition technology, , SOUTH WALES POLICE , https://www.south-wales.police.uk/en/newsroom/response-to-the-court-of-appeal-judgment-on-the-use-of-facial-recognition-technology/ (last visited Oct 20, 2020).

Civil rights activists and advocacy organisations who have been long-concerned with the use of automated facial recognition technology to covertly gather intelligence on citizens, particularly those who exercise rights to engage in political protest, commended the *Bridges* decision when handed down by the Court of Appeal. However, the use of facial recognition technology to monitor political protests has not been banned or severed by the *Bridges* decision. To the contrary, the Court legitimitised such use, by holding the use of facial recognition technology in public places proportional in principle. As a result, the case will only be the first among many in the continuing resistance against the use of intrusive surveillance technologies in public spaces by law enforcement bodies.

The Court of Appeal recognised that automated facial recognition involves 'sensitive processing' and that related issues are very fact- and circumstance-specific. Thus, the judgment was very much confined to issues relating to the appellant's experience with the South Wales Police's use of AFR Locate, as opposed to analysing its impacts at large. *Proportionality*: The Court also considered the fact that facial matches made by AFR Locate were reviewed by a police officer to be an important safeguard for use of the technology. So, while the judgement does not provide *carte blanche* for police arrests based on judgments made by automated facial recognition software alone without human intervention, the decision affirms the role of automated facial recognition in modern policing and law enforcement.

The case does not go far enough in protecting enjoyment of public spaces without surveillance for a few reasons. First, the Court underplayed the wider impact that facial recognition technology deployed in public spaces has on the social fabric of population and on wider democratic participation. The Court held that facial recognition technology use was 'not in accordance with the law',[73] but had it been so, such use would be proportional – indeed, the

[73] BRIDGES (APPEAL), *supra* note 13 at [131].

Court went on to explain this point even if it did not have to.[74] The Court emphasized that, even it had to consider the impact of facial recognition technology, '[a]n impact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication'.[75]

Thus, the Court focused on the individual interference with the right to privacy occasioned to Edward Bridges, and refused to consider the wider, chilling effect of surveillance on the political freedoms of the populace as a whole, the sum of which is arguably greater than its parts. This point was raised by Bridges, who argued that the Court ought to have taken account of the potential reach of AFR Locate,[76] the Court flatly rejected this approach, stating that it is neither 'necessary [nor] helpful to consider hypothetical scenarios which may arise in the future'.[77] It is not clear whether the Court chose not engage with such wider impact because Bridges appeal did not contain a ground that the AFR Locate deployment infringed the rights to freedom of expression, assembly and association under Articles 10 and 11 of the ECHR, or for some other reason. The claim under Articles 10 and 11 RCHR was includedin the initial legal challenge launched by Bridges before the High Court, but was not pursued, and therefore, could not be appealed before the Court of Appeal.

Irrespective of the reasons, such a narrow judicial interpretation of the impact of the facial recognition technology underplays the impact of the surveillance of public spaces not only on the right to privacy of a specific individual, but also on the population as a while and its ability to participate in the political process, and protests, which require privacy and anonymity. The use of facial recognition technology nationwide in intelligence gathering, particularly around protests, has been the main concern of the

[74] *Id.* at [131]–[144].

[75] *Id.* at [143].

[76] *Id.* at [59].

[77] *Id.* at [60].

NGOs in the UK.[78] Indeed, facial recognition technology has been used to directly target protests around the world in the past few years. For example, concerns have been raised that 'smart lampposts' scattered throughout Hong Kong have in-built facial recognition technology. The Hong Kong government claims that such lampposts only collect data on traffic, weather and air quality, but protesters have been cutting them down over concerns that they contain facial recognition software used for surveillance by Chinese authorities.[79] Similarly, facial recognition technology was likely used by law enforcement during Black Lives Matters protests in Oakland and Baltimore in 2015,[80] and a journalist believes that his arrest near the Black Lives Matter protests in 2014 was also due to police use of facial recognition.[81] Facial recognition technology has reportedly been used during the 2020 protests connected to the killing of George Floyd,[82] and officers in Dallas have actively

