Cambridge Law Review (2021) Vol VI, Issue ii, 86-118

Individuals Under Observation: The Law Responds to (Live) Facial Recognition Technology

Ana Rosenthal*

Abstract

'Facial recognition' is an artificial intelligence tool that has the potential to identify individuals in real-time. The technology forms part of the growing system of mass surveillance, itself a multibillion-dollar industry which promises to bolster public safety and security. Police forces in England and Wales began testing the technology in 2017. In the absence of a statutory framework, an individual named Edward Bridges challenged the legality of its use and issued judicial review proceedings against the South Wales Police (SWP) in 2019. The legal challenge was lost by Bridges in the first instance, but the Court of Appeal overturned the decision in August 2020, finding that the use of facial recognition by the SWP had been unlawful. Most importantly, the Appellate Court held that, as a novel technology, the lack of a clear legal framework infringed the right to privacy under Article 8 of the European Convention of Human Rights (ECtHR). The Court also noted that the SWP had failed to safeguard the rights and freedoms afforded to individuals by the Data Protection Act 2018, and found that in each deployment, the police had overlooked whether the technology had a gendered or racial bias. The implications of the judgment are significant, not least because it maps out how Parliament may want to legislate on such technologies in the future. This article explores the theoretical and legal implications behind facial recognition,

* LLM, Birkbeck, University of London. Thank you to Dr Bernard Keenan, my research supervisor, as well as the anonymous reviewers from the Cambridge Law Review. I am also grateful to Eva, Norman, Manuela, and Andrej for listening to my thoughts. Any errors are my own. anarosenthalm@gmail.com.

particularly at a time when individual and fundamental rights have been brought into even sharper focus as a result of the global pandemic.

Keywords: facial recognition technology, surveillance, individuals, data collection, privacy

I. Introduction

Edward Bridges lives in Cardiff, South Wales. He is a white British man, and a father of two. He works in an office job at Cardiff University.[1] Ed is the Claimant in *Bridges v South Wales Police*,[2] the world's first legal challenge in the courts concerning the use of Automatic Facial Recognition (AFR) technology. Ed claimed his face was caught by an AFR camera on two deployments by the South Wales Police (SWP); the first time, he had been shopping in Cardiff, and on the second, he was peacefully protesting against the Cardiff Arms Fair. Today, Ed, together with the human rights group Liberty, has successful campaigned and challenged the SWP in the Court of Appeal for the way AFR was being used.[3]

Robert Williams lives in Detroit, in the US state of Michigan. He is a black African American, and also a father of two.[4] He is an officer worker at an automotive supply company. Robert was the first known individual in the US to be wrongfully arrested because of an incorrect alert on a facial recognition system. He was accused of shoplifting in January 2020. He spent "30 hours in custody and was released on a $1,000 personal bond".[5] Today, Robert, alongside the American Civil Liberties Union and the University of Michigan Law School's Civil Rights

1 Steven Morris, 'Office worker launches UK's first police facial recognition legal action' (*The Guardian*, 21 May 2019) <https://www.theguardian.com/technology/2019/may/21/office-worker-launches-uks-first-police-facial-recognition-legal-action> accessed 28 July 2021. See also, Ed Bridges, 'End lawless and dangerous police use of facial recognition technology' (*Crowdjustice* blog, 11 June 2020) <https://www.crowdjustice.com/case/facial-recognition/> accessed 28 July 2021.

2 *R (Bridges) v Chief Constable of the South Wales Police* [2019] EWHC 2341 (Admin).

3 *The Queen (on the application of Edward Bridges) v The Chief Constable of South Wales Police & others* [2020] EWCA Civ 1058.

4 Kashmir Hill, 'Wrongfully Accused by an Algorithm' (*The New York Times*, 24 June 2020) <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html> accessed 28 July 2021.

5 ibid.

Litigation Initiative, has filed a lawsuit against the Detroit Police Department to obtain compensation and ban the technology for the way it operates in the US.[6]

It is useful to consider how facial recognition has impacted both Ed and Robert because their cases indicate the complexities affecting an individual, including issues of racial bias.[7] This article, however, concentrates on the topical case of Ed Bridges because its aim is to survey the attitude of the UK and its legal system. The legal issues surrounding facial recognition in the UK relate to fundamental rights and data protection laws, particularly in the absence of statutory regulation on the matter. This article considers what it means to be an "individual" as facial recognition systems begin to alter the parameters of mass surveillance in the public sphere, even though the topic has immense legal implications for all countries, those largely democratic and those dictatorial.

This article is primarily library-research based, and relies on internet research and news articles because of the limitations posed by the Covid-19 restrictions in 2020. It involves a doctrinal analysis of recent cases that reveal the justifications for the deployment of AFR. Doctrinal research contrasts primary sources, i.e. case law, with secondary academic papers to help frame how the law has begun to develop. This article pays particular attention to how the *Bridges* case evolved in the courts, using the Divisional Court's judgment to contrast what was later decided by the Court of Appeal – a judgment the SWP chose not to challenge any further.

The article is structured as follows: Section II aims to define AFR. The section explains what the courts have said about the deployment of AFR, and reflects on why this particular technology has become an issue of both public and legal importance. The idea is to start looking more deeply into the socio-legal context behind its use to be able to situate the role of the individual within the debate. Section III outlines useful frameworks that help analyse some of the effects of AFR. It focuses on ideas put forward by theorists such as Michel Foucault or Gilles Deleuze, and situates them amongst more recent ideas developed by writers such as Jackie Wang and Evgeny Morozov. It introduces the work of Claudio Celis Bueno, a researcher who also adopts Deleuze's work to explain why facial recognition is tied to an inherent contradiction, i.e., "the weakening the processes of individualisation on the one hand and the growing centrality of the face on the

6 Tate Ryan-Mosley, 'The new lawsuit that shows facial recognition is officially a civil rights issue', (*MIT Technology Review,* 14 April 2021). <https://www.technologyreview.com/2021/04/14/1022676/robert-williams-facial-recognition-lawsuit-aclu-detroit-police/> accessed 28 July 2021.

7 For further research on race, as well as gender and class issues see: Joy Buolamwini, MIT Media Lab. See also, Steve Lohr, 'Facial Recognition is Accurate, if You're a White Guy' (*The New York Times*, 9 Feb 2018) <https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html> accessed 28 July 2021.

other".[8] Section IV looks more closely at why facial recognition might begin to "weaken" the idea of the individual. We explain this in the context of the growth of mass surveillance. In particular, this section delves deeper into the *Bridges* case and evaluates how human rights law and data protection regulation create highly procedural norms on new surveillance technologies. Section V reflects on why the "face" remains pertinent to the debates on facial recognition. The tool accentuates structural issues in society as it can categorise individuals into different profiles. In particular, we focus on the 'watchlist' – an apparatus that has given facial recognition its unique characteristics and power to individuate. Finally, Section V concludes.

II. Facial Recognition Technology: What Is It and What Have the Courts Said About It?

Automated (or live) facial recognition (hereinafter referred to as 'AFR')[9] can be described as an artificial intelligence tool which measures facial features to develop a unique facial code for an individual. The algorithm then uses those measures and matches them to other facial images that will be stored on a database or 'watchlist'. The result generated by the algorithm is based on a percentage of matching features i.e. a threshold of similarity, rather than a straightforward 'yes' or 'no' test.[10]

AFR is a tool that varies in use: it can open your phone, tag photos on social media or if in operation, may detect that you are at either an airport or busy location. For example, between May 2016 and March 2018, AFR was used by private developers in quasi-public spaces, namely Kings Cross, London.[11] In the future, experts indicate that AFR will have the potential to start analysing our emotions.[12] However, what is certain today is that the tool has become increasingly

[8] Claudio Celis Bueno, 'The Face Revisited: Using Deleuze and Guattari to Explore the Politics of Algorithmic Face Recognition' (2020) 31 Theory, Culture & Society 73-91.

[9] AFR is the technical name used by the SWP in the *Bridges* case.

[10] Silkie Carlo et al., 'Faceoff: The Lawless Growth of Facial Recognition in UK policing' (*Big Brother Watch*, May 2018) <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf> accessed 28 July 2021.

[11] Dan Sabbagh, 'Facial Recognition Technology Scrapped at King's Cross Site' (*The Guardian*, 2 September 2019) <https://www.theguardian.com/technology/2019/sep/02/facial-recognition-technology-scrapped-at-kings-cross-development> accessed 28 July 2021. See also, Zoe Kleinman, 'King's Cross developer defends use of facial recognition' (*BBC*, 12 August 2019) <https://www.bbc.co.uk/news/technology-49320520> accessed 28 July 2021.

