NOTES

DOES THE RIGHT TO PRIVACY APPLY TO FACIAL BIOMETRICS? SPECIFICALLY, WHEN ANALYZED UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS

Grace Callanan[*]

TABLE OF CONTENTS

[*]J.D., University of Georgia School of Law, 2021. B.A. in Political Science, Virginia Tech, 2018. This Note is dedicated to my family, for all their unwavering support.

I. INTRODUCTION

Not only are technological innovations proliferating by the day, current technology is also expanding in both capability and use. One technology in particular is being used in numerous new ways by a variety of groups: facial-recognition technology (FRT).[1] Private companies are utilizing FRT in a number of ways that enhance the personalized nature of their products, but foreign governments have also been testing out uses of the technology.[2] One of the ways governments have used FRT is to assist police in criminal identification.[3] However, many critics warn that police use of FRT violates privacy rights and Congress should introduce legislation to protect these rights.[4] Some localities have gone as far as enacting laws prohibiting local government from using FRT on citizens.[5] In the 2019 case of *Bridges v. Chief Constable of S. Wales Police*, a Welsh citizen sued the South Wales Police Department alleging a violation by the police department of his privacy rights under several laws, including the European Convention on Human Rights.[6] The Court said "the case was the first of its kind worldwide."[7] This Note is divided into two major sections. The first section provides information on how FRT generally works, how FRT is being used differently by private and public organizations, and how various countries and localities are either using FRT or reacting to the possible use of FRT. The second section explores the *Bridges* case in more detail, discussing the Plaintiff's claims, analyzing the lower and appellate Welsh court's reasoning, what the appellate court found, and assessing how the case would likely play out if appealed to the European Court of Human Rights. If appealed, the European Court of Human Rights will most likely affirm the initial *Bridges* ruling that Facial Recognition Surveillance does not violate Article 8 of the European Convention on Human Rights. Lastly, this

---

[1] Steve Symanovich, *How Does Facial Recognition Work?*, NORTON SECURITY (Feb. 8, 2019), https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html.

[2] Ryan Browne, *Tech Giants Want Rules on Facial Recognition, but Critics Warn that Won't be Enough*, CNBC (Aug. 30, 2019, 1:26 AM), https://www.cnbc.com/2019/08/30/facial-recognition-tech-firms-want-regulation-but-critics-want-a-ban.html.

[3] *Id.*

[4] *Id.*

[5] Shirin Ghaffary, *San Francisco's Facial Recognition Technology Ban, Explained*, VOX (May 14, 2019, 7:06 PM), https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained.

[6] *British Activist to Appeal 'Sinister' Police Facial Recognition*, REUTERS (Sept. 4, 2019, 12:42 PM), https://www.reuters.com/article/us-britain-tech-privacy/british-activist-to-appeal-sinister-police-facial-recognition-idUSKCN1VP2CI.

[7] *Id.*

Note considers whether and how the *Bridges* decisions shape current international privacy norms.

II. BACKGROUND

FRT is being used by private and public entities increasingly each day. One of the most highly advertised features of the iPhone is its "Face ID" capability, which is an example of FRT being utilized by private entities.[8] It is important to understand how facial recognition works. Put simply, the technology is "[a] facial recognition system [that] uses biometrics to map facial features from a photograph or video. It compares the information with a database of known faces to find a match."[9] While various FRT systems may operate differently, there are some basic steps. First, a photo or video registers a face and captures the face.[10] Next, the system will "read[] the geometry of" the face, including factors like "the distance between your eyes and the distance from forehead to chin.[11] The software identifies facial landmarks—one system identifies 68 of them—that are key to distinguishing your face."[12] The result is known as the facial signature.[13] Third, the resulting facial signature "is compared to a database of known faces."[14] Lastly, a determination is made on whether the facial signature matches a face within the database.[15] After providing a basic understanding of how the technology works, this Note now focuses on how personal facial biometric data can be used.

Many people are aware of the use of FRT by mobile devices, but how else is this technology being used? Both private and government entities are using FRT in more ways than one could imagine. For example, the Ontario Lottery and Gaming Corporation uses FRT on some of its slot machines to identify problem gamblers.[16] Additionally, some hotels use FRT so that concierges can greet customers by name, there are dating apps that proclaim to match individuals with similar facial features, and some colleges use FRT to take attendance in class.[17]

---

[8] *About Face ID Advanced Technology*, APPLE INC. (Feb. 26, 2020), https://support.apple.com/en-us/HT208108.

[9] Symanovich, *supra* note 1.

