THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOLUME 22 STLR.ORG NUMBER 2

ARTICLE

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

Monika Zalnieriute*

Live automated facial recognition technology, rolled out in public spaces and cities across the world, is transforming the nature of modern policing. R (on the application of Bridges) v Chief Constable of South Wales Police, decided in August 2020, *is the first successful legal challenge to automated facial recognition technology in the world. In* Bridges*, the United Kingdom's Court of Appeal held that the South Wales Police force's use of automated facial recognition technology was unlawful. This landmark ruling could influence future policy on facial recognition in many countries. The* Bridges *decision imposes some limits on the police's previously unconstrained discretion to decide whom to target and where to deploy the technology. Yet, while the decision requires that the police adopt a clearer legal framework to limit this discretion, it does not, in principle, prevent*

* Senior Lecturer and ARC DECRA Fellow, Faculty of Law & Justice, UNSW Sydney; Investigator at the ARC Centre of Excellence for 'Automated Decision-Making and Society'; Senior Fellow at Law Institute of the Lithuanian Centre for Social Sciences; Research Lead at Allens Hub for Technology, Law and Innovation; Associate at Australian Human Rights Institute, UNSW Sydney. m.zalnieriute@unsw.edu.au. This research has been funded by Australian Research Council Discovery Early Career Research Award ('Artificial Intelligence Decision-Making, Privacy and Discrimination Laws', project number DE210101183) and Research Council of Lithuania (LMTLT) ('Government Use of Facial Recognition Technologies: Legal Challenges and Solutions' (FaceAI), agreement number S-MIP-21-38). 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/Dundee, Nicolas Suzor at QUT, Alexander Trechsel at University of Lucerne and Giovanni Sartor at European University Institute for the invaluable feedback on the development of these ideas and earlier drafts. I also thank Jacob Silove and Inderpreet Kaugh Singh for their excellent research assistance.

the use of facial recognition technology for mass-surveillance in public places, nor for monitoring political protests. On the contrary, the Court held that the use of automated facial recognition in public spaces – even to identify and track the movement of very large numbers of people – was an acceptable means for achieving 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 this technology can place on democratic participation and freedoms of expression and association, which require collective action in public spaces. The Court neither demanded transparency about the technologies used by the police force, which is often shielded behind the "trade secrets" of the corporations who produce them, nor did it act to prevent inconsistency between local police forces' rules and regulations on automated facial recognition technology. Thus, while the Bridges *decision is reassuring and demands change in the discretionary approaches of U.K. police in the short term, its long-term impact in burning the "bridges" between the expanding public space surveillance infrastructure and the modern state is unlikely. In fact, the decision legitimizes such an expansion.*

> "[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" – 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." – South Wales Police, 2020.

I. INTRODUCTION

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 biometric features (such as a person's eyes, nose, mouth, skin textures, and shadows) to images in databases to identify individuals.[1] Live automated facial recognition can instantaneously assess the facial biometric data in the captured images against a pre-existing "watchlist," flagging any matches and notifying police officers.

In the United Kingdom and other countries, law enforcement agencies have used facial recognition technologies for many years without a legal framework governing their discretion. Train stations, airports, and city squares are increasingly equipped with facial recognition technologies in the United States, China, France and Hong Kong, among other nations. For example, in the U.K., at least four police departments (Leicestershire Police, South Wales Police, Metropolitan Police Service, and Humberside Police[2]) have experimented with the technology by linking it to CCTV cameras.[3] Across the UK, there are an estimated 5.9 million CCTV cameras,[4] and the country ranks third in the number of cameras per 100

---

[1] Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, MINN. L. REV. (forthcoming 2021); Jagdish Chandra Joshi & K K Gupta, *Face Recognition Technology: A Review*, 1 IUP J. TELECOMM. 53, 53–54 (2016); Relly Victoria & Virgil Petrescu, *Face Recognition as a Biometric Application*, 3 J. MECHATRONICS AND ROBOTICS 237, 240 (2019); Mary Grace Galterio et al., *A Review of Facial Biometrics Security for Smart Devices*, 7 COMPUTERS 37 (2018); IAN BERLE, FACE RECOGNITION TECHNOLOGY: COMPULSORY VISIBILITY AND ITS IMPACT ON PRIVACY AND THE CONFIDENTIALITY OF PERSONAL IDENTIFIABLE IMAGES (2020).

[2] 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.

[3] INFORMATION COMMISSIONER'S OPINION: THE USE OF LIVE FACIAL RECOGNITION TECHNOLOGY BY LAW ENFORCEMENT IN PUBLIC PLACES, 6 (Oct. 31, 2019), https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

[4] David Barrett, *One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey*, TELEGRAPH (July 10, 2013), https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html.

people, after the US and China.[5] Meanwhile, London ranks eighth in a list of the most surveilled cities in the world (the first through seventh cities are all in China).[6] London became one of the first cities to link CCTV cameras to facial recognition technologies in the late 1990s,[7] and their use intensified to address the newly perceived threat of terrorism following the September 11th attacks in the United States.[8] Today, facial recognition technologies can identify a single suspect in a city with a population of over three million people within just seven minutes.[9] Yet, despite the increasing use of facial recognition technology in modern policing, there is no comprehensive regulatory framework overseeing its use in the U.K.[10]

In *R (on the application of Bridges) v Chief Constable of South Wales Police* ([2020] EWCA Civ 1058), the Court of Appeal held that the use of automated facial recognition technology by the South Wales Police ('SWP') was unlawful because it was not "in accordance with law" as required by Article 8 of the European Convention on Human Rights ('ECHR').[11] In addition, the South Wales Police failed to carry out a proper data protection impact assessment and thus did not comply with the United Kingdom's public sector equality duty, which required the SWP to have "due regard" to potential equality implications of facial recognition technology when exercising its public function.[12]

Bridges is the first major successful legal challenge to police use of automated facial recognition technology anywhere in the world. Recent lawsuits brought by

---

[5] Humza Aamir, *Report Finds the US Has the Largest Number of Surveillance Cameras per Person in the World*, TECHSPOT (Dec. 6, 2019), https://www.techspot.com/news/83061-report-finds-us-has-largest-number-surveillance-cameras.html.

[6] Paul Bischoff, *Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?*, COMPARITECH (July 22, 2020), https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities.

[7] AI NOW, REGULATING BIOMETRICS: GLOBAL APPROACHES AND URGENT QUESTIONS 78 (Amba Kak ed.) (2020).