[12] Hannah Devlin, 'AI systems claiming to 'read' emotions pose discriminatory risks' (*The Guardian*, 16 February 2020) <https://www.theguardian.com/technology/2020/feb/16/ai-systems-claiming-to-read-emotions-pose-discrimination-risks> accessed 28 July 2021; Madhumita Murgia, 'Emotion recognition: Can AI detect human feelings from a face?' (*FT*, 12 May 2021) <https://www.ft.com/content/c0b03d1d-f72f-48a8-b342-b4a926109452> accessed 28 July 2021.

pervasive in modern society, largely as public bodies have tested AFR for the purposes of security control and crime detection.

Since 2017, various police departments across the UK have had the capacity to deploy automatic facial recognition, and it can be used in two ways. First, a tool referred to as "AFR Identify" allows law enforcement agencies to upload pictures of an unidentified suspect or by using a "probe image" that may relate to a previous crime incident. This is then matched against images held by a police custody database system containing approximately 500,000 pictures.[13]

Second, the technology has capabilities to be used in real-time using a method known as "AFR Locate".[14] Cameras are mounted onto police vehicles to survey an area, and as people pass within the designated catchment area, every face is filtered through the AFR system. This system includes a 'watchlist': a list of wanted people that has been compiled by the operator in advance of its deployment. If a match alert is triggered, then the system operator, for example, a police officer, would need to decide in real time how to respond based upon whether they consider the alert to be a true positive or not. If no match is made, which will occur in the vast majority of cases, then the AFR Locate system deletes the facial biometrics or images that have been filtered through the live system.[15]

The capabilities of the first model – AFR Identify – incited controversy in early 2020 when *The New York Times* published its investigation into a relatively unknown start-up called Clearview AI, a company that had been "mining" public images on Facebook, YouTube and other well-known portals.[16] It was revealed that Clearview AI's facial recognition tool was holding over three billion images in its database, and the tool was being sold to law enforcement agencies and various private businesses for security purposes.[17] The Clearview-AI model, with its immense database collection and retention system, is not in operation in the UK.[18]

[13] *Bridges* (n 2) 27.

[14] ibid 28.

[15] ibid 37.

[16] Kashmir Hill, 'The Secretive Company That Might End Privacy as We Know It' (*The New York Times*, 18 January 2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> accessed 28 July 2021.

[17] ibid. See also, Kashmir Hill, 'Facial Recognition State-Up Mounts a First Amendment Defence' (*The New York Times*, 11 August 2020) <https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html> accessed 28 July 2021; CCN Business, 'Clearview AI's Founder Hoan Ton-That speaks out [Extended interview], (*YouTube*, 6 March 2020) <https://www.youtube.com/watch?v=q-1bR3P9RAw> accessed 28 July 2021.

[18] 'Clearview AI' (*Clearview AI*, 12 May 2021) <https://clearview.ai/law-enforcement> accessed 28 July 2021.

In fact, the legal issues in *Bridges* focus specifically on the second 'live' model: AFR Locate.[19]

To test AFR, the Home Office first awarded a contract to the South Wales Police (SWP) – which then deployed it at the Champions League final, which took place in Cardiff in June 2017. Thereafter, additional trials were set up by other police departments, including by London's Metropolitan Police in early 2020.[20] As stated above, in 2019, Ed Bridges – represented by the civil liberties group Liberty – brought the first legal challenge concerning the use of AFR against the SWP.[21]

At first instance, the Divisional Court held that whilst AFR interferes with privacy rights, the current legal regime does provide adequate safeguards that guarantee the "appropriate and nonarbitrary use" of the technology, adhering both to the Human Rights Act 1998 and the data protection legislation.[22] In rejecting the Claimant's arguments for Judicial Review, the Court of Appeal decided to review the legal matter – with the three day trial taking place over Skype in June 2020 because of the pandemic.

For a case adjudicating on new technologies, the online trial was replete with technical difficulties – from muffles to echoing sounds, to sudden interruptions and some delay.[23] In fact, as a participant observer, I recall how the trial was initially scheduled to be broadcasted on YouTube, but the sounds coming from the three judges in the courtroom meant it was impossible to hear the Appellant's QC, who also appeared from his echoey office. Shortly after starting, Sir Terence Etherton, the Master of the Rolls, had to temporarily suspended the sitting as he ordered the search for technical aides. The rest of the Court awaited instruction, at which point Dame Victoria Sharp, the President of the Queen's Bench Division, and Lord Justice Singh, both sitting as justices, could be heard in light conversation. I noticed Singh cautioned silence, noting "we might potentially be live on YouTube", whilst gently nodded towards the cameras.[24] It provoked a sense of irony that the judge

[19] *Bridges* (n 2) 27-28; *Bridges* (n 3) 11.

[20] Damien Gayle, 'Met Police Deploy Live Facial Recognition Technology' (*The Guardian*, 11 February 2020) <https://www.theguardian.com/uk-news/2020/feb/11/met-police-deploy-live-facial-recognition-technology> accessed 28 July 2021.

[21] *Bridges* (n 2).

[22] ibid 1, 159.

[23] Owen Bowcott, 'UK's facial recognition "breaches privacy rights"' (*The Guardian*, 3 June 2020) <https://www.theguardian.com/technology/2020/jun/23/uks-facial-recognition-technology-breaches-privacy-rights> accessed 28 July 2021.

[24] Court of Appeal Trial, R (*Bridges) v CC South Wales & ors* (C1/2019/2679) N.p. 2020. Web. 23-25 June 2020.

himself felt very aware that he was being watched – a slight indication as to what would follow.

On 11 August, 2020, the CA released its judgment. The CA held that the SWP's use of AFR was not "in accordance with the law" – specifically, as the legal framework did not support what it called 'the "who" and the "where" question', i.e. in what circumstances can AFR be used.[25] In other words, the technology had the capability to violate our Article 8 rights to privacy because there were insufficient safeguards used to determine who might be on the 'watchlist'.[26] In addition, the SWP had failed to take reasonable steps to make enquires about whether AFR has racial or gender bias.[27] Liberty took to twitter, posting: "it's almost lunchtime, the sun is shining, and discriminatory police #FacialRecognition tech is unlawful".[28]

III. Situating Facial Recongition: A Conceptual Framework

On 24 January, 2020, some weeks prior to the first Covid-19 lockdown, the Metropolitan Police announced that it would start using live facial recognition operationally for the first time on the streets of London. Twitter reacted. Silkie Carlo, Director of the civil liberties group, Big Brother Watch, reshared the Metropolitan's post with the caption: "see you in court".[29]

Perhaps what was most surprising, certainly from a legal perspective, was that the Metropolitan Police had overlooked the fact that the first facial recognition case, *Bridges*,[30] was already making its way through the courts. The Court of Appeal had only recently granted its permission for appeal on the basis that *Bridges* has a "real prospect of success".[31] It seemed as though the Metropolitan Police was using the Divisional Court's judgment as authority for a full-scale operational deployment that moved beyond the trial phase.

A. Theories to surveil

To analyse the effects of the rapid deployment of AFR by the state, a useful starting point is the conceptual triad developed by Gilles Deleuze in his

[25] *Bridges* (n 3) 91.

[26] ibid.

[27] Ibid 182-199.

[28] Liberty (*Twitter*, 11 August 2020). <https://twitter.com/libertyhq/status/1293145042253742081> 11 August 2020.

[29] Silkie Carlo, (*Twitter*, 24 January 2020). <https://twitter.com/BigBrotherWatch/status/1220686136806445057> accessed 28 July 2021.

[30] *Bridges* (n 3)

[31] Monidipa Fouzder, 'Court of Appeal to hear facial recognition technology challenge' (*The Law Society Gazette*, 20 November 2019) <https://www.lawgazette.co.uk/news/court-of-appeal-to-hear-facial-recognition-technology-challenge/5102241.article> accessed 28 July 2021.

short essay 'Postscript on the Societies of Control'.[32] Deleuze recounts the way in which new societies of 'control' have evolved from what Michel Foucault had previously identified as 'discipline' societies. Foucault, as Deleuze contends, had recognised that spaces of enclosure, for example, the factory, the prison, the hospital, had disciplined societies away from what Foucault termed societies of 'sovereignty', which functioned to "tax rather than organise production, to rule on death rather than to administer life". Accordingly, discipline power produces a form of subservience, intended to form an interiorised type of behaviour. But now, Deleuze argues, it is the *disciplinary* systems themselves that have fallen into crisis – to be replaced by societies of control. Writing in 1990, Deleuze did not live to witness the exponential growth of CCTV, let alone the current trialling of facial recognition by the state, but he did envisage a shift taking place within the network of surveillance.