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] Ysolt Usigan*, 7 Surprising Ways Facial Recognition is Used*, CBS NEWS (Aug. 5, 2011, 1:56 PM), https://www.cbsnews.com/pictures/7-surprising-ways-facial-recognition-is-used/2/.

[17] *Id*.

Law enforcement also uses FRT to catch known identity thieves when they are applying for driver's licenses.[18] A more well-known use of FRT is on Facebook. When users upload pictures, Facebook scans faces in each picture and suggests "tagging" the people it believes those faces belong to.[19] According to Facebook, the software accurately identifies a face ninety-eight percent of the time.[20] As FRT usage across all industries becomes more prevalent, the market for this technology is simultaneously growing, expecting to jump from a $4 billion industry in 2017 up to $7.7 billion in 2022.[21]

Like private entities, government entities are also utilizing FRT. In 2016, Georgetown Law conducted a study finding that "more than half of American adults were enrolled in a face recognition network searchable by law enforcement."[22] Some organizations based in the United States are wary of FRT and fear that its use may infringe on constitutional rights because the technology "can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject."[23] One of the major concerns about FRT in the United States is that photographs of citizens from state motor vehicle agencies could be used in conjunction with public video surveillance to create a system that identifies and tracks citizens.[24]

In fact, the United States Government Accountability Office reported that, "[s]ince 2011, the FBI had logged more than 390,000 facial-recognition searches of federal and local databases, including state [Department of Motor Vehicles (DMV)] databases . . . ."[25] Immigration and Customs Enforcement agents have also utilized DMV records for facial recognition purposes in states that allow undocumented immigrants to obtain driver's licenses or permits.[26] The FBI has responded to criticism of FRT usage, stating, "while facial-recognition searches can provide helpful leads, agents are expected to verify the findings and secure

---

[18] *Id.*

[19] Symanovich, *supra* note 1.

[20] Naomi Lachange, *Facebook's Facial Recognition Software is Different from the FBI's. Here's Why*, NPR (May 18, 2016, 9:30 AM), https://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why.

[21] Symanovich, *supra* note 1.

[22] *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO. L. CTR. ON PRIV. & TECH., https://www.law.georgetown.edu/privacy-technology-center/publications/the-perpetual-line-up/ (last visited Mar. 29, 2021).

[23] *Face Recognition Technology*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology (last visited Mar. 29, 2021).

[24] *Id.*

[25] Drew Harwell, *FBI, ICE Find State Driver's License Photos are a Gold Mine for Facial-Recognition Searches*, WASH. POST (July 7, 2019, 3:54 PM), https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

[26] *Id.*

definitive proof before pursuing arrests or criminal charges."[27] Twenty-one states and the District of Columbia allow federal agencies to scan driver's license photos, and the FBI has access to more than 641 million photos for facial-recognition searches.[28] While concerns about FRT inaccurately identifying individuals leading to false arrests are significant, this Note focuses on a critical issue of FRT use: the right to privacy.[29]

FRT is being utilized by various parties across the world, and public reaction to the technology differs. San Francisco was the first major city in the United States to ban local government from using the technology after catching wind of its critiques and possible violation of privacy.[30] Other American cities, such as Oakland, California, and Somerville, Massachusetts, also proposed or passed legislation banning government use of FRT.[31]

Germany's Ministry of the Interior began a pilot program in 2017 using FRT in the Berlin Südkreuz railway station.[32] In order to gain participants for the program, "the ministry recruited around 300 volunteers who agreed, in exchange for a €25 Amazon voucher, to have their names and two biometric photos stored in a database and to carry a transponder around with them."[33] Requiring participants to carry a transponder allowed the authorities to track when participants travelled through the station.[34] The second phase of the program tested whether cameras could identify suspicious behavior in real-time.[35] However, many Germans were unpleased with these new security measures in place; critics of the pilot program worry the technology "is insufficiently transparent and exposes citizens to invasions of privacy, especially if their data is kept on file."[36] Germans, after experiencing "two surveillance states" during the Nazi and East German communist regimes, are especially wary about invasions of personal privacy.[37]

China is using FRT in a multitude of ways, from law enforcement to social uses. Cameras on lamp posts, outside buildings, and on streets are able to

---

[27] *Id.*

[28] *Id.*

[29] Catie Edmondson, *ICE Used Facial Recognition to Mine State Driver's License Databases*, N.Y. TIMES (July 7, 2019), https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html.

[30] Ghaffary, *supra* note 5.

[31] *Id.*

[32] Janosch Delcker, *Big Brother in Berlin*, POLITICO (Sept. 13, 2018, 10:57 AM), https://www.politico.eu/article/berlin-big-brother-state-surveillance-facial-recognition-technology/.