[8] James Meek, *Robo Cop*, THE GUARDIAN (June 13, 2002), https://www.theguardian.com/uk/2002/jun/13/ukcrime.jamesmeek; RHODRI JEFFREYS-JONES, WE KNOW ALL ABOUT YOU: THE STORY OF SURVEILLANCE IN BRITAIN AND AMERICA 183 (2017).

[9] Jon Russell, *China's CCTV Surveillance Network Took Just 7 Minutes to Capture BBC Reporter*, TECHCRUNCH (Dec. 13, 2017), https://social.techcrunch.com/2017/12/13/china-cctv-bbc-reporter.

[10] *See, e.g.*, 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 such as the Protection of Freedom Act 2012); *see also* INDEPENDENT ADVISORY GROUP ON THE USE OF BIOMETRIC DATA IN SCOTLAND 10–12 (2018) (recommending the establishment of a Scottish Biometrics Commissioner, as well as a Code of Practice to govern the use of biometrics).

[11] R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [210] (Eng.).

[12] *Id.* at [210]. 64 of the Data Protection Act 2018 (UK) requires authorities to carry out a data protection impact assessment – that is to measure potential negative implications for data protection of the facial recognition technologies before introducing them. Public sector equality duty in the UK is the obligation on public authorities such as SWP, under section 149(1) of the Equality Act 2010 (UK), to have "due regard" to certain prescribed matters when exercising their public functions.

non-governmental organizations ('NGOs') in the United States[13] and France[14] are still pending, and they might result in different judicial responses to the police use of facial recognition technology. Some American cities, like San Francisco and Berkeley, have banned the use of facial recognition technology by local agencies, including transportation authorities and law enforcement.[15] Some municipalities in Massachusetts have banned government use of facial recognition data in their communities,[16] and a few other states (California, New Hampshire, and Oregon) have also instituted bans on facial-recognition technology used in conjunction with police body cameras.[17] The *Automated Facial Recognition Technology (Moratorium and Review) Bill*, [18] which would ban the use of technologies in the United Kingdom, is pending in Parliament and its future remains uncertain.

In this largely unregulated context the *Bridges* decision is important because it imposed limits on the relatively unrestrained expansion of police use of facial recognition technologies in the U.K.[19] Before *Bridges,* automated facial recognition in the U.K. had been used without any constraints on the police's discretion to decide whom to target and where to deploy such technology. In the absence of judicial precedent on this point in many countries,[20] and the implicit approval by courts of last resort in others,[21] this judgment represents an important turning point

[13] 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 (Oct. 31, 2019), https://www.aclu.org/press-releases/aclu-challenges-fbi-face-recognition-secrecy.

[14] For example, the French digital rights advocacy group La Quadrature du Net had a case before the Conseil d'État, the country's high court for administrative justice. *See* La Quadrature du Net, https://www.laquadrature.net/wp-content/uploads/sites/8/2020/08/LQDN-REQ-TAJ-02082020.pdf (last visited Oct 20, 2020).

[15] Kate Conger et al., *San Francisco Bans Facial Recognition Technology*, N.Y. TIMES (May 14, 2019), https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. 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. *Id.*

[16] CHRISTOPHER JACKSON ET AL., REGULATION OF FACIAL RECOGNITION SYSTEMS AT THE MUNICIPAL LEVEL 3 (2020), https://escholarship.org/uc/item/7qp0w9rn.

[17] Max Read, *Why We Should Ban Facial Recognition Technology*, N.Y. MAG.: INTELLIGENCER (Jan. 30, 2020), https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html; American Civil Liberties Union, *California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams*, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA (Oct. 8, 2019), https://www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams.

[18] Automated Facial Recognition Technology (Moratorium and Review) Act 2020, HL Bill [87].

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

[20] 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 L. REV. ONLINE 1,1-32 (2018).

[21] *See, e.g.*, Justice K.S. Puttaswamy (Retd.) v. Union of India and Others. (2017) 10 SCC 1 (India). The Supreme Court of India held that the Indian government could make compulsory the

in legal discourse on the use of sophisticated technologies for biometric analysis in modern policing.

Yet, despite the plaintiff's celebrations of the decision's far-reaching impact,[22] the ruling leaves much to be desired. Most significantly, the Court ruled that deploying automated facial recognition in public spaces to identify very large numbers of people and track their movements is, *in principle*, acceptable in light of law enforcement goals. While the judgment insisted on a clearer articulation of limits on police discretion while using such technology, the decision did not generally prohibit the use of automated facial recognition technology for mass-surveillance in public places. In particular, the Court dismissed the broader risks posed by automated facial recognition technology use in public spaces as 'hypothetical'.[23] It thus underplayed the heavy burden that surveillance of public places has on the population as a whole, and especially on democratic participation and the right to protest, which require collective action in public spaces. In addition, the Court did not demand transparency about the technologies used by the police, which are often shielded behind the 'trade secrets' of the corporations who produce them.[24] Thus, while the *Bridges* decision reduces police discretion in the UK in the short term, its long-term impact in burning the "bridges" between the expanding public space surveillance infrastructure and the modern state is much weaker. In fact, the judgment opens the door for such an expansion.

The remainder of this Article is structured as follows. Part II provides the factual and legal background of the case. Part III explains the Court of Appeal's reasoning in the *Bridges* decision. Part IV emphasizes the formalistic nature of the Court's pronouncement and considers the impact that mass surveillance, facilitated by the use of facial recognition technology, has on political participation worldwide. Part V argues that the *Bridges* decision will have little impact on the use of automated facial recognition technologies in practice for two reasons. First, the Court offered only a limited discussion of this technology's potential for discrimination. Second, proprietary barriers make it harder to understand how this technology actually operates. Part VI concludes and predicts that automated facial recognition technologies will be regulated in a fragmented, *ad hoc* fashion in the future.

---

use of the "Aadhaar" authentication system, which incorporates facial recognition technology, in accessing government schemes and benefits. While the case is not about the use of facial recognition technology by police, the case concerned the use of this technology by government bodies more generally.

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

[23] R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [60] (Eng.).

[24] Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in The Criminal Justice System*, 70 STAN. L. REV. 1343, 1367 (2018).