According to Deleuze, societies of control move away from the structure of enclosure and allow for an illusion of freedom. The apparatus of power can exert control over us precisely by provoking a sense of variation and continuous change. The contemporary writer Jackie Wang, who has examined the racial, economic and legal influence of the US carceral state, writes that: "it is possible that as technologies of control are perfected, carcerality will bleed into society".[33] She implies that the physical structures of prisons might be superseded by new surveillance methods because those methods can be portrayed as both economically viable as well as a benefit to individual freedom. Wang argues that this development may bring about the "birth of a more all-encompassing police state".[34] To her mind, spaces that are policed develop into carceral spaces.

In *Discipline and Punish*, Foucault famously developed a theory of modern urban *panopticism* to describe a process of observation that is utilised to guarantee order. Foucault details how: "the panoptic mechanism arranges spatial unities that make it possible to see constantly and recognise immediately".[35] He notes that the key effect of the Panopticon is: "to induce […] a state of conscious and permanent visibility that assures the automatic functioning of power".[36] However, the subtlety to Foucault's argument reveals that the Panopticon is essentially a tool of power

[32] Gilles Deleuze, 'Postscript on the Societies of Control' (1992) 59 MIT Press 3-7. <https://cidadeinseguranca.files.wordpress.com/2012/02/deleuze_control.pdf> accessed 28 July 2021.

[33] Jackie Wang, *Carceral Capitalism* (Semiotext(e) Intervention Series 2018) 39.

[34] ibid 40.

[35] Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Penguin 1991) 200.

[36] ibid 201.

used to supervise individual conduct to increase profitability and the productivity of an activity.

The notion of productivity, therefore, is useful for thinking about the way norms on new surveillance have been framed. In fact, an example of this appeared during the *Bridges* trial at the Court of Appeal in an argument made by the SWP – the defendants. In their submissions, the SWP openly declared that AFR should be understood as a tool for policing "lower-level suspected persons".[37] This point was made on the basis that current forms of policing remain too resource intensive and require a large workforce to trace those who fail to engage with the criminal process, for example, people on warrants. To that end, Jason Beer QC, appearing for the SWP, submitted that AFR serves as "a tool that narrows the pool of individuals".[38]

In his lectures on *The Birth of Biopolitics*, Foucault traces the origins of productivity in what he denotes to be the liberal art of government, which originated during the eighteenth century. Foucault argues that liberalism is not aimed at securing freedom, but it is instead closely related to the freedoms provided for by the market. He writes: "the formula of liberalism is not: 'be free'. Liberalism simply formulates the following: I am going to produce what you need to be free".[39] In other words, it emphasises a technique of governance that is less focused on the imperatives of individual freedoms and more on "the management […] of the conditions in which one can be free".[40] Foucault continues: "freedom is something which is constantly produced", but notes that the cost to manufacturing this freedom is "security".[41]

Liberalism, therefore, develops as a mechanism that continually needs to: "arbitrate between the freedom and security of individuals by reference to [a] notion of danger".[42] Indeed, the "problem of security" requires finding the balance between the collective and individual interest. This framework certainly applies to the way in which the courts produce and apply legal norms to surveillance technologies. This is because the courts will limit themselves on interfering on issues of national security. Thus, the law will engage itself in a process that is less about "ruling" and more about finding a balance between liberty and the protection of rights on the one hand, and the power of state to surveil on the other.

Interestingly, the philosopher Frédéric Gros developed a theory on security in his book *The Security Principle*. Gros formulates four definitions for security, but

[37] Court of Appeal Trial, *R (Bridges) v CC South Wales & ors* (C1/2019/2679). N.p. 2020. (23-25 June 2020).

[38] ibid.

[39] Michel Foucault, *The Birth of Biopolitics: Lectures at the Collège de France 1978-79* (Palgrave Macmillan 2008) 63.

[40] ibid 63-64.

[41] ibid.

[42] ibid.

relevant here is the notion of 'biosecurity' – which is defined as a measure that is necessary to "protect, control and regulate the individual".[43] Importantly, he suggests 'control' is one of the practices of biosecurity as it seeks to trace human beings through unique biological traits.[44] In other words, Gros suggests that "control" is not about observing nor correcting individual behaviour through a centralised gaze or institution, but rather a means to track movements and actions through the numerous traces that individuals leave behind.

For Gros, facial recognition would be another identifier that "helps things run more fluidly".[45] Gros indicates how tracking devices now allow security forces to identify and locate individuals, serving as "irrefutable evidence".[46] Gros adds that the other major function of the new techniques of control is the "compiling of digital data".[47] In his words: "our acts today have acquired an almost indestructible memory".[48] In this context, Gros comes close to describing what the watchlist might be: "the traces can be brought up again for anyone at any moment – and the justice system can itself lay hold of them".[49]

In a manner akin to Hannah Arendt's concept of "objective enemies" that occur under totalitarian regimes, Gros says that the countless files that exist mean we are all now "objective subjects". However, Gros dismisses the idea that new technologies of control are lifting the "spectre" of totalitarianism.[50] This is because modern forms of control fall short of spying on people to verify their ideological conformity. In fact, technology lacks an ideological undertone in the sense that informed consumers seem willing to share their biometric identity so that they can access a "mode of sociability".[51]

Importantly, as Gros suggests, totalitarianism would follow a principle of nonreciprocity between those that controlled the surveillance apparatus versus those that were *subjected* to it.[52] In fact, totalitarian forms of surveillance were rooted in highly centralised and hierarchical forms of power. Today, the difference is that

[43] Frédéric Gros, *The Security Principle* (Verso 2019) chapter 4.
[44] ibid 152.
[45] ibid 157.
[46] ibid 153.
[47] ibid 154.
[48] ibid.
[49] ibid.
[50] ibid. 159.
[51] ibid.
[52] ibid.

modern technologies of control also exist in more democratic and participatory systems, though this is perhaps an increasingly "privatised" hybrid model.

B. Eternal technological amelioration?

Evgeny Morozov has contributed to the argument by outlining how the ideological imperative of new technologies are in fact rooted in their quest to problem solve. Morozov states that the fall back to the promise of "eternal amelioration" brought about by technology inevitably carries less scrutiny in regard to its ethics.[53] Morozov does not oppose technology itself, but he seeks to alert the reader to the idea that not every problem will demand a technological fix. In fact, any belief in technological perfection that fails to address the intricacies of the human existence, he argues, is likely to create new problems.[54]

Race, for example, has become a central problem in the debate surrounding the rapid deployment of AFR by the state. Evidence gathered in an independent report for the Metropolitan Police Trial of AFR, by Professor Peter Fussey and Dr. Daragh Murray, suggests that indirect discrimination appears in two ways. First, the technology may react differently depending on an individual's sex, race, or colour, which is an issue linked to technical performance as the technology carries an inbuilt bias. The second, and perhaps more long-standing issue, relates to the way in which the technology is used because it often correlates with potentially discriminatory policing processes.[55] The legal scholar Andrew Guthrie Ferguson offers a detailed account as to why machines get racial or gender bias wrong.[56] Specifically, algorithms replicate biases as machine-learning tools learn by correlating past data sets. Ferguson explains:

> "[…] even if race were completely stripped out of the model, the correlation with communities of colour might still remain because of the location. A proxy for racial bias can be baked into the

[53] Evgeny Morozov, *To Save Everything Click Here: Technology, solutionism, and the urge to fix problems that don't exist* (Penguin, 2014) xiii.

[54] ibid 1-16.

[55] Murray P. Fussey and Daragh Murray, *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology* (The Human Rights, Big Data and Technology Project 2019) 40. <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf> accessed 28 July 2021.

[56] Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York University Press 2020).

system, even without any formal focus on race as a variable".[57]

Therefore, a key limitation that is likely to occur is the potential for the algorithm to misidentify an individual as a result of racial or gender biases being built into the model. Jackie Wang elegantly summarises the issue: "A wrong 'You may also like […]' product recommendation on Amazon is one thing, but a wrong prediction in the arenas of punishment, policing, and finance is quite another".[58]

The rapid development of data science is creating methodologies for policing that focus on anticipating and predicting crime.[59] Anticipatory methods that aim to prevent crime have always been used, but new data tools may increasingly allow police officers to make decisions based on an algorithm. Interestingly, Evgeny Morozov has labelled predictive policing as the "epitome of solutionism" as it appears to be an easy and logical step, but it does not adequately consider the complex "environmental vulnerabilities" that encourage crime to begin with.[60] In addition, any underreporting in crime can also lead to huge discrepancies that limit the capabilities of algorithmic policing.[61] The fear is that labelling subjects as potential risks could actually end up producing individuals as such.[62] Ferguson reminds us that data is not blind. In fact, he says: "data is us, just reduced to binary code".[63]

Here, we ought to recall Deleuze's argument on how new modes of power brought about by digital technologies no longer sustains the individual as the product – which arose more clearly under Foucault's disciplinary mode of power. To Deleuze, in the society of control, individuals have become "*dividuals*".[64] The implication is that the individual can be fragmented into endless data points or codes. Deleuze notes that: "The numerical language of control is made of codes that mark access to information, or reject it".[65] In short, it is the way that data can be collected, and then used as a method of control, that delineates us as "dividuals".[66] However, Deleuze's digital theory of control perhaps sits at odds with the pervasive

57 ibid 122.
58 Wang (n 33) 49.
59 ibid 42.
60 Morozov (n 53) 182-185.
61 ibid.
62 Wang (n 33) 43.
63 Ferguson (n 56) 123.
64 Deleuze (n 32) 5.
65 ibid.
66 Celis Bueno (n 8) 79.