[33] *Id.*

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Id.*

recognize Chinese citizens.[38] Moreover, some public housing projects use FRT to prevent illegal subletting, allowing only residents and delivery persons to enter.[39] Chinese law enforcement "use[s] facial recognition to pluck persons of interest from concert crowds, and have even used wearable Google Glass-style devices that allow a cop to scan the face of anyone they're looking at."[40] Chinese citizens found a way to possibly avoid FRT usage.[41] As noted in media coverage, "[m]any protesters now cover their faces, and they fear that the police are using cameras and possibly other tools to single out targets for arrest."[42]

In Wales, the South Wales Police began a pilot program using FRT, allowing officers to monitor the movement of people in specific locations.[43] The Police explained that camera positions would be used to identify people who were on a pre-determined watch list. The makeup of each watch list could include wanted persons or persons suspected of criminality, missing persons, and persons of interest.[44] The Police also said FRT could be used for both public safety and national security purposes, including for uses such as identifying individuals during a disturbance, or maintaining the security of high-traffic places.[45]

The South Wales Police call the program "AFR Locate," for automated facial recognition technology.[46] It can be used in "live-time" and compares live images from cameras placed around the city against a predetermined watchlist of persons of interest.[47] The program was used around fifty times between May 2017 and April 2019.[48] The South Wales Police created a website that provides the basis of the technology, upcoming events where they are utilizing the program, past events where they used the program, and frequently asked questions and

---

[38] Arjun Kharpal, *China's Surveillance Tech is Spreading Globally, Raising Concerns About Beijing's Influence*, CNBC (Oct. 8, 2019, 1:18 AM), https://www.cnbc.com/2019/10/08/china-is-exporting-surveillance-tech-like-facial-recognition-globally.html.

[39] Tom Simonite, *Behind the Rise of China's Facial-Recognition Giants*, WIRED (Sept. 03, 2019, 7:00 AM), https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants/.

[40] *Id.*

[41] Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, N.Y. TIMES (July 26, 2019), https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

[42] *Id.*

[43] *Introduction of Facial Recognition into South Wales Police*, S. WALES POLICE, https://afr.south-wales.police.uk/ (last visited Apr. 13, 2021).

[44] *Id.*

[45] *Id.*

[46] *Id.*

[47] *Id.*

[48] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

answers.[49] The website reassures citizens "[f]aces that are not matched against the watchlist are not remembered or kept," and "[p]eople not featured in a watchlist can't be identified."[50]

While the South Wales Police support the use of FRT, not all Welsh citizens feel similarly.[51] In 2019, Ed Bridges brought the first major legal challenge against the use of FRT by the South Wales Police.[52] Bridges believes his face was scanned by the Wales Police twice—once during busy holiday shopping and once during a peaceful protest.[53] Bridges stated that the van equipped with FRT "was parked directly opposite" of a "peaceful demonstration—seemingly aimed at discouraging us from lawfully exercising our right to protest."[54] At the core of Bridges' argument is his belief that the use of FRT by the police violates citizens' privacy. Bridges is also concerned about FRT's behavioral effect on privacy, such as people feeling scared to protest.[55] Along with his privacy infringement claim, Bridges argues the technology the police are using is highly flawed, with ninety-one percent of their 'matches' being misidentifications, totaling 2,451 people wrongly identified.[56] Based on these concerns, Bridges sued the Chief Constable of South Wales Police in *Bridges v. Chief Constable of S. Wales Police*, claiming a violation of his privacy rights under the Welsh Equality Act of 2010, the European Convention on Human Rights, and the Data Protection Acts of 1998 and 2018.[57] On September 4, 2019, the High Court in Wales dismissed the case.[58] Afterwards, Bridges publicly stated that he would appeal the decision.[59] The case was appealed to the Court of Appeal and it ruled in Bridges's favor on August 11, 2020, finding that the use FRT by the police violated Article 8 of the European Convention on Human Rights.[60] The remainder of this Note

---

[49] *Introduction of Facial Recognition into South Wales Police*, *supra* note 43.

[50] *Id.*

[51] *Police Facial Recognition Technology Rules 'Need Tightening*,*'* BBC NEWS (May 23, 2019), https://www.bbc.com/news/uk-wales-48383920.

[52] *Id.*

[53] Ed Bridges, *End Lawless and Dangerous Police use of Facial Recognition Technology*, CROWDJUSTICE, https://www.crowdjustice.com/case/facial-recognition/ (last visited Mar. 31, 2021).

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *5 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

[58] *Id.*

[59] *British Activist to Appeal 'Sinister' Police Facial Recognition*, *supra* note 6.