II. SETTING THE SCENE

A. Factual and Legal Background

The *Bridges* case concerned a live automated facial recognition technology, called 'AFR Locate,' which instantly assesses the facial biometric data gathered from a live video feed against a pre-existing database (or 'watchlist') of photographs.[25] If no match registers, the video 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 machine learning software, which 'learns' to recognize facial features and matches biometrics to large databases containing facial photographs of people who have been arrested.[28] Data published by the U.K. Home Office shows that arrest rates in the U.K. are 3.2 times higher for people of African origin than Caucasians.[29] Facial recognition databases therefore often over-represent ethnic minorities.[30]

Between 2016 and 2018, the South Wales Police was awarded £2.6 million for an automated facial recognition technology pilot program.[31] 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, music concerts, and sporting events.[32] The South Wales Police used AFR Locate to identify individuals who were "wanted on suspicion for an offence, wanted on warrant, vulnerable persons and other persons where intelligence [was] required."[33] It is estimated that around 500,000 faces may have been scanned.[34] Although AFR Locate is designed to identify a pre-specified list of people, the technology must collect biometric data from every person who appears on the live feed in order to scan it. Therefore, the vast majority of faces scanned were not of persons flagged on a watchlist, and their images were automatically deleted.

In October 2018, civil society activist Edward Bridges, with the support of the UK non-governmental organization Liberty, filed a claim for judicial review. Bridges argued 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 European

---

[25] Bridges [2020] EWCA (Civ) 1058 at [8]-[9].

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

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

[28] *Id.* at [8]–[9].

[29] GOV.UK ETHNICITY FACTS AND FIGURES, https://www.ethnicity-facts-figures.service.gov.uk/crime-justice-and-the-law/policing/number-of-arrests/latest (last visited May 11, 2021).

[30] RUHRMANN, *supra* note 2, at 41.

[31] 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 May 11, 2021)..

[32] SOUTH WALES POLICE, ALL DEPLOYMENTS (2020), https://afr.south-wales.police.uk/wp-content/uploads/2020/04/All-Deployments.pdf.

[33] SOUTH WALES POLICE, SOUTH WALES POLICE DATA PROTECTION IMPACT ASSESSMENT, https://afr.south-wales.police.uk/wp-content/uploads/2019/10/DPIA-V5.4-Live.pdf (last visited May 11, 2021).

[34] R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [16] (Eng.).

Convention on Human Rights[35] and breached both the U.K.'s data protection law[36] and public sector equality duty.[37] Bridges claimed to have been in the proximity of the automated facial recognition technology on two occasions: near the automated facial recognition-equipped van in the city center of Cardiff on December 21, 2017[38] and at the entrance of a protest he attended against the U.K. defense exhibition of arms at Motorpoint Arena on March 27, 2018.[39] The initial legal challenge also included an explicit claim that the AFR Locate deployment infringed Bridges' rights to freedom of expression, assembly and association under Articles 10 and 11 of the ECHR, but this claim was not pursued before the High Court.[40]

In September 2019, the High Court (which in this case was a court of first instance) dismissed Bridges' claim, determining that the use of automated facial recognition was both in "accordance with the law" and "necessary and proportionate" to achieve South Wales Police's statutory obligations.[41] Under the ECHR, the standard of "necessity and proportionality" is satisfied only when a restrictive measure is more than merely useful, reasonable or desirable.[42] The standard also requires a demonstration that such measures are the least intrusive instrument among those which might achieve their protective function and are proportionate to the interest to be protected.[43] In the High Court's view, the facial recognition technology satisfied both of these criteria.[44] The High Court also dismissed Bridges' claims under the U.K.'s 2018 Data Protection Act for the same reason. Further, it 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 2010 Equality Act.[45] 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

---

[35] Article 8 of the ECHR provides: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 230 [hereinafter European Convention on Human Rights] (entered into force Sept. 3, 1953).

[36] Bridges alleged breaches of sections 4(4) of Data Protection Act 1998, and section 35(1) of Data Protection Act 2018 (requirement to comply with data protection principles), and section 64 of Data Protection Act 2018 (requirement to carry out a data protection impact assessment); Bridges [2020] EWCA (Civ) 1058 at [32].

[37] *Id.* at [32]. Public sector equality duty is the obligation on public authorities such as SWP, under section 149(1) of the Equality Act 2010 (UK), to have "due regard" to certain prescribed matters when exercising their public functions. R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2019] EWHC (Admin) 2341, [18]-[21] (Eng.).

[38] Bridges [2020] EWCA (Civ) 1058 at [26]-[27].

[39] *Id.* at [28]-[30].

[40] *Id.* at [32]–[33].

[41] Bridges [2019] EWHC (Admin) 2341 at [18]-[21].

[42] The Sunday Times v. The United Kingdom, 6538/74, Eur. Ct. H.R. (1979) at 59.

[43] See *id.* at 62.

[44] Bridges [2019] EWHC (Admin) 2341 at [18]-[21].

[45] *Id.* at [149]-[158].

consistent with the requirements of the Human Rights Act, and the data protection legislation."[46]

In June 2020, Bridges appealed the decision of the High Court to the Court of Appeal on five grounds. Bridges claimed that: 1) 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); 2) 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; 3) the High Court wrongly held that the South Wales Police's Data Protection Impact Assessment complied with statutory requirements; 4) the High Court erred in declining to opine on whether the South Wales Police had an appropriate policy document to comply with its data protection duties; and 5) the High Court wrongly held 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. [47]

B. The Decision of the Court of the Appeal

In August 2020, the Court of Appeal overturned the High Court's determination, finding in favor of Bridges on three of the five original grounds. The High Court held that: 1) 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); 2) the Data Protection Impact Assessment did not comply with the Data Protection Act 2018 (ground 3); and 3) the South Wales Police failed to satisfy its public service duty under section 149 of the Equality Act 2010 in not recognizing the risk of a disproportionate impact upon women and minorities of the AFR technology (ground 5).[48]

First, the Court found "fundamental deficiencies" in the legal framework governing the use of automated facial recognition, declaring that its use was *not* "in accordance with law" under the well-established ECHR three-step test governing rights to respect for privacy and family life. That test requires that any interference with a right must 1) be 'in accordance with the law', 2) pursue a legitimate aim, and 3) be necessary and proportional.[49] The first element requires that any interference must be in accordance with the law and limited to what is explicitly articulated in the law.[50] In other words, the policy and practice of police use of facial recognition technology must be articulated in the law. This criterion of the

[46] *Id.* at [159].

[47] R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [53] (Eng.).

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

[49] European Convention on Human Rights, *supra* note 37, at art. 8(2).