[78] Hugh Tomlinson QC, *Case Law: R (on the application of Bridges) v Chief Constable of South Wales, Police use of "automatic facial recognition technology unlawful*, INFORRM'S BLOG (2020), https://inforrm.org/2020/08/17/case-law-r-on-the-application-of-bridges-v-chief-constable-of-south-wales-police-use-of-automatic-facial-recognition-technology-unlawful-hugh-tomlinson-qc/ (last visited Sep 23, 2020).

[79] `ABC News, *Hong Kong protesters cut down data-collecting lamppost*, ABC NEWS (2019), https://www.abc.net.au/news/2019-08-24/hong-kong-protests-smart-lampposts-cut-down-surveillance-fears/11445606 (last visited Feb 16, 2020).

[80] Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color | ACLU of Northern CA, , https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target (last visited Jun 3, 2020).

[81] Ali Winston, *Oakland Cops Quietly Acquired Social Media Surveillance Tool*, EAST BAY EXPRESS , https://www.eastbayexpress.com/oakland/oakland-cops-quietly-acquired-social-media-surveillance-tool/Content?oid=4747526 (last visited Jun 3, 2020).

[82] Police Facial Recognition Tech Could Misidentify Protesters, , DIGITAL TRENDS (2020), https://www.digitaltrends.com/news/police-protests-facial-recognition-misidentification/ (last visited Jun 4, 2020) The Minneapolis police department deny possession of facial recognition technology.

requested video footage of protest activity, presumably to run through facial recognition software.[83]

These global examples of police use of facial recognition technology illustrate the ability of the surveillance infrastructure to interfere with protest movements. When the privacy of the individual is at risk, so too is the integrity of group demonstrations in public places. The police deployment of facial recognition technology in public spaces is likely to have a 'chilling' effect on collective action. [84] Studies have shown that individuals are less likely to share their opinions, both online[85] and offline,[86] where they feel they are in the minority.

Many US scholars have imputed this 'chilling effect' to the use of facial recognition technology,[87] which threatens the right to protest anonymously, which is fundamental to social movements and protests, and which requires a population to feel confident and safe

[83] Heather Kelly & closeHeather KellyTechnology reporterEmailEmailBioBioFollowFollowRachel Lerman closeRachel LermanReporter covering breaking news in, *America is awash in cameras, a double-edged sword for protesters and police*, WASHINGTON POST , https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/ (last visited Jun 4, 2020).

[84] See, eg, Murphy, *supra* note 22; Matthew Schwartz, *Color-Blind Biometrics? Facial Recognition and Arrest Rates of African-Americans in Maryland and the United States*, 2019.

[85] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNAL. MASS COMMUN. Q. 296–311 (2016); Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECHNOL. LAW J. 117 (2016); See also THE FDR GROUP, *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (2013), https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (last visited Jun 30, 2020).

[86] C. J. Glynn, A. F. Hayes & J. Shanahan, *Perceived support for one's opinions and willingness to speak out: A meta-analysis of survey studies on the "spiral of silence."*, 61 PUBLIC OPIN. Q. 452–463 (1997); *Id.*; D. A. Scheufele & P Moy, *Twenty-five years of the spiral of silence: A conceptual review and empirical outlook*, 12 INT. J. PUBLIC OPIN. RES. 3–28 (2000).

[87] Roberto Iraola, *Lights, Camera, Action! Surveillance Cameras, Facial Recognition Systems and the Constitution*, 49 LOYOLA LAW REV. 773–808 (2003); Murphy, *supra* note 22.

in their ability to gather in public spaces to manifest their disagreement with the *status quo*. Such sense of safety is necessary to facilitate robust democratic participation, with protesting acting as a display of an understanding that an individual is advocating for something greater than themselves. Protests, riots, or revolutions require a tangible location, typically in the streets and other public places.[88] Public spaces act as the areas of societal interaction, and occupy not just a physical space but also a symbolic one.[89] Interrupting these public spaces by dissenters/protesters 'touch upon the very core of the current structure and organization of social systems, namely the balance of power, rule of law and democratic governance'.[90] It questions the ability of government authorities to maintain the integrity of these shared spaces,[91] challenging existing power structures.