Western ideologies of individuality – and this includes the legal logic employed in human rights law, that seeks to protect the individual's rights and freedoms.[67]

Rouvroy and Berns use the term "algorithmic governmentality" to uncover the rationality behind the automated collection and analysis of big data, and its effects on populations.[68] However, central to their argument is that such processes are not focused on individuals, nor subjects, but "on relations".[69] The result is a "reduction of opportunities to challenge forms of 'knowledge' production based on datamining and profiling".[70] Most interestingly, they contend that: "[…] 'power' grasps the subjects of algorithmic governmentality no longer through their physical body, nor though their moral conscience […] but through multiple 'profiles' assigned to them, often automatically, based on digital traces of their existence and their everyday journeys".[71]

It appears that Rouvroy and Berns' analysis anticipates the power of the 'watchlist' in facial recognition technology:

> "The fact of [algorithmic] power having a digital rather than a physical 'grasp' in no way means than individuals are […] reducible to networks of data. Instead, the function of algorithmic power is to draw out: […] 'profiles' (as a potential fraudster, a consumer, a potential terrorist, a student with high potential, etc.)".[72]

AFR does, therefore, seem to create a problematic position for the individual in light of its algorithmic capabilities. In a more recent article, which has also adopted Deleuze's theoretical framework of control, academic Claudio Bueno Celis argues that facial recognition technologies encounter an inherent contradiction: "a weakening of the processes of individualisation on the one hand, and an ever-growing centrality of the face as a mechanism of individualisation on the other".[73]

Importantly, Celis contends that the technology does not simply function as a ubiquitous panopticon, but ought to be understood as an "apparatus of metadata that goes beyond the task of individualisation".[74] And yet, the tool also retains an element that will utilise the individual's "face" as a disciplinary diagram of

67 Paul Bernal, 'Data gathering, surveillance and human rights: Recasting the debate' (2016) 1(2) Journal of Cyber Policy 243-264, 243.

68 Antoinette Rouvroy and Thomas Berns, 'Algorithmic governmentality and the prospects of emancipation' (2013) Réseaux 163-169.

69 ibid v.

70 ibid x.

71 ibid xi-xii.

72 ibid xii.

73 Celis Bueno (n 8) 81.

74 ibid 80.

control.[75] The remainder of this article will explore this contradictory duality through a legal context. In using Celis' argument as a generalised framework, it aims to address what the law is doing for the individual within the context of ever-growing AFR systems.

IV. Mass Surveillance: The 'Weakening of the Individual'

The 'weakening of the processes of individualisation' might be best understood within the context of mass surveillance capabilities. In fact, Celis suggests that AFR can be viewed from the perspective of what he recognises as "machinic enslavement" – the idea that AFR algorithms "do not operate as apparatuses of individualisation but rather as an apparatus of metadata", i.e. "information about information" to create control.[76]

Importantly, the legal and political debate on surveillance intensified in the wake of the Edward Snowden revelations in 2013. Previously, ideas about surveillance levels in the UK were largely a matter for speculation – as intelligence and security agencies can adopt a "neither confirm nor deny" policy.[77] Today, we can differentiate new forms of surveillance from more "traditional" methods like phone-tapping or photography.[78] Present-day techniques capture both "content" data and also what is referred to as "metadata". The former targets communications of known individuals, whilst the latter can involve "bulk" interception of large amounts of data with no specific target in mind.[79] The important point, however, is that "metadata", which is perhaps best described as the "residual-like" part of collected data, is often more revealing as it can be processed and analysed very quickly.

In particular, facial recognition uses machine-learning algorithms to harvest biometric data, which can be collected in bulk from large numbers of people. In essence, these algorithms do not use a pre-given template to match a facial image to a specific person. Instead, they are based on statistical calculations that uncover patterns in the "training datasets".[80] Broadly speaking, the process involves "feeding" millions of images to the algorithm in order to "train" it to identify faces. During the process, however, the face "fragments […] into bits of information that no longer belong to a private individual, but rather constitute a data bank of face templates and training sets".[81] It follows, therefore, that identity

[75] ibid 81.
[76] Celis Bueno (n 8) 84, 80.
[77] Bernal (n 67) 246. Also see, *Bridges* (n 3) 95.
[78] ibid 246.
[79] Bernal (n 67) 248.
[80] Celis Bueno (n 8) 80.
[81] ibid 84.

is reduced to a number of quantitative measures[82] – what Deleuze would define as the "*dividuals*".[83] Accordingly, the next section discusses how the law has responded to the way AFR has increased the 'potential' for mass surveillance by the state, and why it has often developed a problematic position for the individual. We review this in the context *Bridges*[84] – contrasting certain elements from the Divisional Court position with the final judgment by the Court of Appeal.

Importantly, *Bridges* was initiated on the premise that AFR would have profound consequences for privacy (Article 8 of the European Convention on Human Rights – ECHR) and data protection rights.[85] In this section, we will first look at the grounds challenging the breach of Article 8(1) and (2) of the ECHR, which primarily considered if the use of AFR was "in accordance with the law" – per Article 8(2). Second, we briefly review how the courts addressed the data protection claim in *Bridges*, once again showing that judges will engage in a proforma checklist exercise, rather than assessing broader questions in regard to the need to collect large amounts of information belonging to the individual. We argue that the Court of Appeal recognised that AFR is a technology that might "weaken" what it means to be an individual given the potential baleful surveillance capabilities. At the same time, we show how the courts tend to avoid making assessments in regard to the wider "necessity" for bulk surveillance capabilities, favouring instead a procedural approach that relies on formal safeguards, as well as controls set by UK regulatory bodies. In many ways, adopting a procedural approach means the legal discussion has moved beyond a reiteration of Ed Bridges as the individual subject, essentially focusing on the effects of the overall system.

We should note that *Bridges* disputed one final key point in regard to the public sector equality act, though it is not discussed here as the focus of this section is on the laws approach to mass data.

A. Privacy: *Bridges v South Wales Police*

To reiterate, in *Bridges*, the Divisional Court had considered that whilst AFR interferes with the privacy of every individual scanned, i.e. Article 8(1) ECHR, the legal frameworks assumed adequate safeguards for police forces to utilise AFR.[86] The Court of Appeal, however, overturned this decision in part. Most importantly, in a unanimous decision, the judges held that the Divisional Court

[82] ibid 81; see also: Bernal (n 67) 248.

[83] Deleuze (n 32) 5.

[84] *Bridges* (n 2); Bridges (n 3).

[85] Dan Squires QC, Aidan Wills and Megan Goulding 'Skeleton Argument on Behalf of the Claimant for the Substantive hearing on 21-23 May 2019' *R (Bridges v The Chief Constable of South Wales Police*) CO/4085 2.

[86] *Bridges* (n 2) 159.

had erred in finding that South Wales Police's (SWP) interference with Mr Bridge's privacy right was "in accordance with the law" – per Article 8(2). In particular, although the SWP relied on a legal framework comprised of primary legislation, secondary legislation in the form of codes of practice, and local policies, there was no specific guidance as "to 'where' AFR could be used and 'who' could be put on a watchlist".[87] As such, the Court of Appeal recognised the debilitating potential of AFR for an individual, like Mr Bridges, who had never appeared on a watchlist. However, and equally important, the Court of Appeal said that the Divisional Court had been right in its balance of the "proportionality" question. In their view, the benefits of AFR remain important, and the Court of Appeal specified that the impact on Ed Bridges, as an individual, had ultimately been minor in the circumstances.[88] Thus, the general 'use' of AFR could be proportionate under an Article 8(2) assessment if the technology operated under clear safeguards, which alludes to the idea that the individual remains secondary to the Court of Appeal in that the technology has a role in monitoring elements of society.