[50] The Sunday Times v. The United Kingdom, 6538/74, Eur. Ct. H.R. (1979).

three-part test is only satisfied if the law is clear, accessible, predictable, and uniformly applied.[51]

In this regard, the Court distinguished novel automated facial recognition technology, which involves the *automated* processing of sensitive personal data, from other intrusive measures operating under established legislative frameworks, such as retention of fingerprints and DNA records,[52] or police use of secret 'extremism databases'.[53] 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.[54] The Surveillance Camera Code of Practice[55] and South Wales Police local policies did not contain limitations on who can be put on a watchlist, or where the AFR can be deployed.[56] 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."[57] The Court further described the discretion afforded by the existing policies as "impermissibly wide"[58] because 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.[59] Noting the broad discretion that the police retained, the Court implied the significance of the police's reasonable belief when it stated that "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."[60] As such, 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.[61]

Because the use of automated facial recognition was ruled unlawful, the Court of Appeal did not need to decide whether its use satisfied the standard of proportionality. But, in an unexpected move, the Court went beyond its strict mandate to address this ground. It held that the High Court had correctly balanced the actual and anticipated benefits of AFR Locate on the one hand with its impact on Bridges on the other hand. Mr. Bridges had specifically argued that proportionality balancing should consider the impact not only on himself, but also

---

[51] *Id.*

[54] S and Marper v. United Kingdom, 30562/04 and 30566/04, Eur. Ct. H.R. (2008) [1581].

[53] R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [65]-[81], [86]-[90] (Eng.) (citing R (on the application of Catt) v. Association of Chief Police Officers [2015] UKSC 2013/0114, [20]).

[54] *Id.* at [91].

[55] The Surveillance Camera Code of Practice is a not legally binding piece of guidance. However, it is expected that police forces will adopt the code voluntarily to comply with their obligations under the Human Rights Act, Data Protection Act, and Regulation of Investigatory Powers Act. HOME OFFICE, SURVEILLANCE CAMERA CODE OF PRACTICE (2013), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/282774/SurveillanceCameraCodePractice.pdf.

[56] Bridges [2020] EWCA Civ 1058 at [109]-[130]

[57] *Id.* at [94].

[58] *Id.* at [152].

[59] *Id.* at [130].

[60] *Id.* at [96].

[61] *Id.* at [210].

on all other individuals whose biometric data was processed by the technology on the relevant occasions.[62] The Court of Appeal disagreed, noting that Bridges had only pled the impact on himself, not the wider public, in his original complaint.[63] Further, according to the Court, the impact on Mr Bridges was "negligible," and the Court explained that "an impact that has very little weight cannot become weightier simply because other people were also affected."[64] The balancing exercise, according to the Court, "is not a mathematical one; it is an exercise which calls for judgement."[65] The benefits were potentially great, and the impact on Bridges was minor, so the use of AFR was proportionate under Article 8(2). The Court also found it significant 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."[66] The Court therefore found that the use of facial recognition technology was necessary and proportionate to the South Wales Police's law enforcement goals.

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 under Section 64 of the UK's Data Protection Act of 2018. A data protection impact assessment is a is a process that helps organizations identify and minimize the data protection risks of a particular tool, project or technology. Such an assessment "must describe the nature, scope, context and purposes of the personal data processing; assess necessity, proportionality and compliance measures; identify and assess risks to individuals; and identify any additional measures to mitigate those risks."[67] In *Bridges,* the Court rejected the bulk of the applicant's arguments on the SWP assessment's deficiency – namely, that the assessment failed to acknowledge that personal data which were deleted were still 'processed' within the meaning of the data protection law; that the assessment did not mention the rights of individuals under Article 8 of the European Convention on Human Rights; and that it did not acknowledge the risks to freedom of expression and assembly.[68] Nonetheless, the Court agreed with Bridges that the South Wales Police's data protection impact assessment was deficient because it failed to establish the correct legal framework for using automated facial recognition. The Court noted that the assessment "proceed[ed] on the basis that Article 8 . . . is not infringed," and therefore, failed to properly address the requirement that facial recognition be "in accordance with the law."[69] The Court concluded that "[t]he inevitable consequence of those deficiencies is that . . . the DPIA failed properly to assess the risks to the

[62] *Id.* at [136]–[137].
[63] *Id.* at [142].
[64] *Id.* at [143].
[65] *Id.* at [143].
[66] *Id.* at [70].
[67] *Data Protection Impact Assessments*, INFORMATION COMMISSIONER'S OFFICE, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments (last visited May 12, 2021).
[68] Bridges [2020] EWCA Civ 1058 at [147]-[151].
[69] *Id.* at [152].

rights and freedoms of the data subjects" and consequently breached Section 64 of the Data Protection Act 2018.[70]

The Court next addressed the fourth ground of appeal, quickly dismissing it. This ground challenged the use of facial recognition under Section 42 of the Data Protection Act 2018, which sets out what an appropriate policy document relating to data protection matters must contain.[71] However, this ground failed because that provision had not been enacted at the time of the two occasions on which the appellant was captured by AFR Locate.[72]

Finally, the Court addressed Bridges' complaint that the South Wales Police breached their positive duty to have 'due regard' to the need to eliminate potential bias and indirect discrimination associated with automated facial recognition technology.[73] The Court held that the South Wales Police were deficient in fulfilling their public sector equality duty because they failed to recognize the risk that automatic facial recognition profiling could disproportionately impact women and minorities.[74] The Court found that the breach of the public sector equality duty was a "serious issue of public concern."[75] This duty requires 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."[76]

Here, the Court reasoned the South Wales Police had "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."[77] The Court pointed to evidence from computer expert Dr. Anil Jain showing that automated facial recognition can sometimes have unacceptable bias because their training data sets contain a disproportionate number of people from certain demographics.[78] Consequently, the automated facial recognition technology could result in a higher rate of false positives when scanning women or ethnic minorities. The Court did not determine whether the South Wales Police's technology actually resulted in disparate impact.[79] Nevertheless, the Court found 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." Consequently, the Court upheld the fifth and final

---

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

[71] Data Protection Act 2018, c. 2, §42 (UK), https://www.legislation.gov.uk/ukpga/2018/12/section/42.

[72] Bridges [2020] EWCA Civ 1058 at [159].

[73] *Id.* at [165].

[74] *Id.* at [164].

[75] *Id.* at [173].

[76] *Id.* at [179].

[77] *Id.* at [199].

[78] *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.