Therefore, the Court's pronouncement and refusal to consider the wider impact of facial recognition surveillance in public places on the population legitimises public space surveillance as *proportional*, and reaffirms, if not strengthens, the legitimacy of the facial recognition technology use for mass surveillance in modern policing.

5 Discrimination and Commercial Secrecy: A Limited Judicial Demand for Transparency

> 'This judgment is a major victory in the fight against discriminatory and oppressive facial

[88] Daniel Trottier & Christian Fuchs, *Theorising Social Media, Politics and the State: An Introduction*, *in* SOCIAL MEDIA, POLITICS AND THE STATE 3–38, 33 (Daniel Trottier & Christian Fuchs eds., 2015).

[89] Jens Kremer, *The End of Freedom in Public Places? Privacy problems arising from surveillance of the European public space*, 2017.

[90] *Id.* at 73.

[91] Protestbewegung - Warum einen öffentlichen Platz besetzen? (Why occupy a public space?), , DEUTSCHLANDFUNK (2014), https://www.deutschlandfunk.de/protestbewegung-warum-einen-oeffentlichen-platz-besetzen.1184.de.html?dram:article_id=299327 (last visited Jun 17, 2020).

> recognition. The Court has agreed that this dystopian surveillance tool violates our rights and threatens our liberties'[92] –Megan Goulding, Lawyer, Liberty, 2020'

The *Bridges* judgment also highlights the tensions between the discriminatory impact of facial recognition technology on ethnic minorities and women on the one hand, and the inability to investigate the technologies' operation because of trade and commercial secrecy surrounding the technologies. The Court made a number of remarks suggesting that to comply with its equality duties, the South Wales Police and the facial recognition technology software should be more transparent (or at least independently reviewable). Even before the *Bridges Appeal*, the UK Equality and Human Rights Commission had, in March 2020, called on suspensions on the use of facial recognition technology in England and Wales pending independent scrutiny of the discriminatory impacts the technology may have against protected groups.[93] The Court's explicit judgment that the South Wales Police failed in its public sector equality duty because *it did not independently seek to verify* whether or not the software could give rise to bias[94] is important because it puts the onus on police to carefully select and scrutinise the technologies they buy from private companies, which, in turn, may make the standards for such technologies on the private market higher as companies seek to sell to government agencies.[95] However, commercial and trade secrecy

[92] Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech, *supra* note 1.

[93] Facial recognition technology and predictive policing algorithms out-pacing the law, , EQUALITY AND HUMAN RIGHTS COMMISSION (2020), https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law (last visited Sep 16, 2020).

[94] BRIDGES (APPEAL), *supra* note 13 at [199].

[95] Martin Kwan, *Ensuring the lawfulness of automated facial recognition surveillance in the UK*, OXFORD HUMAN RIGHTS HUB (2020), https://ohrh.law.ox.ac.uk/ensuring-the-lawfulness-of-automated-facial-recognition-surveillance-in-the-uk/ (last visited Oct 16, 2020).

surrounding machine learning technologies[96] may entirely preclude use of those technologies by UK public agencies due to the inability to verify the equal application of that technology with respect to the "protected characteristics" contained in the public sector equality duty. Therefore, to prevent any discriminatory impact the technologies used by public authorities should be open source and available for public scrutiny, if they are used at all.