Importantly, the dispute over whether AFR ever "engaged" Article 8 was settled by the parties before the case got to the Court of Appeal. This is because the collection of biometric data contains personal information of an "intrinsically private" nature.[89] In other words Article 8 matters in circumstances where facial biometrics are retained even for a short time, including the near instantaneous processing of an individual's biometric data where no match occurs. Therefore, privacy rights are merely "triggered by the initial gathering of the information".[90] However, any lawful interference with Article 8 privacy rights will also need to abide by Article 8(2) of the ECHR:

> 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.

The legal question that often takes shape in regard to laws that grant powers of "bulk interception" to law enforcement agencies tend not to focus on whether concrete harm has been done to a specific person. Instead, the issue for the courts is whether the law abides by the principles of "legality, legitimacy, [incorporating]

87 *Bridges* (n 3) 91.
88 ibid 131-141.
89 ibid 57.
90 ibid 59.

checks and balances" as a means to safeguard against potential abuses by the state.[91] Broadly speaking, the Court of Appeal's judgment in *Bridges* supports this statement, to the extent that the Divisional Court was wrong to find that SWP's use of AFR was "in accordance with the law" as per 8(2) largely because: "AFR is a novel technology".[92]

Previously, the Divisional Court had found the legal framework to be satisfactory, in large part because the police is "a creature of the common law".[93] The Divisional Court had relied on both *R (Wood)*[94] and *R (Catt)*,[95] to state that the use and retention of photographs by police is justifiable to maintain "public order and identify crime".[96] Moreover, the lower court had suggested that AFR was less intrusive than other technologies, like DNA or fingerprints, which had reinforced the idea that police would not require new and express statutory powers. However, the Court of Appeal overturned this position – on the suggestion that AFR "involves the capturing of the images and processing of digital information of a large number of members of the public […] the vast majority of them will be of no interest whatsoever".[97] In fact, the technology gathers '"sensitive" personal data,' which is then "processed in an automated way".[98] If viewed from Celis' conceptual framework, the Court seems to express concern that AFR might "weaken" the processes of individualisation because the technology operates within a power vacuum, to the extent that "too much discretion is currently left to individual police officers".[99]

Nonetheless, in asking whether a lawful interference with Article 8(1) could be necessary, both courts referred to the four-stage test in *Bank Mellat*,[100] which enlists four broad principles for the objective justification of a limitation on a Convention right, i.e. when might it be necessary to restrict our individual human rights.[101] Before the Court of Appeal in *Bridges*,[102] the Appellants expressed concern over the "fourth" question in *Bank Mellat* within the context of AFR, namely "whether a fair balance has been struck between the rights of the individual and

91 Bart van der Sloot and Eleni Kosta, 'Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance' (2019) 5 Eur Data Prot L Rev 252, 256.
92 *Bridges* (n 3) 86.
93 *Bridges* (n 2) 69.
94 *R (Wood) v Commissioner of Police of the Metropolis* [2010] 1 WLR.
95 *R (Catt) v Association of Chief Police Officers* [2015] AC 1065.
96 ibid 7. See also, *Bridges* (n 2) 70-71.
97 *Bridges* (n 3) 87.
98 ibid 88-89.
99 ibid 91.
100 *Bank Mellat v Her Majesty's Treasury* (No 2) [2014] AC 700.
101 ibid; see also, *Bridges* (n 2) 98; *Bridges* (n 3) 132.
102 *Bridges*, CA (n 3) 132.

the interests of the community".[103] On this substantive question, the Divisional Court had previously concluded that the deployment of AFR by SWP "struck a fair balance and was not disproportionate".[104] Various reasons had been given, including that SWP deployed it in an "open and transparent way, with significant public engagement". Furthermore, the Divisional Court had stated that the trials had only ever sought individuals on a "watchlist", and no data had been kept.[105] In fact, the lower court noted that AFR could be used to save resources for the police.[106]

By contrast, the Appellants argued that the Divisional Court had erred in finding that SWP's use of AFR was proportionate according to Article 8(2) because it AFR Locate affects individual rights as well as the rights of every member of the public. Interestingly, the Court of Appeal considered that because the interference with the Appellant's Article 8 rights had never been "in accordance with the law", it should not be expected to adjudicate on this matter, yet the Court felt it was important to briefly address the issue to some degree.[107] The judges suggested that the impact on Mr Bridges – as an individual – had been minor in relation to the potential benefits of this technology, saying that "an impact that has very little weight cannot become weightier simply because other people were also affected. It is not a question of simple multiplication".[108] This assessment by the Court of Appeal implies that AFR might be deemed "proportionate" and "necessary" under Article 8(2) assessment in the future, which could ultimately overshadow many individual concerns.

B. Privacy: procedural v necessity

The European Court of Human Rights (ECtHR) itself has typically avoided questions of 'necessity' in regard to surveillance measures.[109] Instead, the ECtHR favours a more pragmatic/procedural approach and preserves the right for governments to have a "margin of appreciation" in regard to their own security issues.[110] However, the ECtHR has upheld that surveillance is "necessary in a democratic society" if it responds to a "pressing social need", and if the

[103] ibid.
[104] *Bridges* (n 2) 101.
[105] ibid.
[106] ibid 106.
[107] *Bridges* (n 3) 131.
[108] ibid 143.
[109] Maria Helen Murphey, 'A Shift in the Approach of the European Court of Human Rights in Surveillance Cases: a rejuvenation of necessity?' (2014) 5 *European Human Rights Law Review* 507-518. 510. See also, Kirsty Hughes. 'Mass surveillance and the European Court of Human Rights', (2018) E.H.R.L.R. 6, 589-599
[110] Murphey (n 109) 515.

interference is proportionate to the aim pursued and can be readily justified by national authorities.[111]

Accordingly, the ECtHR has also focused on whether the interference with Article 8 rights was "in accordance with the law", which should be noted means an adherence to the "quality" of the law doctrine – i.e. is the law foreseeable, accessible and overall compatible with the rule of law.[112] We know that this was the key dispute in *Bridges*.[113] However, the specificity of this approach shows that the courts will concentrate on evaluating the adequacy of existing procedural safeguards rather than determining with greater detail the 'necessity' of surveillance "in a democratic society".

The question of 'necessity' is important because data gathering – of any kind – continues to have the potential to invade the privacy of a population.[114] In an article on human rights and bulk surveillance, the academics Murray and Fussey propose that a more "nuanced" approach to privacy is required.[115] In particular, the threshold for use of bulk capabilities should only be satisfied by issues that constitute a "active" threat or impairment to the workings of a "democratic society". This means the law needs to change to be able to fully position the difference "between those situations in which bulk powers are useful and those situations in which they are vital".[116] To that end, we submit that "necessity" allows us to situate the individual in the context of mass surveillance more clearly.

Nonetheless, questions of "necessity" have often been superseded by the courts precisely because in a "democratic society" there is expectation that institutions abide by principles of accountability and oversight.[117] Moreover, abiding by a rigorous application of proportionality might interfere with the boundaries marked by the separation of powers as surveillance policy is usually thought to be better suited to executive expertise.[118] In that way, Maria Murphey shows us that the perceived benefit to the procedural approach is that: "it avoids

[111] *Catt v United Kingdom*, ECtHR, (Application nos. 43514/14), 24 Jan 2019, para 109. See also Kyriakos Kotsoglou and Marion Oswald, Marion, 'The Long Arm of the Algorithm? Automated Facial Recognition as evidence and trigger for police intervention' (2020) 2 Forensic Science International: Synergy 86-89, 87.

[112] Murphey (n 109), 508. See also, Keenan (n 109) 4.

[113] *Bridges* (n 3).

[114] Bernal (n 67) 259-260.

[115] Daragh Murray and Pete Fussey, 'Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data' (2019) 52(1) Israel Law Review 31-60.

[116] ibid 58.

[117] Bernal (n 67) 259-260.

[118] Murphey (n 109) 517.

direct competition between individual rights and the stated public interest in this complex and highly sensitive area" we call surveillance.[119]

This procedural logic in regard to Article 8 appeared most acutely in the case of *Big Brother Watch v UK*,[120] a prolonged legal dispute in response to the Edward Snowden revelations in 2013, now settled by the Grand Chamber of the ECtHR. It is useful to highlight some of its key consequences to outline why favouring a procedural approach on issues of mass surveillance capabilities carries certain limitations. In generalised terms, the procedural method to justice prioritises an oversight system that works to evaluate its own procedures, rather than delineating what forms an acceptable level of surveillance and what is "necessary in a democratic society" to truly protect individuals.[121]

In *Big Brother Watch*, various NGO's raised concerns over the UK's legal regime governing the sharing of foreign intercepted material collected by the US government, as well as the 'bulk' collection of metadata by UK intelligence services GCHQ under the codename TEMPORA.[122] Put very simply, the ECtHR reviewed key questions in regard to the compliance of the UK surveillance framework under the Regulation of Investigatory Powers Act 2000 (RIPA).[123] This act allowed for the interception of internal and external communications, after the Secretary of State had issued the relevant warrants.[124] On this matter – and relevant to our discussion – the Claimants argued that the UK's legal framework on the interception of bulk communications/metadata was not "in accordance with the law" and amounted to an interference with Article 8(2) – the right to privacy.