[79] R (Bridges) [2020] EWCA (Civ) 1058 at [199].

ground of appeal, finding that the South Wales Police had failed to fulfill its public sector equality duty.[80]

III. ANALYSIS AND IMPLICATIONS

Bridges is the first case to consider police use of automated facial recognition technology in public spaces. As such, it has important implications for the rights to privacy and data protection, and for the rights to political protest and democratic participation more generally. Although *Bridges* concerned the legality of facial recognition technology under specific legislation in the U.K., it is emblematic of wider concerns worldwide around the *ad hoc* regulation and discretionary use of automated facial recognition technology by police. This technology is used without an appropriate legal framework to govern its use and without sufficient oversight or public awareness. Meanwhile, governments can use algorithmic and biometric technologies to discriminate against various groups. Thus, while *Bridges* is a landmark ruling about the limits of police discretion when using automated facial recognition technology, the long-term impact of the Court's pronouncement on future expansion and deployment of automated surveillance technologies in public spaces is much weaker. In particular, the Court found that the deployment of facial recognition technology for mass surveillance in public spaces was acceptable and proportional to law enforcement goals. And the Court did not mandate increased transparency or require that the police publicly release clear information about their operation of facial recognition technology. The Court also did not consider how regulatory guidance may fragment across local authorities, making the law less predictable and certain. Instead, the Court imposed minimal formalistic requirements that the police must meet to comply with the public sector equality duty and the right to privacy. I discuss these limitations in turn.

A. Surveillance and Protests in Public Spaces: The Acceptance of the FRT as 'Proportionate'

> "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."[81] –South Wales Police, 2020

Civil rights activists and advocacy organizations, who have long been 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 handed down by the Court of

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

[81] Sebastian Klovig Skelton, *Police Use of Facial Recognition Found 'Unlawful' in Court*, COMPUTERWEEKLY (Aug. 12, 2020), https://www.computerweekly.com/news/252487490/Police-use-of-facial-recognition-found-unlawful-in-court.

Appeal.[82] However, the *Bridges* decision did not ban or limit the use of facial recognition technology to monitor political protests. On the contrary, the Court legitimized the use of facial recognition technology in public places by declaring it proportionate in principle. As a result, the case will likely only be the first among many in the continuing resistance to law enforcement's use of intrusive surveillance technologies in public spaces.

The Court of Appeal acknowledged that automated facial recognition involves "sensitive processing," and that issues in the case are very fact- and circumstance-specific.[83] Thus, its judgment was narrowly confined to issues relating to Bridges' experience with the South Wales Police's use of AFR Locate; it did not analyze AFR Locate's broader impacts. The Court also emphasized what it considered to be two important safeguards: that image data which did not result in a match was automatically deleted[84] and that facial matches made by AFR Locate were reviewed by a police officer.[85] The judgment therefore does not provide *carte blanche* for the police to make arrests solely on the basis of automatic facial recognition without human review. But the decision still affirms the role of automated facial recognition in modern policing and law enforcement.

The *Bridges* ruling does not go far enough to protect public spaces from intrusive surveillance. First, the Court understated the wider impact of facial recognition technology in public spaces on the social fabric of population and on wider democratic participation. The Court held that the South Wales Police's use of facial recognition technology was "not in accordance with the law."[86] But had it been so, its use would have been proportional to law enforcement goals. Indeed, the Court chose to explain this point even though it did not have to.[87] The Court emphasized that, even if 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."[88] In other words, the Court views public space surveillance as small separate harms affecting individuals rather than an aggregate harm affecting the entire population.

The Court focused on the burden on Edward Bridges' individual right to privacy, refusing 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. Bridges raised this point and argued that the Court ought to have taken into account the potential reach of AFR Locate.[89] But the Court flatly rejected this approach, stating that it is neither "necessary [nor] helpful to consider

---

[82] *Liberty Wins Ground-Breaking Victory Against Facial Recognition Tech*, LIBERTY (Aug. 11, 2020), https://www.libertyhumanrights.org.uk/issue/liberty-wins-ground-breaking-victory-against-facial-recognition-tech.

[83] *See, e.g,* Bridges [2020] EWCA Civ 1058 at [159]-[162].

[84] *Id.* at [93].

[85] *Id.* at [184].

[86] *Id.* at [131].

[87] *Id.* at [131]-[144].

[88] *Id.* at [143].

[89] *Id.* at [59].

hypothetical scenarios which may arise in the future."[90] It is unclear whether the Court chose not to engage with the wider impact argument because Bridges' appeal did not sufficiently plead 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 of the ECHR was included in the initial legal challenge launched by Bridges before the High Court, but it was not actually argued before that Court and therefore could not be appealed.

Irrespective of its reasons, the Court's opinion understates the wide-ranging implications of surveillance in public spaces. These implications include not only particular individuals' right to privacy, but also the ability of the population as a whole to participate in the political process. NGOs in the UK have been especially concerned about the use of facial recognition technology nationwide to gather intelligence, particularly around protests.[91]

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 built-in 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.[92] Similarly, law enforcement likely used facial recognition technology to scan Black Lives Matters protests in Oakland and Baltimore in 2015.[93] A journalist, who participated in the protests, believes that his arrest near the Black Lives Matter protests in 2014 was due to police use of facial recognition.[94] Facial recognition technology has reportedly been used to monitor and screen crowds during the 2020 protests connected to the killing of George Floyd,[95] and officers in Dallas have actively requested video footage of protest

---

[90] *Id.* at [60].

[91] 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 (Aug. 17, 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.

[92] *Smart lamppost toppled to ground by Hong Kong demonstrators over Chinese surveillance fears*, ABC NEWS (Aug. 24, 2019, 8:58 AM), https://www.abc.net.au/news/2019-08-24/hong-kong-protests-smart-lampposts-cut-down-surveillance-fears/11445606.

[93] Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU NORTHERN CALIFORNIA (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[94] Ali Winston, *Oakland Cops Quietly Acquired Social Media Surveillance Tool*, EAST BAY EXPRESS (Apr. 13, 2016), https://www.eastbayexpress.com/oakland/oakland-cops-quietly-acquired-social-media-surveillance-tool/Content?oid=4747526.

[95] *See* Maya Shwayder, *Police Facial Recognition Tech Could Misidentify Protesters*, DIGITAL TRENDS (June 2, 2020), https://www.digitaltrends.com/news/police-protests-facial-recognition-misidentification/ (The Minneapolis police department denying possession of facial recognition technology).

activity, presumably to run through facial recognition software.[96] These global examples illustrate how police can use facial recognition technology to interfere with protest movements by threatening crowds with monitoring, screening and matching faces, and aiding in potential arrests.

The police deployment of facial recognition technology in public spaces may have a 'chilling' effect on collective action.[97] Protests typically take place in public places. As more public spaces come under surveillance, fewer protesters are truly anonymous. But anonymity is fundamental to protest movements. When people can protest anonymously, they tend to feel confident that they can gather in public spaces, without fear of reprisal, to manifest their disagreement with the *status quo*. For this reason, many scholars have argued that facial recognition technology can result in a chilling effect on dissident speech.[98] Indeed, studies have shown that individuals are less likely to share their opinions, both online[99] and offline,[100] when they feel they are in the minority and feel monitored. And when citizens feel unsafe voicing their opinions, robust democratic participation is not possible.