[60] Lara White & Janine Regan, *Key Takeaways for the Private Sector from The Bridges v South Wales Police Facial Recognition Case*, NORTON ROSE FULBRIGHT (Aug. 27, 2020), https://www.dataprotectionreport.com/2020/08/key-takeaways-for-the-private-sector-from-the-bridges-v-south-wales-police-facial-recognition-case/.

discusses the Courts' reasoning in *Bridges*, and whether, if appealed all the way to the European Court of Human Rights, the European Court of Human Rights would find a violation of the European Convention on Human Rights, and lastly, how those decisions might shape international privacy norms.

III. ANALYSIS

Wales is a part of the United Kingdom, and the United Kingdom is a member of the Council of Europe.[61] The forty-seven states that are members of the Council of Europe are all parties to the European Convention on Human Rights.[62] The idea for the European Convention on Human Rights arose during the Second World War in the 1940s.[63] The convention was adopted in 1950 and entered into force in 1953.[64] Agreement to the convention is a prerequisite for joining the Council of Europe.[65] If an individual feels that their rights under the convention have been violated, they may bring a complaint to the Strasbourg Court when they have exhausted all their appeal opportunities in their member state's courts.[66]

There are fifty-nine Articles in the heart of the European Convention on Human Rights.[67] Bridges claimed his rights were violated under Article 8 of the Convention.[68] Article 8, the "[r]ight to respect for private and family life," states the following:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

---

[61] *Our Member States*, COUNCIL OF EUROPE, https://www.coe.int/en/web/about-us/our-member-states (last visited Mar. 31, 2021).

[62] *What is the European Convention on Human Rights?*, AMNESTY INT'L UK (Aug. 21, 2018, 4:47 PM), https://www.amnesty.org.uk/what-is-the-european-convention-on-human-rights.

[63] *Id.*

[64] *Id.*

[65] *The European Convention on Human Rights: A Convention to Protect your Rights and Liberties*, COUNCIL OF EUROPE, https://www.coe.int/en/web/human-rights-convention/home (last visited Mar. 31, 2021).

[66] *Id.*

[67] European Convention on Human Rights, COUNCIL EUR., https://www.echr.coe.int/Documents/Convention_ENG.pdf (last visited Mar. 31, 2021).

[68] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *10 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

> 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.[69]

Moreover, Bridges brought claims under the Data Protection Acts (DPA) of 1998 and 2018 and the Public-Sector Equality Duty Claim; however, this Note does not discuss Bridges' claims under these laws in detail because they do not have the same international significance as the convention. The *Bridges* case has been heard by a lower-level court, the High Court of Wales, and an appellate court, the Court of Appeal. Both decisions will be briefly discussed here.

In the first decision of the *Bridges* case, the High Court of Wales looked at Bridges' claim that the South Wales Police's use of AFR Locate violated Article 8 of the European Convention on Human Rights.[70] The court acknowledged that the use of FRT was "technology of the sort that must give pause for thought because of its potential to impact upon privacy rights."[71] The court further recognized the warranted concern of FRT usage, quoting "the Grand Chamber of the Strasbourg Court" in *S v. United Kingdom*:

> [T]he protection afforded by art.8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests . . . any state claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.[72]

In determining whether the police violated Article 8 of the Convention, the court first looked at the "reach" of Article 8.[73] The opinion acknowledged that while Article 8 has its limits, it is still a broad law.[74] The words "private life"

---

[69] European Convention on Human Rights, *supra* note 67.

[70] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *10 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

[71] *Id.*

[72] *Id.* (quoting S v. United Kingdom, 2008 Eur. Ct. H.R. 32).

[73] *Id.*

[74] *Id.*

comprise many spheres of life and can "embrace multiple aspects of a person's 'physical and social identity,' including . . . gender, name, other means of personal identification and of linking to a family, ethnic identity, and elements relating to a person's right to their image."[75]