In its judgment, the Grand Chamber of the ECtHR stated that "Surveillance which is not targeted directly at individuals […] has the capacity to have a very wide reach indeed, both inside and outside the territory of the surveilling State".[125] Interestingly, the Court noted that "the degree of interreference with individuals Article 8 rights will increase as the bulk interception process progresses",[126] even where "the stored material is in coded form, intelligible only with the use of

[119] Murphey (n 109) 511.

[120] *Big Brother Watch and Others v United Kingdom ECtHR* (Application nos. 58170/13, 62322/14 and 24960/15) 25 May 2021.

[121] Keenan (n 109) 8, 17. See also, Murphey (n 109) 511.

[122] *Big Brother Watch* (n 120). See also, Van der Sloot and Kosta (n 91).

[123] RIPA has now repealed by the Investigatory Powers Act 2016 (IPA). See also, Keenan (n 109) 9; Tzanou, Maria, '*Big Brother Watch and others v. the United Kingdom*: A Victory of Human Rights over Modern Digital Surveillance?' (*Verfassungsblog*, 18 September 2018) <https://verfassungsblog.de/big-brother-watch-and-others-v-the-united-kingdom-a-victory-of-human-rights-over-modern-digital-surveillance/> accessed 28 July 2021.

[124] *Big Brother Watch* (n 120).

[125] ibid (n 120) 322.

[126] ibid (n 120) 330.

computer technology".[127] In deciding on the bulk interception of communications, the Grand Chamber said that national authorities withhold a "wide margin of appreciation" to address mounting national security concerns.[128] However, the Court acknowledged that since all interception regimes, whether bulk or targeted, are potentially open to abuse, the discretion "afforded [to Contracting States] must be narrower and a number of safeguards will have to be present".[129] To that end, the Court upheld that surveillance: "must be subject to end-to-end safeguards", i.e. a checklist of requirements for "supervision and independent *ex post facto* review".[130] In short, the Grand Chamber enlisted the *procedure* for how collected data ought to be used, stored, and then destroyed. In a similar manner, the Court of Appeal in *Bridges* considers that at the very least there needs procedural rigour on "who" is placed on a watchlist and "where" AFR can be deployed to be "in accordance with the law".[131]

Importantly, the Claimants in *Big Brother Watch*, had urged the Court to "update" the list of requirements, demanding for both prior "judicial authorisation" to be sought, and for "subsequent notification" be given to a target of surveillance.[132] The lower ECtHR court – the First Chamber – in its 2018 judgement, had rejected this view on the premises that "it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into private life of an individual than targeted interception".[133] The Grand Chamber agreed, noting that "judicial authorisation" might be a useful safeguard against arbitrariness, but 'not a "necessary requirement". The Grand Chamber went further and upheld that "bulk interception should be authorised by an independent body" – separate from the "executive".[134] Such authorising bodies should be "informed" of any bulk interception operations, overriding a system based on "notifying" a target of surveillance.[135] To give just one example, the ECtHR reviewed the supervisory role carried out by the IC Commissioner to examine any complaints concerning unlawful interception.

Notably, the Divisional Court in *Bridges* did the same on the question of "proportionality", for example, saying that the Information Commissioner and

[127] ibid.
[128] ibid 338.
[129] ibid 347.
[130] ibid 350.
[131] *Bridges* (n 3) 91.
[132] *Big Brother Watch and Others v United Kingdom ECtHR* (Application nos. 58170/13, 62322/14 and 24960/15) 18 September 2018. 316. See also, Keenan (n 109) 5-6; Van der Sloot and Kosta (n 91) 257.
[133] *Big Brother Watch* (n 132) 316.
[134] *Big Brother Watch* (n 120) 351.
[135] ibid 357-359.

Surveillance Camera Commissioner both exist to provide oversight.[136] Interestingly, the Court of Appeal concluded that it should not be for the Divisional Court to adjudicate on whether the SWP had an "appropriate policy document" regarding the use of AFR within the meaning of Section 42 of the DPA 2018 for determining the sensitive processing of data as the Information Commissioner exists to issue guidance on that point.[137] However, as mentioned earlier, there are limits to relying on such a highly procedural approach, largely because it reflects a form of surveillance bureaucracy whereby the courts end up limiting their own supervisory role. The overreliance on "oversight" bodies means that verifying the actual "need" for surveillance in general becomes difficult.[138] Moreover, such systems have been described by legal academics as "judicial-executive hybrids", and it is important to note that such systems have failed in their supervisory role in the past: i.e. like the surveillance programmes revealed by Edward Snowden.[139]

In adopting such a procedural approach – the debate on surveillance, or AFR, is then largely shaped through a definition of how "intrusive" a technology is rather than assessing its substantive necessity. In fact, the notion of "intrusiveness" played a key role in the *Bridges* litigation – and the concept shaped much of the Divisional Court's assessment on the "proportionality" of AFR use.[140] Interestingly, the Divisional Court, in accordance with Lord Sumption's judgment in *Catt*, had said that: "intrusive methods" only equate to "entry on private property or acts […] which would constitute an assault".[141] Accordingly, AFR was not like fingerprints or DNA because there exists: "no physical entry, contract or force […] to obtain biometric data".[142] The Court of Appeal agreed, but nonetheless stated that AFR was not "analogous" to photographs or CCTV either,[143] thus pushing the debate to focus on procedural safeguards, i.e. how the collected data is "utilised, stored, and destroyed" rather than addressing the need for collecting mass data and assessing whose biometric data should be stored in the Police National Database.[144]

C. Data protection: *Bridges v South Wales Police*

We briefly turn to how data protection law responds to the growth of data within the context of facial recognition, showing that whilst individual protection

136 *Bridges* (n 3) 108.
137 *Bridges* (n 3) 160-161.
138 Bernal (n 67) 259.
139 Keenan (n 109) 14.
140 Kotsoglou and Oswald (n 111) 87.
141 *Bridges* (n 2) 74; refer also to: *Catt* (n 95) 7.
142 ibid 75.
143 *Bridges* (n 3) 77.
144 Keenan (n 109) 8. See also, Bernard Keenan, 'Automatic Facial Recognition and the Intensification of Police Surveillance' *Modern Law Review* (2021) 1-21, 17.

is considered, the law does not sufficiently control the initial *collection* of that data. Put very simply, regulation protects "personal data" – i.e. the information about an identifiable individual. However, understanding that data "is a commodity challenges the status quo".[145] This is because the gathering of image data "depersonalises the individual data subject; whereby, ultimately the subject becomes a template for future reference or [even] a marketing target".[146] Accordingly, there is a sense that a "weakening of the process of individualisation" might begin to occur, particularly as a highly proceduralised methodology is followed.

In many ways, Edward Snowden has accurately captured how the problematic nature of data protection laws, including GDPR, is simply cited within the name: "the concern is with data protection, not data collection".[147] In this manner, the laws in place also exist to list procedures, rather than addressing wider questions over the necessity of collecting large amounts of data. As the Appellants had contended in their skeleton argument before the court: "The Defendant places considerable reliance on the DPA 2018. […] [T]he data protection principles contain little of specific relevance to determine when and in what circumstances the capturing of facial biometrics through AFR is or is not permissible".[148]

The Divisional Court had explained that the first key issue in regard to the data protection claims, concerned the extent to which AFR involved the processing of personal data according to the Data Protection Act 2018 (DPA). Interestingly, the Divisional Court reasoned that AFR does "individuate" people in the sense that AFR will distinguish individuals from one another: an indication that data protection principles will apply.[149] Though the individual would be taken into consideration once data is processed, the impact of data surveillance is largely "portrayed" to occur when data is examined by humans and not when it is gathered or decoded by an algorithm.[150]

To that end, the Court of Appeal adjudicated on two points: first, whether the SWP had complied with the obligation to undertake an "impact assessment" – in compliance with section 64 of the DPA 2018; and second, given that AFR involves the "sensitive processing" of an individual's biometric data by a public authority, whether the SWP would be expected to comply with three requirements enlisted in section 35(5) per DPA 2018. Specifically, the Court of Appeal was

[145] Ian Berle, 'The Future of Face Recognition Technology and Ethics: Legal Issues' in Berle Ian, *Face Recognition Technology* (Springer 2020) 180.