The discriminatory effects of facial recognition technology and surveillance generally on minority groups has been demonstrated in an increasing body of academic research.[97] The emerging consensus is that facial recognition technologies are not 'neutral',[98] but instead reinforce historical inequalities.[99] For example, studies have shown that facial recognition technology performs poorly in relation to women, children, and individuals with darker skin tones.[100] The bias and discrimination can be introduced into the

[96] See, eg, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in The Criminal Justice System*, 70 STANFORD LAW REV. 1343, 1346 (2018); Deven R. Desai & Joshua Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J. LAW TECHNOL. 1, 9; Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM LAW REV. 1085, 1091–1093 (2018).

[97] CLARE GARVIE, ALVARO BEDOYA & JONATHAN FRANKLE, *The Perpetual Line-Up* (2016), https://www.perpetuallineup.org/ (last visited Nov 11, 2019); B. F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 6 INF. FORENSICS SECUR. IEEE TRANS. 7 1789–1801 (2012); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 *in* PROCEEDINGS OF MACHINE LEARNING RESEARCH 1–15 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf (last visited Jun 17, 2020).

[98] GARVIE, BEDOYA, AND FRANKLE, *supra* note 97; Klare et al., *supra* note 97; Buolamwini and Gebru, *supra* note 97.

[99] Schwartz, *supra* note 84 at 15.

[100] Salem Hamed Abdurrahim, Salina Abdul Samad & Aqilah Baseri Huddin, *Review on the effects of age, gender, and race demographics on automatic face recognition*, https://link-springer-com.wwwproxy1.library.unsw.edu.au/content/pdf/10.1007/s00371-017-1428-z.pdf (last visited Jun 2, 2020); Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, , AMERICAN CIVIL LIBERTIES UNION , https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28 (last visited Jun 2, 2020).

facial recognition technology software in three technical ways: first, through the machine learning process through the training data set and system design; secondly, through technical bias incidental to the simplification necessary to translate reality into code; and thirdly, through emergent bias which arises from users' interaction with specific populations.[101] Because the training data for facial recognition technologies comes from photos relating to past criminal activity,[102] minority groups are overrepresented in facial recognition technology training systems,[103] especially in some jurisdictions such as the United States, where racial minorities are at a much higher risk of being *pulled over,*[104] *searched,*[105] *arrested,*[106]

[101] Rebecca Crootof, *"Cyborg Justice" and the Risk of Technological–Legal Lock-In*, 119 COLUMBIA LAW REV. 1, 8 (2019); Batya Friedman & Helen Fay Nissenbaum, *Bias in Computer Systems*, 14 ACM TRANS. INF. SYST. 330, 333–36 (1996).

[102] Ruhrmann, *supra* note 4 at 46; GARVIE, BEDOYA, AND FRANKLE, *supra* note 97.

[103] Ruhrmann, *supra* note 4 at 63; GARVIE, BEDOYA, AND FRANKLE, *supra* note 97.

[104] New Data Reveals Milwaukee Police Stops Are About Race and Ethnicity, , AMERICAN CIVIL LIBERTIES UNION , https://www.aclu.org/blog/criminal-law-reform/reforming-police/new-data-reveals-milwaukee-police-stops-are-about-race-and (last visited Jun 2, 2020); FRANK R BAUMGARTNER, DEREK A EPP & KELSEY SHOUB, SUSPECT CITIZENS WHAT 20 MILLION TRAFFIC STOPS TELL US ABOUT POLICING AND RACE (2018).

[105] New Data Reveals Milwaukee Police Stops Are About Race and Ethnicity, *supra* note 104; Camelia Simoiu, Sam Corbett-Davies & Sharad Goel, *THE PROBLEM OF INFRA-MARGINALITY IN OUTCOME TESTS FOR DISCRIMINATION*, 11 ANN. APPL. STAT. 1193–1216 (2017); Lynn Lanton, *Police Behavior during Traffic and Street Stops, 2011*, https://www.bjs.gov/content/pub/pdf/pbtss11.pdf (last visited Jun 2, 2020).