To find for Bridges, the court would have had to conclude his rights were violated under Article 8, and then determine the use of FRT by the police was not in accordance with the law or unnecessary for the listed reasons in Article 8(2).[76] In determining whether the technology infringed upon Bridges' privacy, the court noted that in another case "where state actions complained of were 'expected and unsurprising,' it might well be that such actions might entail no breach of Article 8(1)" and stated that merely taking pictures of citizens in public spaces, without aggravating circumstances, was not an infringement of Article 8 rights.[77] However, the court deemed that AFR Locate could not be characterized the same way as merely taking a photograph could be.[78] The court reasoned the two instances were much different because in AFR Locate, "[t]he digital information that comprises the image is analysed and the biometric facial data is extracted. That information is then further processed when it is compared to the watchlists information. The fact that this happens when the Claimant is in a public space is not a sufficient response."[79] Further, the court noted that "[t]he extraction and use of the Claimant's biometric data takes the present case well beyond the 'expected and unsurprising.'"[80] Once again, the decision quoted the European Court of Human Rights, which previously stated, "[t]he mere storing of data relating to private life of an individual amounts to an interference within the meaning of art.8.'"[81] Much like fingerprints or DNA, AFR Locate provides "the extraction of unique information and identifiers" which can lead to identification of an individual.[82] The court determined the time period of the retention of the facial data did not matter; rather, that the collection of data is sufficient under Article 8 if the data is captured, stored, and processed.[83] For reasons

---

[75] *Id.* (citation omitted).

[76] European Convention on Human Rights, *supra* note 67.

[77] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *12 (Eng.) (quoting R . (On the Application of Wood) v. Commissioner of Police of the Metropolis [2010] 1 WLR 123), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

[78] *Id.* at *17.

[79] *Id.* at *12.

[80] *Id.* at *13.

[81] *Id.*

[82] *Id.* at *18.

[83] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *14 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

discussed above, as well as a few other minor factors discussed by the court, the court ruled that the use of AFR Locate did infringe upon Bridges' rights under Article 8 of the European Convention on Human Rights.[84]

The next question in resolving Bridges' claims under Article 8 of the European Convention on Human Rights was the more complex piece of the analysis: Whether the South Wales Police's use of AFR Locate was in accordance with the law.[85] Bridges presented several contentions that the Police's use of FRT was not in accordance with the law.[86] For example, Bridges pointed to legislation that regulated the Police's collection and use of fingerprints and DNA, and noted that there was no similar, or adequate, legal framework for facial recognition technology at the time.[87] Considering that understanding of the police's common law powers, and looking at some applications of that power, the court found that the police did not need express statutory powers in order to use AFR Locate.[88]

Bridges's second contention was that there was no sufficient legal framework for AFR Locate.[89] The court noted that a previous decision found that the necessary qualities of a legal framework were foreseeability, predictability, and legality.[90] In Wales, there are different legal frameworks for obtaining other types of biometric data such as fingerprints and DNA.[91] The court acknowledged that different types of biometric information should be evaluated individually when determining the appropriate legal framework for each.[92]

The court found there was a "clear and sufficient legal framework" to determine when and how AFR Locate could be used by the police.[93] It reasoned that just because the technology was new, the technology was not "outside the scope of existing regulation, or that it is always necessary to create a bespoke legal framework for it."[94] The court asserted that the use of FRT was already regulated in three ways: primary legislation, secondary legislative instruments, like codes, and the local police's own policies.[95] In light of these regulations and common

---

[84] *Id.* at *14.
[85] *Id.* at *15.
[86] *Id.* at *15–16.
[87] *Id.* at *20–21.
[88] *Id.* at *18.
[89] *Id.*
[90] *Id.* (citing R (Gillan) v. Commissioner of Police of the Metropolis [2006] 2 AC 307 at [34]).
[91] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *19 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.
[92] *Id.*
[93] *Id.* at *20.
[94] *Id.*
[95] *Id.*

law, the court found that the use of AFR Locate was "sufficiently foreseeable and accessible for the purpose of the 'in accordance with the law' standard."[96]

The court then considered whether the use of AFR Locate passed a four-part test that was established in a previous case.[97] An interference with Article 8(1) rights is justified if the interference passes the test set forth in *Bank Mellat v. Her Majesty's Treasury*.[98] The four factors in the test are:

> 1. whether the objective of the measure pursued is sufficiently important to justify the limitation of a fundamental right;
>
> 2. whether it is rationally connected to the objective;
>
> 3. whether a less intrusive measure could have been used without unacceptably compromising the objective; and
>
> 4. whether, having regard to these matters and to the severity of the consequences, a fair balance has been struck between the rights of the individual and the interests of the community.[99]

The court deemed that the first two factors were satisfied without much discussion, finding the police force "uses AFR Locate for a legitimate aim, that the legitimate aim is sufficiently important to justify interfering with the Claimant's rights under Article 8" and that the police's "use of AFR Locate is rationally connected to the legitimate aim."[100] Thus, the Court turned to the second two factors to determine fully whether a less intrusive measure could have been used to accomplish the same objective and whether a fair balance was struck.[101]

As noted above, the court did not find for Bridges on any of his claims, and the court therefore dismissed the case on all claims.[102] The court was "satisfied both that the current legal regime is adequate to ensure the appropriate and non-arbitrary use of AFR Locate, and that police force's use to date of AFR Locate has been consistent with the requirements of the Human Rights Act, and the data protection legislation."[103]

---

[96] *Id.*

[97] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *22 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

[98] *Id.*

[99] *Id.*

[100] *Id.* at *22–23.