[146] ibid.

[147] Marius Dumitrescu, 'WebSummit 2019 – Edward Snowden: The problem isn't data protection. The problem is data collection' (*YouTube*, 5 November 2019) <https://www.youtube.com/watch?v=Ezp16KD8dVw> accessed 28 July 2021.

[148] Squires QC (n 85) 68.

[149] *Bridges* (n 2) 122, 124.

[150] Bernal (n 67) 243.

concerned only with the third criteria: if data processing occurs, the "controller", for example, the police, must have an "adequate" policy document in place (section 42 of the DPA 2018) that outlines all procedures relating to the sensitive handling of information, including the retention and deletion of data.

On the first point, and based on their Article 8 justifications, the Court of Appeal held that the "impact assessment" by the SWP had failed to properly assess the "risks to the rights and freedoms of data subjects".[151] There is a sense that the Court of Appeal recognises how AFR can "weaken" the position of the individual given the fact almost anyone could have been placed on the watchlist.[152] However, on the second point, the Court of Appeal dismissed the claim. The Divisional Court had said the SWP had an existing policy document, even though it may have lacked sufficient detail.[153] It was agreed that it was up to the Information Commissioner to give "further guidance" on the level of detail necessary, rather than having the judges intervene. It shows the courts relying on the oversight of regulatory bodies and the existing formal safeguards – a position the Court of Appeal was quick to adopt.[154]

To some extent, we might say that the "political struggles" for data protection (and privacy) are somewhat "losing strategies"[155] as norms for surveillance as both favour a highly procedural method. In this way, the law is not so much "ruling" as it is moderating, regulating, and also responding to the need for balance. The recent Court of Appeal judgment ultimately gives way for the future regulation of AFR, rather than acknowledging wider issues regarding the actual need for AFR use and the impact it may have on individuals.

V. The Face: A Mechanism of Individualisation

This last section remembers the idea of the face as a mechanism of individualisation. To reiterate, Celis indicates that even though the growth of mass surveillance helps us trace a "shift from individual to population" the human face – which "belongs to the human domain of individuality" – is still important to the debate on AFR. He highlights that: "the face is always political", and therefore, it becomes useful to consider the "concrete circumstances which trigger the social production of the face".[156] This section will expand on this analysis through

[151] *Bridges* (n 3) 152-153.
[152] ibid 152.
[153] *Bridges* (n 2) 139-141.
[154] *Bridges* (n 3) 161.
[155] Celis Bueno (n 8) 88.
[156] ibid 77.

its socio-legal perspective, and in particular reflects on the importance of the 'watchlist' given its vital role in selecting faces to help categorise the individual.

In *Discipline and Punish*, Foucault suggests that disciplinary societies "characterize, classify, specialize; they distribute along a scale, around a norm, hierarchize individuals in relation to one another and, if necessary, disqualify and invalidate".[157] Celis, however, draws attention to another important passage in Foucault's book that pinpoints how disciplinary techniques "mark the moment when the reversal of the political axis of individualisation […] takes place".[158] Foucault describes how in feudal regimes, and perhaps certain other societies too, individualisation belonged to the "echelons of power". However, inside the modern, or disciplinary society, as power is "more anonymous and more functional, those on whom [power] is exercised tend to be most strongly individualised". Accordingly, "in a system of discipline, the child is more individualized than the adult, the patient more than the health man, the madman and the delinquent more than the normal and the nondelinquent".[159]

However, as suggested earlier, Foucault, as well as Deleuze, elucidate the ways in which mechanisms of "security" and "control" gradually replaced disciplinary societies, which implies the individual is also replaced by the population as the new mode of power.[160] Nonetheless, as Celis contends, even if the individual might recede in the society of control, the "face" still retains "haunting significance and political consequence".[161] He suggests that the face gathers new meaning if understood from the context of "social subjection".[162] This can be explained as a "diagram of power" that sees humans "subjected" to external objects, such as machines. Celis notes that if facial recognition is viewed as an "apparatus of social subjection [AFR technologies] link the face to a private individual, rendering the face as the sign of a privatized body".[163] This is how subjects become: 'a potential "consumer", "criminal" or "terrorist"'.[164] In other words, social subjection provides

[157] Foucault (n 35) 223.
[158] ibid 192. See also, Celis Bueno (n 8) 79.
[159] Foucault (n 35) 192-193.
[160] Celis Bueno (n 58) 79.
[161] Claudio Celis Bueno, 'The Face Revisited: Using Deleuze and Guattari to Explore the Politics of Algorithmic Face Recognition' (2020) 31 Theory, Culture & Society 73-91, 81.
[162] Celis Bueno (n 8) 81.
[163] ibid 83.
[164] ibid.

roles, it categorises, and it "produces individual subjects with identities – and ID cards".[165]

Therefore, the face itself remains pertinent to the debate on ARF as the technology is still "automating the process of individualisation".[166] In a somewhat more Foucauldian manner, the consequence is that individuals can be easily hierarchized in relation to one another – and selected within the crowd. In regard to AFR, this process occurs most acutely though the formulation of the "watchlist", which simultaneously acts as a legitimating system for the deployment of AFR by the state.

A. The 'watchlist'

Faces within a crowd will be cross-referenced against a prepopulated 'watchlist' of individuals during an AFR operation. The facial geometry of identifiable information is collected from the individual and will then be aggregated against an image on the watchlist made up of specific identifiable faces. This will subsequently generate new data about an individual i.e. whether or not that "face" is of interest to the authorities.[167] If no match occurs, the system will delete the data.

In *Bridges*,[168] the Divisional Court eloquently situated how watchlists are generated from images held on police databases, a practice that is part of "ordinary" policing tactics.[169] In our discussion on mass surveillance, we allude to the notion that compiling watchlists is within the common law powers of the police.[170] For AFR, the SWP would create bespoke watchlist of suspected individuals that may be present at the deployment, anywhere between four-hundred to eight-hundred people.[171] Importantly, the Divisional Court described how the SWP had categorised individuals into separate watchlists, for example, "persons wanted on warrants", "individuals who are unlawfully at large" or "vulnerable persons" – to name a few.[172] Therefore, the watchlist acts as the identifier of faces.

Ed Bridges, the Claimant, was not on the watchlist. In fact, the Divisional Court made the claim that Ed is "not a 'victim' in this regard, and therefore can

[165] McKenzie Wark, 'Maurizio Lazzarato: Machinic enslavement' in Wark McKenzie (ed.), *General Intellects: Twenty-One Thinkers for the Twenty-First Century* (Verso 2017) 77–92, 78-79.
[166] Celis Bueno (n 8) 83.
[167] Joe Purshouse and Liz Campbell, 'Privacy, Crime Control and Police Use of Automated Facial Recognition Technology' (2019) 3 Criminal Law Review 188-204, 208.
[168] *Bridges* (n 2).
[169] ibid 30.
[170] ibid 77. See above (n 81).
[171] ibid 30-31.
[172] ibid 30.

have no personal complaint about the watchlists".[173] The initial decision detailed that there was "no minimum threshold of seriousness for the types of offences" to be included on the watchlist, subject to overarching provisions on proportionality.[174] And yet, there remained a general lack of transparency in terms of which individual faces will be selected for the watchlist, i.e. who are the police targeting.