Therefore, the *Bridges* court's judgment reaffirms, if not strengthens, the legality of the facial recognition technology used for mass surveillance in modern policing. Given the already-existing use of this technology to monitor public protests, and the harmful chilling effects that result, the Court's legitimization of automated facial recognition and the failure to consider its wider impact will be harmful in the long-term.

---

[96] Heather Kelly & Rachel Lerman, *America Is Awash in Cameras, a Double-edged Sword for Protesters and Police*, WASHINGTON POST , (June 3, 2020, 7:00 AM EDT), https://www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters.

[97] *See, e.g.*, Murphy, *supra* note 22; *see also* Matthew Schwartz, Color-Blind Biometrics? Facial Recognition and Arrest Rates of African-Americans in Maryland and the United States (Apr. 15, 2019) (unpublished Master of Public Policy Thesis, Georgetown University) (Georgetown Repository).

[98] *See e.g.*, Roberto Iraola, *Lights, Camera, Action! Surveillance Cameras, Facial Recognition Systems and the Constitution*, 49 LOY. L. REV. 773 (2003); Murphy, *supra* note 22.

[99] *See e.g.*, Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMMC'N Q. 296 (2016); Jonathon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117 (2016); 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.

[100] *See e.g.*, Carroll J. Glynn et al., *Perceived support for one's opinions and willingness to speak out: A meta-analysis of survey studies on the "spiral of silence."*, 61 PUB. OP. Q. 452 (1997); Dietram A. Scheufele & Patricia Moy, *Twenty-five years of the spiral of silence: A conceptual review and empirical outlook*, 12 INT'L J. PUB. OP. RES. 3 (2000).

IV. DISCRIMINATION AND COMMERCIAL SECRECY: A LIMITED JUDICIAL DEMAND FOR TRANSPARENCY

> "This judgment is a major victory in the fight against discriminatory and oppressive facial recognition. The Court has agreed that this dystopian surveillance tool violates our rights and threatens our liberties."[101] – 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 and the public's inability to investigate the technologies' operation because of trade and commercial secrecy barriers. The Court made a number of remarks suggesting that, to comply with its equality duties, the South Wales Police's use of facial recognition technology software should be more transparent—or at least independently reviewable. Even before *Bridges*, the UK Equality and Human Rights Commission had called for a moratorium on facial recognition technology in England and Wales pending independent scrutiny of the discriminatory impact the technology may have on protected groups.[102] In *Bridges*, the Court of Appeals expressly held that the South Wales Police breached its public sector equality duty because *it did not independently seek to verify* whether or not the software could give rise to bias.[103] This judgment is important because it puts the onus on police to carefully select and scrutinize the technologies they buy from private companies. This scrutiny may require companies to reduce the discriminatory impact of their technology if they seek to sell to government agencies.[104]

An increasing body of academic research has demonstrated the discriminatory effects of facial recognition technology—and surveillance generally—on minority groups.[105] The emerging consensus is that facial recognition technologies are not "neutral"[106] but instead reinforce historical inequalities.[107] For example, studies have shown that facial recognition technology performs poorly when applied to

---

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

[102] *Facial recognition technology and predictive policing algorithms out-pacing the law*, EQUALITY AND HUMAN RIGHTS COMMISSION (Mar. 12, 2020), https://www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law.

[103] R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [199] (Eng.).

[104] Martin Kwan, *Ensuring the lawfulness of automated facial recognition surveillance in the UK*, OXFORD HUMAN RIGHTS HUB (Sep. 3, 2020), https://ohrh.law.ox.ac.uk/ensuring-the-lawfulness-of-automated-facial-recognition-surveillance-in-the-uk.

[105] Clare Garvie et al., *The Perpetual Line-Up* (Oct. 18, 2016), https://www.perpetuallineup.org/; Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE TRANSACT. ON INFO. FORENSICS & SEC. 1789 (2012); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *in* 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[106] Garvie et al., *supra* note 105; Klare et al., *supra* note 105; Buolamwini & Gebru, *supra* note 105.

[107] Schwartz, *supra* note 97, at 15.

women, children, and individuals with darker skin tones.[108] Such poor performance is concerning because groups that have been historically discriminated against and marginalized may be discriminated against further. This kind reinforced discrimination is particularly important in the law enforcement context because training data for facial recognition technologies comes from photos relating to previous arrests and convictions.[109] Thus, minority groups are overrepresented in facial recognition technology training databases.[110] This is especially true in jurisdictions like the United States, where racial minorities face a much higher risk of being pulled over,[111] searched,[112] arrested,[113] incarcerated,[114] and wrongfully convicted.[115] Under these circumstances, facial recognition technology is capable of producing a large number of false positives for individuals from overpoliced communities because it operates against a background of structural inequality and discrimination. A false positive is when a system says that two images are of the same person when, in fact, they are not. The rate of such false positives is much higher for African-American population, which is over-represented in criminal databases, leading to wrong members of this demographic to be arrested.

The *Bridges* Court acknowledged that it would be difficult to detect or measure any discriminatory impact of the AFR Locate system because a 'safeguard' "would instantly delete the majority of profiles registered by the system."[116] The Court recognized that details of the training dataset could not be made public due to "commercial confidentiality," yet, the Court held that "it does not enable a public

---

[108] Salem Hamed Abdurrahim et al., *Review on the effects of age, gender, and race demographics on automatic face recognition*, 34 INT'L J. OF COMPUT. GRAPHICS 1617 (2018), https://link-springer-com.wwwproxy1.library.unsw.edu.au/content/pdf/10.1007/s00371-017-1428-z.pdf; Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots*, ACLU, (July 26, 2018, 8:00 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[109] Ruhrmann, *supra* note 2, at 46; Garvie et al. *supra* note 105.

[110] Ruhrmann, *supra* note 2, at 63; Garvie et al., *supra* note 105.

[111] Nusrat Choudhury, *New Data Reveals Milwaukee Police Stops Are About Race and Ethnicity*, AMERICAN CIVIL LIBERTIES UNION , (Feb. 23, 2018, 2:45 PM) https://www.aclu.org/blog/criminal-law-reform/reforming-police/new-data-reveals-milwaukee-police-stops-are-about-race-and; FRANK R. BAUMGARTNER ET AL., SUSPECT CITIZENS WHAT 20 MILLION TRAFFIC STOPS TELL US ABOUT POLICING AND RACE (2018).