[101] *Id.* at *23.

[102] *Id.* at *32–33.

[103] *Id.* at *32.

Based on the "sensitive processing of personal data of members of the public" present in the case before them, the court decided to apply a "close standard of scrutiny" when analyzing the third and fourth factors.[104] On the factor of proportionality, Bridges made five claims as to why the use was not proportionate.[105] The court did not find any of Bridges's contentions on the third factor to be convincing.[106]

Regarding the fourth factor of the *Bank Mellat* test, a fair balance between rights of individuals with community interests, the court ruled—even under a higher level of scrutiny—that the use of AFR Locate was not disproportionate to their aim.[107] The decision was based on the following reasons:

> AFR Locate was deployed in an open and transparent way, with significant public engagement. On each occasion, it was used for a limited time, and covered a limited footprint. It was deployed for the specific and limited purpose of seeking to identify particular individuals (not including the Claimant) who may have been in the area and whose presence was of justifiable interest to the police. On the former occasion it led to two arrests. On the latter occasion it identified a person who had made a bomb threat at the very same event the previous year and who had been subject to a (suspended) custodial sentence. On neither occasion did it lead to a disproportionate interference with anybody's Article 8 rights. Nobody was wrongly arrested. Nobody complained as to their treatment (save for the Claimant on a point of principle). Any interference with the Claimant's Article 8 rights would have been very limited. The interference would be limited to the near instantaneous algorithmic processing and discarding of the Claimant's biometric data. No personal information relating to the Claimant would have been available to any police officer, or to any human agent. No data would be retained. There was no attempt to identify the Claimant. He was not spoken to by any police officer.[108]

Thus, all four factors of the *Bank Mellat* test were met, meaning that infringing on Article 8(1) rights is permissible.

---

[104] *Id.* at *23.

[105] R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *23–24 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

[106] *Id.* at *23–24.

[107] *Id.* at *32.

[108] *Id.*

Bridges appealed his case to the Court of Appeal and on August 11, 2020, the Court of Appeal of England and Wales overturned the dismissal of the case, finding that the use of AFR was unlawful and violated human rights.[109] Bridges appealed the dismissal from the High Court on the following five grounds:

> 1. The High Court had erred in its conclusion that South Wales Police's use of AFR and interference with Mr. Bridges' rights was in accordance with the law under Article 8(2) of the ECHR.
>
> 2. The High Court had incorrectly concluded that the use of AFR and interference with Mr. Bridges' rights was proportionate under Article 8(2) of the ECHR.
>
> 3. The High Court was wrong to consider the DPIA carried out in relation to the processing sufficient for the purposes of Section 64 of the DPA 2018.
>
> 4. The High Court should not have declined to reach a conclusion as to whether South Wales Police had an "appropriate policy document" in place regarding the use of AFR Locate that was within the meaning of Section 42 of the DPA 2018 for carrying out sensitive data processing.
>
> 5. The High Court was wrong to hold that South Wales Police had complied with the Public Sector Equality Duty ("PSED") under Section 149 of the Equality Act 2010, on the grounds that the Equality Impact Assessment carried out was 'obviously inadequate' and failed to recognize the risk of indirect discrimination on the basis of sex or race.[110]

Ultimately, the Court of Appeal granted the appeal on the basis of the contentions in 1, 3, and 5, but rejected the contentions in 2 and 4.[111] While the Court of Appeal ruled differently than the High Court, they did not admonish the lower court for its decision, but rather acknowledged its "admirably clear and comprehensive judgments," and that it would be "impossible in following brief summary

---

[109] *UK Court of Appeal Finds Automated Facial Recognition Technology Unlawful in Bridges v. South Wales Police*, HUNTON ANDREWS KURTH PRIV. & INFO. SEC. LAW BLOG (Aug. 12, 2020), https://www.huntonprivacyblog.com/2020/08/12/uk-court-of-appeal-finds-automated-facial-recognition-technology-unlawful-in-bridges-v-south-wales-police/.

[110] *Id.*

[111] *Id.*

to do justice to the judgment."[112] The reasoning of the Court of Appeal will now be briefly discussed.