[106] NAACP | Criminal Justice Fact Sheet, , NAACP , https://www.naacp.org/criminal-justice-fact-sheet/ (last visited Jun 2, 2020); Megan Stevenson & Sandra Mayson, *The Scale of Misdemeanor Justice*, 98 BOSTON UNIV. LAW REV. 371 (2018).

incarcerated,[107] *and wrongfully convicted*[108]. Therefore, facial recognition technology is capable of producing a large number of false positives because it is already functioning in a highly discriminatory environment.

The Court in *Bridges* acknowledged that gender and racial bias of the ''AFR Locate system could not be established because a 'safeguard' would instantly delete the majority of profiles registered by the system.[109] The Court recognised that details of the training dataset could not be made public due to 'commercial confidentiality', which 'may be understandable but, in our view, it does not enable a public authority to discharge its own, non-delegable, duty'.[110] To bring up once more, with the success of the *Bridges* case, the onus is now on police department and the legislature to provide appropriate safeguards against possible discriminatory application of law enforcement technologies.[111] Thus, the Court explained that it was necessary for the South Wales Police to take 'reasonable steps to make enquiries about what may not yet be known to a public authority about the potential impact of a proposed decision or policy on people with the relevant characteristics'.[112]

[107] The Color of Justice: Racial and Ethnic Disparity in State Prisons, , THE SENTENCING PROJECT , https://www.sentencingproject.org/publications/color-of-justice-racial-and-ethnic-disparity-in-state-prisons/ (last visited Jun 2, 2020).

[108] SAMUEL GROSS, MAURICE POSSLEY & KLARA STEPHENS, *Race and Wrongful Convictions in the United States* (2017), http://www.law.umich.edu/special/exoneration/Documents/Race_and_Wrongful_Convictions.pdf (last visited Jun 2, 2020).

[109] BRIDGES (APPEAL), *supra* note 13 at [191].

[110] *Id.* at [199].

[111] Surveillance Camera Commissioner, *Surveillance Camera Commissioner's statement: Court of Appeal judgment (R) Bridges v South Wales Police – Automated Facial Recognition*, GOV.UK (2020), https://www.gov.uk/government/speeches/surveillance-camera-commissioners-statement-court-of-appeal-judgment-r-bridges-v-south-wales-police-automated-facial-recognition?utm_source=miragenews&utm_medium=miragenews&utm_campaign=news (last visited Sep 16, 2020).

[112] BRIDGES (APPEAL), *supra* note 13 at [181].

The inability for public authorities to satisfy the public sector equality duty stems from the mode of operation between private companies developing automated facial recognition software and the public bodies, such as police departments, who employ them, which is based on corporate secrecy laws and procurement practices of the South Wales Police "fail to foreground the public interest".[113] Where government agencies contract and use algorithms, transparency and accountability features should be 'built in' to the contracts used to commission such technology, and the technology itself. Such procurement practices should be standardised in legislation. A good example of procurement regulation which supports transparency and accountability, and therefore provide public authorities with the ability to satisfy their public sector equality duty, is the originally proposed (now substituted) *2019 Washington State House Bill 1655*,[114] which included sections banning nondisclosure provisions (Section 4(4)), and required that all automated decision systems and the data used in the system was "freely available by the vendor before, during, and after deployment for agency or independent third-party testing, auditing, or research to understand its impacts, including potential bias, inaccuracy, or disparate impacts" (Section 4(3)(b)).[115]

Therefore, facial recognition technology should be open source as a condition for the use by public authorities, including police. While in Courts view, an independent review of the automated facial recognition training data set and regular audits of the software performance on new datasets could be sufficient,[116] it is hard to justify commercial secrets when technologies are used for

[113] Hannah Bloch-Wehba, *Access to Algorithms*, 88 FORDHAM LAW REV. 1265, 1307 (2020).

[114] STATE OF WASHINGTON, *House Bill 1655* (2019), http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Bills/1655-S.pdf?q=20200728230015.

[115] These sections were removed in the Substitute Bill, which is still before the House Committee: STATE OF WASHINGTON, *Substitute House Bill 1655* (2019), http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Bills/1655-S.pdf?q=20200728230015.