[112] Choudhury, *supra* note 111; Camelia Simoiu, Sam Corbett-Davies & Sharad Goel, The Problem of Infra-Marginality In Outcome Tests for Discrimination 11 ANN. APPL. STAT. 1193–1216 (Sept. 2013); Lynn Lanton, *Police Behavior during Traffic and Street Stops*, US DOJ, *(*Sept. 2013*)*, https://www.bjs.gov/content/pub/pdf/pbtss11.pdf.

[113] C*riminal 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 B.U. L. REV. 371 (2018).

[114] Ashley Nellis, T*he Color of Justice: Racial and Ethnic Disparity in State Prisons*, THE SENTENCING PROJECT (June 14, 2016), https://www.sentencingproject.org/publications/color-of-justice-racial-and-ethnic-disparity-in-state-prisons.

[115] Samuel Gross et al., *Race and Wrongful Convictions in the United States*, NATIONAL REGISTRY OF EXONERATIONS, (Mar. 7 2017), http://www.law.umich.edu/special/exoneration/Documents/Race_and_Wrongful_Convictions.pdf.

[116] R (ON THE APPLICATION OF EDWARD BRIDGES) V. THE CHIEF CONSTABLE OF SOUTH WALES POLICE [2020] EWCA CIV 1058, [191] (ENG.).

authority to discharge its own, non-delegable, duty."[117] To the extent *Bridges* protects individual rights, it is because it puts the onus on the police and the legislature to provide appropriate safeguards against the discriminatory application of automated facial recognition technology.[118] 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."[119]

However, it is unclear what steps can be taken to ensure that facial recognition technologies are applied equally with respect to the characteristics protected under the public sector equality duty. In particular, the relationship between private companies developing automated facial recognition software and police departments who employ them is based on corporate secrecy laws and procurement practices. Facial recognition software is considered a trade and commercial secret and is not shared with police or any other parties.[120] Such secrecy, some scholars note, "fails to foreground the public interest[.]"[121] Importantly, commercial secrecy may entirely preclude the use of facial recognition technologies by UK public agencies if it prevents them from complying with their public sector equality duty.

Therefore, when government agencies procure private technologies, such technologies should be open-source and the procurement contracts should be transparent. The procurement practices should be standardized in legislation. For example, the original draft of the 2019 Washington State House Bill 1655 would have addressed some of these concerns.[122] This legislation, which has now been substituted, likely because of industry pressure, included sections banning nondisclosure provisions,[123] and required that all automated decision systems and the data used in the system be made "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."[124] While these provisions were removed from the substitute bill, they

---

[117] *Id.* at [199].

[118] Surveillance Camera Commissioner & Tony Porter, *Surveillance Camera Commissioner's Statement: Court of Appeal judgment (R) Bridges v South Wales Police – Automated Facial Recognition*, GOV.UK (Aug. 11, 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.

[119] R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [181] (Eng.).

[120] *See, e.g.*, Wexler, *supra* note 26, at 1346; Deven R. Desai & Joshua Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J. LAW & TECH. 1, 9 (2017); Andrew D. Selbst & Solon Barocas, *The Intuitive Appeal of Explainable Machines*, 87 FORDHAM L. REV. 1085, 1091-1093 (2018).

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

[122] H.B. 1655, 66th Leg., 2019 Reg. Sess. (Wash. 2019).

[123] Wash. H.B. 1655 at § 4(4).

[124] Wash. H.B. 1655 at §4(3)(b). Both sections 4(4) and 4(3b) have been removed from the Substitute Bill, which is still before the House Committee. Substitute H.B. 1655, 66th Leg., 2019 Reg. Sess. (Wash. 2019).

demonstrate one potential way to regulate procurement contracts in the public interest.

However, to foreground the public interest even further, police and other public authorities should only use facial recognition technologies if they are open source. In the Court's 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.[125] But this does not go far enough: it is hard to justify commercial secrecy when the technology has such a significant impact on the rights of the public. Compliance with the public sector equality duty requires built-in transparency and accountability safeguards in relevant commercial contracts and in the designs of technologies themselves. Such safeguards should be a prerequisite for technology companies seeking to sell their software to government agencies.

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"[126] – 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."[127] – South Wales Police, 2020

Despite the Court's insistence on more procedural safeguards and transparency, the judgment left a lot of room for fragmentation and divergence in police practices around the use of facial recognition technology. In particular, the Court reasoned that the South Wales Police's local policies would constitute "law" under Article 8 of the ECHR: "As we have said, in principle a police force's local policies can constitute relevant 'law' in the present context, provided they are published."[128] Instead of emphasizing the need for legislative reform on a national scale, 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 facial recognition technology policies across the U.K.

This is concerning, as police use of facial recognition technology in the United Kingdom is only likely to expand. London police plan to integrate the technology

---

[125] R (on the application of Edward Bridges) v. The Chief Constable of South Wales Police [2020] EWCA Civ 1058, [199] (Eng.).

[126] Amy Smethurst, *Facial Recognition - What is the impact of the Bridges case?*, JMW (Aug. 19, 2020), https://www.jmw.co.uk/services-for-you/media-law/blog/facial-recognition-what-impact-bridges-case.

[127] *Id*.

[128] Bridges [2020] EWCA Civ 1058 at [121].

with the CCTV and Automatic Number-Plate Recognition network.[129] There are plans to use facial recognition technology on video footage taken from mobile devices, CCTV, and police body cameras after the fact.[130] There are also plans for mobile facial recognition technologies which integrate biometric tracking software across multiple devices.[131] In early 2020, the Metropolitan Police Service in London announced that it would roll out live facial recognition as part of its general policing strategy.[132] Facial recognition is becoming and essential tool of modern policing and is here to stay.

If law enforcement use of facial recognition technology is not comprehensively regulated, the *ad hoc* and fragmented regulatory framework will reduce the predictability and consistency of police action. It will enable police departments, as well as other public and private agencies, to share citizens' information among themselves with little transparency or oversight. For example, in the United States, law enforcement agencies in at least 40 states use facial recognition technology in the absence of a federal regulatory framework.[133] State and federal agencies also promote inter-agency access to facial recognition databases, enlarging the size of the population over which individual jurisdictions hold biometric information.[134] Police also actively collaborate with other public authorities and private corporate entities. For instance, the New-York-based company Clearview AI claims to have a database of over three billion images.[135] Their software was purportedly used by over 600 law enforcement agencies in 2019 and 2020.[136] Even if a police department has stringent collection and storage guidelines, that department may share the information with other police departments lacking such safeguard requirements, thereby defeating the purpose of such protective policies. The *ad hoc* regulation of facial recognition technology use in the United States illustrates the risks of granting police departments too much discretion. Allowing police

---

[129] Big Brother Watch, *supra* note 33, at 31.

[130] *Id.* at 32.

[131] *Id.* at 32–33.