On ground 1, the Court of Appeal did not "accept the submission on behalf of SWP that the present context is analogous to the taking of photographs or the use of CCTV cameras. The following features of the present case lead us to conclude that it falls somewhere in between the two poles on a spectrum . . . ."[113] The court noted that AFR was not analogous to previous technology use by the police for several reasons.[114] The reasons were that AFR is a novel technology, it involved the capturing of images of a large member of the public, most of which would be no interest to the police, this data constituted "sensitive" personal data within the DPA 2018, and that the data was processed in an automated manner.[115] Within the legal framework, the court found "fundamental deficiencies" in two areas for the use of AFR. The fundamental deficiencies were the "who question" and the "where question," finding that "[i]n relation to both of those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed."[116] Ultimately, the Court stated, "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."[117]

On ground 2, the issue of proportionality of the use of AFR to harm the police were trying to mitigate, the Court noted that it was technically unnecessary for them to consider the issue because once it was determined that "the interference with the Appellant's Article 8 rights was not in accordance with the law," that one does not need to proceed to the next stage where it is determined if the interference was proportionate.[118]

Grounds 3 and 4 of Bridges's appeal related to section 64 of the DPA 2018 so it will not be discussed due to its lack of relevancy to the European Convention on Human Rights. While Ground 5 dealt with the Public Sector Equality Duty, so there will be no discussion of this section for the same reason.

The Court granted the appeal on Grounds 1, 3, and 5, and found declaratory relief to be the correct remedy.[119] The declaration of the Court is as follows:

---

[112] R (on the application of Bridges) v. The Chief Constable of South Wales Police, [2020] EWCA Civ 1058 at *9, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

[113] *Id.* at *21.

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.* at *22.

[118] *Id.* at *28.

[119] *Id.* at *44.

> 1. The Respondent's use of Live Automated Facial Recognition technology on 21 December 2017 and 27 March 2018 and on an ongoing basis, which engaged Article 8(1) of the European Convention on Human Rights, was not in accordance with the law for the purposes of Article 8(2).
>
> 2. As a consequence of the declaration set out in paragraph 1 above, in respect of the Respondent's ongoing use of Live Automated Facial Recognition technology, its Data Protection Impact Assessment did not comply with section 64(3)(b) and (c) of the Data Protection Act of 2018.
>
> 3. The respondent did not comply with the Public Sector Equality Duty in section 149 of the Equality Act 2010 prior to or in the course of its use of Live Automated Facial Recognition technology on 21 December 2017 and 27 March 2018 and on an ongoing basis.[120]

If Bridges's case had been denied an appeal, his case had been dismissed, or is appealed and loses on the merits before the Supreme Court of the United Kingdom, then Bridges could appeal to the European Court of Human Rights.[121] After the final decision from the Welsh courts, Bridges must submit an application to the European Court of Human Rights within six months.[122] The application to must relate to one of the rights within the European Convention on Human Rights.[123] Therefore, Bridges could appeal his challenge on the grounds that the use of AFR Locate violated his Article 8 rights, but not on his claims under Welsh law.

Once the European Court of Human Rights receives an application, it determines the admissibility of the application. To be admissible, the application "must comply with certain requirements set out in the Convention."[124] If the court finds the application inadmissible, then the decision is final and cannot be overturned.[125] If the court finds the application admissible, then the court encourages the parties to reach a settlement.[126] However, if the parties refuse to settle,

---

[120] *Id.*

[121] *Questions & Answers*, EUROPEAN CT. HUM. RTS. at 6, https://www.echr.coe.int/Documents/Questions_Answers_ENG.pdf (last visited Nov. 3, 2019).

[122] *Id.*

[123] *Id.* at 7.

[124] *Id.* at 10.

[125] *Id.*

[126] *Id.*

then the court will hear the case and decide whether a violation of the European Convention on Human Rights transpired.[127]

The current backlog of cases in the court means it could take up to a year before the court hears a case.[128] Almost all European Court of Human Rights proceedings take place in writing, and parties are informed of the final decision in writing.[129] If the court finds a violation under the Convention, it awards "a sum of money in compensation for certain forms of damage."[130] The court cannot "overrule national decisions or annul national laws."[131] So, in the event that Bridges appeals his case and wins at the European Court of Human Rights, he would gain financial compensation; however, he would not receive any guarantee the Welsh government will stop using the technology.

The European Court of Human Rights has evaluated hundreds, if not thousands, of claims under Article 8 of the European Convention on Human Rights.[132] The court published a guide for Article 8 claims in 2016, citing more than 700 cases.[133] While the court has yet to consider a case on facial recognition technology of this sort, it has issued opinions involving personal images, video surveillance, and personal data privacy.[134] Several cases the Court has disposed of contain claims with similar elements to those in *Bridges*, which demonstrates how the court may frame and ultimately rule on this issue.