[116] BRIDGES (APPEAL), *supra* note 13 at [199].

public purposes and significantly impact on the public. Compliance with the public sector equality duty by public authorities requires built-in transparency and accountability safeguards in relevant commercial contracts and designs of technologies themselves. Such safeguards should be a pre-requisite for technology corporations seeking to engage in public procurement contracts.

6 A Room for Fragmentation and *Ad Hoc* Use

> "I very much welcome the findings of the court in these circumstances. I do not believe the judgement is fatal to the use of this technology, indeed, I believe adoption of new and advancing technologies is an important element of keeping citizens safe. It does however set clear parameters as to use, regulation and legal oversight".[117] – UK Surveillance Camera Commissioner, 2020

> "What the judgement has done is helpfully describe how we might strengthen deployment policies and influence codes of practice in how this technology is used across the UK … *[It has been]* a really helpful process…placing a rigorous test on our policies and the way that we approach things".[118] – South Wales Police, 2020

Finally, despite the Court's insistence on more procedural safeguards and transparency for police use of automated facial recognition, the judgment left a lot of room for fragmentation and divergence in police practices around the use of the technology. In particular, the Court reasoned that the South Wales Police's local policies would constitute 'law' for considering the legitimacy of interference under Article 8 of the ECHR: "As we have said, in

[117] Facial Recognition - What is the impact of the Bridges case?, , https://www.jmw.co.uk/services-for-you/media-law/blog/facial-recognition-what-impact-bridges-case (last visited Oct 16, 2020).

[118] South Wales Police, *supra* note 2 at 3.

principle a police force's local policies can constitute relevant "law" in the present context, provided they are published."[119] Instead of demanding legislative reform, which would apply across the UK, the Court has opened the door for each police department to develop their own guidelines on the use of facial recognition technology, which will result in fragmentation of the use of facial recognition technology across the UK.

Future police uses of facial recognition technology in the UK include the integration of technology with the CCTV and ANPR network in London (proposed by West Yorkshire Police in 2017,[120] and the City of London Police in 2018[121]),[122] analysis of video footage taken by mobile devices, CCTV, and police body cameras after the fact,[123] as well as mobile facial recognition technologies which integrate biometric tracking software across multiple devices.[124] In early 2020 the Metropolitan Police Service in London announced it would roll out live FRT software *NeoFace*, as part of its general policing strategy.[125]

If these activities are not comprehensively regulated, the ad hoc fragmented regulatory framework will reduce the predictability and consistency of police action, and will enable police departments, as well as other public and private agencies, to share gathered information with little transparency or limitations. For example, in the US, law enforcement agencies in at least 40 states use facial

[119] BRIDGES (APPEAL), *supra* note 13 at [121].

[120] Louise Cooper, *New-style CCTV could help find missing people more quickly*, YORKSHIRELIVE (2017), http://www.examiner.co.uk/news/west-yorkshire-news/how-new-style-cctv-could-13532881 (last visited Jun 11, 2020).

[121] New ring of steel, , PROFESSIONAL SECURITY , https://www.professionalsecurity.co.uk/news/interviews/new-ring-of-steel-proposed/ (last visited Jun 11, 2020).

[122] Big Brother Watch, *supra* note 30 at 31.

[123] *Id.* at 32.

[124] *Id.* at 32–33.