[132] James Vincent, *London police to deploy facial recognition cameras across the city*, THE VERGE (Jan. 4 2020), https://www.theverge.com/2020/1/24/21079919/facial-recognition-london-cctv-camera-deployment.

[133] *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*, 116th Cong. 7 (2019) (statement of Kimberly Del Greco, Criminal Justice Information Servs. Div.).

[134] Gretta Goodwin, *Face Recognition Technology: DOJ and FBI have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, but Additional Work Remains*, US GAO (Jun. 4, 2019) https://www.gao.gov/assets/700/699489.pdf. 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. Garvie et al., *supra* note 105. As of 2019, the FBI reports that 14 states had access to their Next Generation Identification technology. *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*, 116th Cong. 7 (2019) (statement of Kimberly Del Greco, Criminal Justice Information Servs. Div.).

[135] Jordan Valinsky, *Clearview AI Has Billions of Our Photos. Its Entire Client List Was Just Stolen*, CNN BUSINESS (Feb. 26, 2020), https://www.cnn.com/2020/02/26/tech/clearview-ai-hack/index.html; Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[136] Hill, *supra* note 135.

departments to effectively write their own rules undermines the basic protections for citizens that sound public policy, as well as the courts, should seek to preserve.

Instead of enabling police departments to rely on their internally developed 'local policies' to meet the 'in accordance with law' standard, the Court of Appeals should have encouraged the development of a comprehensive regulatory framework. This framework could be implemented through amendments to the Data Protection Act 2018, the Surveillance Camera Code of Practice, or by an entirely new law. Legislative intervention could prevent fragmentation and limit undue police discretion. Currently, the Automated Facial Recognition Technology (Moratorium and Review) Bill proposes to ban the use of technologies in the UK.[137] However, it is unlikely to be enacted, given the long history of use of CCTV and facial recognition technology in the UK.

The *Bridges* decision opened the door for police to use facial recognition technology, but it left the regulation of this technology to other courts and policymakers. Other jurisdictions are in the process of considering such regulation. For example, in the US, the Algorithmic Accountability Act was introduced in the House of Representatives,[138] while New York City's Public Oversight of Surveillance Technology Act[139] was introduced and has increased transparency around the New York Police Department's use of facial recognition technology.[140]

A legal action launched in 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 that jurisdiction. The claim focuses on provisions in the French Criminal Code of Procedure which authorizes police use of facial recognition to identify people registered in a police criminal record database. This database called the *"Traitement des antécédents judiciaires"* contains 19 million files and more than eight million images of people.[141] The ACLU is bringing similar challenges before U.S. courts. In October 2019, it 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 utilized under the Freedom of Information Act. The case was filed after the ACLU made a freedom of information request in January of 2019, and the DOJ, FBI, and DEA failed to produce any responsive documents.[142]However, it remains to be seen whether these challenges will result in more stringent, comprehensive regulation of police use of

---

[137] Automated Facial Recognition Technology (Moratorium and Review) Bill 2019-20, HL Bill [87] (UK).

[138] Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019).

[139] *See* NEW YORK CITY ADMIN. CODE § 14-188 (2020).

[140] Max Pellegrini, *Facial-Recognition Technology Requires Smart Legislation*, CRAIN'S NEW YORK BUSINESS (2019), https://www.crainsnewyork.com/op-ed/facial-recognition-technology-requires-smart-legislation.

[141] La Quadrature du Net, *supra* note 16.

[142] *ACLU Challenges FBI Face Recognition Secrecy*, AM. CIV. LIBERTIES UNION (Oct. 31, 2019), https://www.aclu.org/press-releases/aclu-challenges-fbi-face-recognition-secrecy.

facial recognition technology, or whether the current *ad hoc* and fragmented regulatory framework will continue.

V. CONCLUSION

The *Bridges* decision is an important first step in limiting police discretion over the use of facial recognition technology. But it is far from a great victory for those opposed to the expansion of surveillance infrastructure in public spaces. The Court has underplayed, if not explicitly rejected, facial recognition technologies' wide-ranging impact on public participation, public life, and civil discourse. The Court also did not require transparency as a prerequisite for the use of facial recognition technology, which can remain shielded behind trade secret law. Nor did the Court insist on any comprehensive legislative reform, leaving room for inconsistent and fragmented regulation of these technologies in the future.

Notwithstanding the Court's short-sighted analysis, facial recognition infrastructure in public spaces not only impacts the individual's right to privacy and ability to pass through public spaces but also burdens the population's ability to act collectively. The presence of facial recognition technology in public spaces is not merely a 'negligent' invasion of privacy, but cuts to the heart of democratic participation. The Court in *Bridges* considered the use of automated facial recognition technology "proportionate" to law enforcement's goals—but only because the Court did not take into account these broader societal concerns. The Court failed to engage directly with questions of democracy, public participation, and individual identity in public spaces. It therefore missed an opportunity to balance law enforcement goals with the broader democratic value 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 facial recognition technology did not address the barriers preventing public officials from determining whether the technology they use satisfies their legal obligations. Although the Court acknowledged the need for safeguards when government agencies use cutting edge surveillance technologies, it left development of specific safeguards to the police. It is unclear what safeguards would satisfy the Court's standard. Would the creation of an independent advisory board with access to the software be sufficient? And can such a board genuinely demonstrate to any public authority that the technology applies to all persons if there is no way to know how it operates? The tension between trade secrecy laws and public governance is not easily resolvable, and the Court could have signaled the direction in which the balance should be tipped. It is hard to see why police forces should be able to use the technologies 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 much room for fragmentation in the regulatory framework overseeing police use of automated facial recognition technologies. By accepting that a local 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 distinct guidelines. National legislative reform could ensure consistency and predictability in police use of facial recognition technology. Other courts will have to more firmly demand comprehensive reforms in the future.

The Court of Appeal's decision in the *Bridges* case has sparked a public debate on the use of automated facial recognition technology. By requiring police departments to rethink their deployment of the technology, the Court opened the door for reform on police use of biometric technologies more generally. The Court signaled that some regulation of such technology was appropriate. Instead of allowing individual police departments to invent the rules as they go, legal limits on the use of automated facial recognition must be clearly articulated in advance. However, the Court has also given police forces significant leeway to define these limits through their own policies rather than insisting on legislative intervention. Importantly, the Court held that the use of facial recognition for mass surveillance in public places is proportional to the goals of modern policing. Because it demands clearer limits on police discretion, the *Bridges* decision is reassuring in the short term. But its long-term impact in burning the bridges between the expanding public space surveillance infrastructure and the modern state is much weaker, if not damaging.