In several cases, the court held "that the recording of a video in the law enforcement context or the release of the applicants' photographs by police authorities to the media constituted an interference with their right to respect for private life."[135] However, the court has also found "the taking and retention of a photograph of a suspected terrorist without her consent was not disproportionate to the legitimate terrorist-prevention aims of a democratic society."[136] Bridges's claim of privacy violation seems to arise in a situation much more similar to the latter case, as Bridges's photo was not distributed to anyone nor was he identified based on that video surveillance as a criminal by the police department or the media.

---

127 *Id.*
128 *Id.*
129 *Id.* at 9.
130 *Id.* at 11.
131 *Id.*
132 *See Comprehensive New Guide to Article 8 Published by the European Court of Human Rights*, ELEC. IMMIGR. NETWORK (Nov. 13, 2017), https://www.ein.org.uk/news/comprehensive-new-guide-article-8-published-european-court-human-rights.
133 *Id.*
134 EUROPEAN COURT OF HUMAN RIGHTS, *Guide on Article 8 of the European Convention on Human Rights*, at 38–40, 44–50 (Apr. 30, 2020).
135 *Id.* at 40.
136 *Id.*

In another case, the court held that rights under Article 8 would be "unacceptably weakened" if modern scientific techniques used by the criminal justice system "were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests."[137] While that holding came out of *S. and Marper v. the United Kingdom*, which involved fingerprint and DNA data,[138] the court could easily apply such principles to *Bridges*, as his claim derives from utilizing new technology in the criminal justice system and involves personal data. Nevertheless, as discussed above, the High Court of Wales went into a rather thorough balancing analysis between citizens' Article 8 rights and the government's interests.[139] Thus, the High Court of Wales will likely carefully balance such interests, as the European Court of Human Rights calls for, given a similar situation.

Peck v. the United Kingdom is another useful case in framing Bridges' Article 8 claim.[140] In this case, video surveillance identifying a man attempting suicide in a public place was distributed to media for broadcast.[141] Despite the fact that the surveillance of this man was in a public place, the Court held that the government's actions here violated his privacy rights.[142] While this case has some similarities to *Bridges* in that both involved video surveillance of citizens in a public place, the major distinction between the two is the dissemination of that footage to the media in *Peck*. Thus, based on the major factual difference in dissemination, the Court may see the government's actions regarding Bridges as less of an invasion of privacy.

IV. CONCLUSION

As technological advances proliferate, the legal framework surrounding and governing the use of technology is also expanding. As personal information becomes increasingly accessible, a pertinent question emerges: Where will the legal community draw the line concerning privacy rights? Facial Recognition Technology is rapidly developing, as well as its application by government services on their citizens. Countries and cities around the world are starting to wrestle with the tension between public safety and personal privacy regarding law

---

137 *Id.* at 44.

138 S. & Marper v. United Kingdom, [2008] Eur. Ct. H.R. 1581.

139 R. (on the application of Bridges) v. Chief Constable of S. Wales Police [2019] EWHC (QB) 2341, 2019 WL 04179616 at *23 (Eng.), https://www.westlaw.com/Document/I4A7E5AE0CF3211E99573C5E0B6E03B9F/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0.

140 Peck v. United Kingdom, [2003] Eur. Ct. H.R. 44.

141 EUROPEAN COURT OF HUMAN RIGHTS, *supra* note 134, at 40.

142 *Id*.

enforcement agencies employing FRT as a tool to monitor citizens in public spaces.

Bridges highlights this delicate balancing act that courts and legislatures will face when considering this topic. Bridges believed his face had been scanned by Welsh police during peaceful protests and challenged the usage of FRT by claiming that it violated his privacy rights. The High Court of Wales and the Court of Appeal of England and Wales provided detailed analyses of all of Bridges' claims, including his Article 8 claim. Comparing the factual events in *Bridges* to other Article 8 claims the European Court of Human Rights has ruled on, it appears that as the Welsh program currently stands, the Court would probably not find a violation of Bridges' Article 8 rights. Based on the lack of public distribution, storage, and limited target lists, the Welsh AFR Locate program does not seem invasive enough to constitute a violation of Bridges' Article 8 rights. At this time, if Bridges were to exhaust all his remedies at the national level, it is unlikely that the European Court of Human Rights would hold the use of AFR Locate violated his Article 8 rights.

While FRT used in the manner the South Wales Police Department used it in AFR Locate does not appear to violate Article 8 of the European Convention on Human Rights, other governments' use of FRT very well may be more invasive and violate other international laws or norms. As governments continue to utilize facial recognition technology in various ways, it is highly likely that many new legal questions will present themselves.