[125] James Vincent, *London police to deploy facial recognition cameras across the city*, THE VERGE (2020), https://www.theverge.com/2020/1/24/21079919/facial-recognition-london-cctv-camera-deployment (last visited May 5, 2020).

recognition technology in the absence of a federal regulatory framework, and State and Federal agencies promote inter-authority cooperation in access to databases, actively enlarging the size of the population over which they hold biometric information.[126] Police also actively collaborate with other public authorities as well as private, corporate entities. For instance, the New York based company, Clearview AI, claims to have a database of over 3 billion images,[127] and their software was purportedly used by over 600 law enforcement agencies in 2019-20.[128] Even if a police department has stringent collection and storage guidelines, that department may share the information with other police departments which do not have such stringent requirements. Such *ad hoc* regulation of facial recognition technology use in the US illustrates the risks in

[126] Gretta Goodwin, *Face Recognition Technoloy: DOJ and FBI have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains*, https://www.gao.gov/assets/700/699489.pdf (last visited Jun 1, 2020); It is estimated that at least one in four state or local police departments have access to their own database of facial recognition images, or have access to another agency's database ACLU, *ACLU Letter to Department of Justice concerning Facial Recognition* 2–3, https://www.aclu.org/sites/default/files/field_document/coalition_letter_to_doj_crt_re_face_recognition_10-18-2016_1.pdf (last visited Jun 1, 2020); As of 2019, 14 states had access to the FBI's NGI-IPS Facial Recognition Technology: Ensuring Transparency in Government Use — FBI, , https://www.fbi.gov/news/testimony/facial-recognition-technology-ensuring-transparency-in-government-use (last visited Jun 2, 2020).

[127] Jordan Valinsky Business CNN, *Clearview AI has billions of our photos. Its entire client list was just stolen*, CNN , https://www.cnn.com/2020/02/26/tech/clearview-ai-hack/index.html (last visited Mar 6, 2020); Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N. Y. TIMES (2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; The ACLU has brought an action against ClearView AI, claiming that it has breached the Illinois Biometric Information Privacy Act We're Taking Clearview AI to Court to End its Privacy-Destroying Face Surveillance Activities, , AMERICAN CIVIL LIBERTIES UNION , https://www.aclu.org/news/privacy-technology/were-taking-clearview-ai-to-court-to-end-its-privacy-destroying-face-surveillance-activities/ (last visited Jun 1, 2020).

[128] Kashmir Hill, *supra* note 127.

granting police departments too great a discretion to effectively write their own rules, undermining basic protections for citizens.

Therefore, instead of enabling police departments to rely on their own-developed 'local policies' to meet the 'in accordance with law' standard, the Court should have encouraged a development a comprehensive regulatory framework, either by amendments to the *Data Protection Act 2018* and the *Surveillance Camera Code of Practice* or by developing new law, which would apply across the UK. For example, legislative intervention could prevent fragmentation and remove undue discretion from police departments, left by the Court of Appeal in *Bridges*. Currently an *Automated Facial Recognition Technology (Moratorium and Review) Bill*, proposes to ban the use of technologies in the UK,[129] yet it is unlikely to come to fruition.

The regulation and limits on police use of facial recognition technology, for which the *Bridges* decision has opened the door, has thus been left for other courts or policy-makers to articulate. Other jurisdictions are considering ways to regulate, for example, in the US, the *Algorithmic Accountability Act* was introduced,[130] while the *Public Oversight of Surveillance Technology Act*[131] in the State of New York aims to increase transparency for how surveillance technologies are used by the New York Police Department.[132]

[129] Lord Clement-Jones. 2019. Automated Facial Recognition Technology (Moratorium and Review) Bill [HL] 2019-20. https://services.parliament.uk/bills/2019-20/automatedfacialrecognitiontechnologymoratoriumandreview.html/ (last visited 23 October 2020).

[130] YVETTE D. CLARKE, *H.R.2231 - 116th Congress (2019-2020): Algorithmic Accountability Act of 2019* (2019), https://www.congress.gov/bill/116th-congress/house-bill/2231 (last visited Oct 23, 2020).

[131] The New York City Council - File #: Int 0487-2018, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0 (last visited Oct 10, 2019).

[132] Facial-recognition technology requires smart legislation, CRAIN'S NEW YORK BUSINESS (2019), https://www.crainsnewyork.com/op-ed/facial-recognition-technology-requires-smart-legislation (last visited Oct 10, 2019).

A legal action, launched in August 2020, against the use of facial recognition by the French police before the *Conseil d'État* (the highest administrative court in France) might clarify the limits on police use of facial recognition technology in France. The claim focuses on the provisions of the French *Criminal Code of Procedure* which authorises police use of facial recognition to identify people registered in a police criminal record database – called the *"Traitement des antécédents judiciaires"* – which contains 19 million files and more than 8 million images of people.[133] It will be seen whether the *Conseil d'État* and US courts examining ACLU claims will demand more stringent comprehensive regulation of police use of facial recognition technology or leave a lot of room for an *ad hoc* and fragmented regulatory framework.

7 Conclusion

While the Bridges decision is an important first step in limiting police discretion over the use of facial recognition technology, the judgment is far from a great victory for those opposing the expansion of surveillance infrastructure in public spaces. The Court has underplayed, if not explicitly rejected, facial recognition technologies' wide-ranging impact on the public participation, public life, and civil discourse. Neither did it recognize transparency as a pre-requisite for the facial recognition technology shielded behind commercial trade secrecy yet deployed by the police. Nor did Court insisted on a comprehensive legislative reform, leaving room for fragmentation of the future regulation of facial recognition technologies in modern policing.

Contrary to Courts narrow approach, facial recognition infrastructure in public spaces impacts not only an individual right to privacy, and their ability to pass through public spaces, but it also affects population's ability to act collectively. Facial recognition technology in public spaces is not merely a 'negligent' invasion of privacy, but an expanding infrastructure which cuts at

[133] Conseil D'état, *supra* note 16.

the heart of democratic participation. In *Bridges,* the use of automated facial recognition technology was 'proportionate' to the law enforcement goals, but the Court did not take into account these broader societal concerns. In failing to engage directly with questions of democracy, public participation, and individual identity in public spaces, the Court of Appeal missed an opportunity to balance law enforcement goals with broader democratic values of political participation and to secure the future of public spaces in the technological state.

Similarly, the Court's analysis of the discriminatory nature of the facial recognition technology leaves a lot of room for the status quo of proprietary technology, shrouded by corporate secrecy laws, to be used by public authorities. While the Court acknowledged the need for safeguards when government agencies use cutting edge technologies, it left it for the police to decide what those safeguards should be. Would the creation of an independent advisory board with access to the software be sufficient? And can such a board genuinely satisfy any public authority of the technology's equal application to all persons, if there is no way to know how it operates? The tension between trade secrecy laws and public governance however is not easily resolvable, and the Court could have signalled the direction in which the balance should be tipped. It is hard to see why police forces should be able to use the technologies, surrounded by trade secrecy, when exercising public functions and duties, especially when they themselves are unable to know how using such technology may discriminate against large segments of the population.

Finally, the Court left a lot of room for fragmentation in the regulatory framework overseeing police use of automated facial recognition technologies. By accepting that a locality-wide policy could constitute a 'law' for the purposes of Article 8 of the ECHR, the Court opened the door for different police forces to establish their own individual guidelines. Nationwide legislative reforms would ensure consistency and predictability in police use of facial recognition technology, and it will be for other courts to demand for comprehensive reforms more firmly in the future.

In conclusion, the Court of Appeal decision in *Bridges* case has sparked a public debate on the use of automated facial recognition technology, and by requiring police departments to rethink their deployment of the technology, opened the door for a reform of police use biometric technologies more generally. The Court was clear that a paradigm shift is needed: instead of allowing individual police departments to 'make up' the rules as they go, the limitations on the use of automated facial recognition must be clearly spelled out in advance. Yet, the Court has also given the polices forces a lot of leeway to spell out these limits in their own policies – not necessarily laying foundations for the legislative intervention. Importantly, the Court opined that the use of facial recognition for mass surveillance in public places is proportional to the goals of modern policing. In sum, while the *Bridges* decision is reassuring for demanding change in the discretionary approach by the police in the UK in the short term; its long-term impact in burning bridges between the expanding public space surveillance infrastructure and the modern state is less certain.