Today, the Court of Appeal, unlike the Divisional Court, has perhaps given a greater degree of importance to the notion of the individual face: "who" might be categorised on the watchlist. For example, the Court of Appeal recognised that "persons where intelligence is required" was not an objective category as it could cover "anyone who is of interest to the police".[175] In their words, the "fundamental deficiencies" in the legal framework concerned 'the "who" and "where" question'. The judgment suggested that perhaps: "once the 'who' question can be satisfactorily resolved, that will give clear guidance as to the 'where' question".[176] In relation to both questions, the Court of Appeal expressed concern that there is "too broad a discretion vested in the individual police officer to decide who should go on the watchlist".[177]

In a study on the politics of "blacklisting individuals", Margaret Hu suggests that "matches and mismatches" in watchlist systems ultimately creates an inferred guilt because it can "categorise individuals as administratively 'guilty until proven innocent' by virtue of [a] digitally generated suspicion".[178] Importantly, if facial recognition identifies a possible match between a face and the watchlist image, it will be up to the "system operator", for exa the police, to establish whether a match has in fact occurred.[179] The Divisional Court had suggested that "the human eye" acts as a vital safeguard "to ensure that an intervention is justified".[180] However, whether it will ever be a safeguard that is truly objective is somewhat open to debate, particularly when an officer is required to act in real-time to a finding provided by the algorithm.[181] In many ways, it raises the possibility for discrimination, which led the Court of Appeal to agree that the issue "ought to be considered properly […] as human beings can also make mistakes. This is particularly acknowledged in the

[173] ibid 77.
[174] ibid 31.
[175] *Bridges* (n 3) 124.
[176] ibid 96.
[177] *Bridges* (n 3) 124.
[178] Margaret Hu, 'Big Data Blacklisting' (2016) 67 Florida Law Review 1735, 1744.
[179] ibid 33.
[180] ibid.
[181] Kotsoglou and Oswald (n 111) 88.

context of identification".[182] The Court concluded that police forces must take all "reasonable steps" to ensure the software does not have a racial or gender bias.[183]

Interestingly, Jackie Wang writes that police forces in general have recently begun to adopt the logic of "objectivity" and "science" to respond to their critics. She argues this is a clever way to take away agency from individual officers and show the police is being "neutral, unbiased and rational".[184] Objectivity is an essential way to "retain public support […] [and] solve the police's crisis of legitimacy".[185] Nonetheless, the belief that facial recognition algorithms create "objectivity" when they identify persons of interests in real time overshadows the issue that this technology can reproduce, or even intensify, the biases that already exist in modern day policing.[186] As Gutherie Ferguson has said: "the danger, of course, is that human consequences get subsumed in the quest for technological guidance".[187] The visual artist Trevor Paglen adequately captures this feeling when he wrote: "because image operations […] are not (actually) dependent on a human seeing-subject […] they are harder to recognise for what they are: immensely powerful levers of social regulation that serve specific race and class interests while presenting themselves as objective".[188]

B. Beyond the face, the future for the individual

From the above discussion, it is worth asking whether the individual can ever be the 'victim' of facial recognition technologies. I pose this question because it previously seemed highly dependent on whether or not your face was on the watchlist. Today, Ed Bridges has shown that if you are not on the watchlist, there will be safeguards in place to challenge your privacy rights. However, what happens to those individuals whose face is on a watchlist? We know that the Court of Appeal accepts it will not "design" the future policies on it,[189] making it a matter of time before new regulation comes in.

The 'risk' of being on an AFR watchlist is likely to be higher for people with minor or previous convictions. The risk is intensified because of the general legal safeguards that currently oversee the collection and retention of custody images by the police, as this can include pictures of people that may have had contact with

[182] *Bridges* (n 3) 173, 185.
[183] ibid 181, 201.
[184] Wang (n 33) 236-237.
[185] ibid.
[186] Purshouse and Campbell (n 153) 200. See also, Kotsoglou and Oswald (n 11) 88.
[187] Ferguson (n 56) 198.
[188] Paglen, Trevor, 'Invisible Images (Your Pictures Are Looking at You)' (*The New Inquiry*, 9 December 2016) <https://thenewinquiry.com/invisible-images-your-pictures-are-looking-at-you/> accessed 28 July 2021.
[189] *Bridges* (n 3) 94.

the police but were then never convicted. In *Catt*, the Supreme Court held that the retention of personal data by the police for someone with a "clean record" can still be justified for three key reasons – all related to allowing the police to take decisions on what makes individuals a public safety risk.[190] In Lord Sumption's words, it is difficult for the police to determine whether a "piece in the jigsaw is irrelevant". He continues: "the most than can be done is to assess whether the value of the material is proportionate to the gravity of threat to the public".[191] *Catt* cautions that it is not for the courts to interfere with how the police assess risk. In *Bridges*, the Court of Appeal held that though AFR is not analogous to taking photos or CCTV, *Catt* retained importance: "just as the human eye can observe a person in a public place […] the police have the power to take photographs of people".[192] The decision, in fact, implies that the general standard for being placed on a watchlist could remain relatively low.

Interestingly, at the *Bridges* appeal, the Appellant's barrister, Dan Squires QC, said AFR would "radically" alter the way Britain is policed in the future.[193] Earlier, we alluded to the idea that a key fear is the rise of predictive policing and the effects it has on the individual. The extreme is a situation whereby in "marking subjects as potential risks, they are actually produced as such".[194] Civil liberty groups, including Liberty, continue to remind us that it will be marginalised communities that will be the most affected in society.[195] We have begun to see these trends in countries like China, with great controversy surrounding the Muslim Uighur communities in the Xinjiang province. This region has been labelled as the "Frontline Laboratory for Surveillance".[196] Specifically, Human Rights Watch reports that facial recognition and other similar technologies are being used by Chinese government to "generate lists of individuals to be rounded-up by the police".[197] The result is to: "bolster its repression of the Muslim minorities […] by tracking virtually their every move, subjecting them to mass arbitrary

[190] *Catt* (n 95) 29.
[191] ibid 31.
[192] *Bridges* (n 3) 84.
[193] Bowcott (n 18). Court of Appeal Trial, R (*Bridges) v CC South Wales & ors* (C1/2019/2679) N.p. 2020. Web. 23-25 June 2020.
[194] Wang (n 33) 43.
[195] Carlo (n 10) 41.
[196] ibid 36.
[197] Human Rights Watch, 'China: Big Data Fuels Crackdown in Minority Region: Predictive Policing Program Flags Individuals for Investigations, Detentions' (*Human Rights Watch*, 26 February 2018) <https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region> accessed 28 July 2021.

detention, forced political indoctrination, restrictions on movement, and religious oppression".[198]

It is important to draw attention to the situation in China because even though some might repeat the mantra: *if you have nothing to hide, you have nothing to fear*, the value of understanding the breadth of this technology will ultimately allow the individual, and therefore the collective, to "recognise the pervasive aspect of […] regimes of power"[199] – perhaps like Ed Bridges, and his legal team, did in the UK.

VI. Conclusion

This article began by illustrating the stories of two individuals: Ed Bridges and Robert Williams – both impacted by facial recognition in their own way. These are not unique stories, nor do they tell us everything that we need to know about this technology, but they can help us understand why the individual has a problematic relationship with a tool like facial recognition. However, the Court of Appeal's decision also shows that an individual, in this case Ed Bridges, can act to resist AFR.

In light of the continual expansion of AFR as the technology improves, it is useful to theorise on the mechanisms of power that sit beneath the notion of the individual within the context of facial recognition. Using Deleuze, in particular, we traced the idea that digital technologies no longer sustain the individual as the product of self-identity, as shown under Foucault's description of disciplinary modes of power. Instead, the individual is being replaced with the notion of the "*dividual*" – he/she is reduced merely to observable data.

We must remember that *Bridges* is the first case in the world adjudicating on AFR, which means the debate is still taking shape, and therefore, often appears heavily contradictory. As Celis described, facial recognition technologies have this dual inconsistency: on the one hand the position of the individual is weakened, but on the other, we also must recognise that AFR also means the ever-growing centrality of the face as a mechanism of individualisation.[200]

This article considered the contradictory duality in Celis' argument through a legal context. First, we explored how the law responds to the way AFR has increased the "potential" for mass surveillance by the state, and why this leads to a problematic or "weakening" role for the individual. We found that the courts will use a procedural approach to respond to surveillance methods to allow the state to determine what might be "necessary in democratic society". This is beneficial

[198] Maya Wang, 'The Robots Are Watching Us' (*Human Rights Watch*, 6 April 2020). <https://www.hrw.org/news/2020/04/06/robots-are-watching-us> accessed 28 July 2021.

[199] Celis Bueno (n 8) 88.

[200] Celis (n 58) 81.

to the courts given the risk of adjudicating on seemingly politicised decisions. However, procedural requirements for facial recognition simply "set the conditions for surveillance to occur, which will normalise tracking and identification, as well as reorganise and entrench organisational structures and practices"[201] – all of which intensify the "weakening" of the individual. Second, we reviewed why facial recognition has simultaneously created a situation whereby algorithms develop a "securitised identity" for the individual through their faces – a process that has in some ways become legitimised through the parameters of the watchlist. In fact, a unique characteristic of facial recognition technology is the watchlist, which carries with it a capacity to both categorise and amplify structural issues in society.

The global Covid-19 pandemic and the Black Lives Matter protests in 2020 (and beyond) have shown how quickly debates on facial recognition can be reignited, even in favour of a complete ban. Interestingly, various civil liberty groups in the UK, including Liberty or Big Brother Watch, campaign to ban AFR.[202] Arguably, this debate has become more pertinent since various conglomerates, including Amazon or Microsoft, declared a moratorium on the sale of AFR technologies to law enforcement bodies in the US in the wake of George Floyd's death.[203] With this in mind, it might be interesting to consider what legal arguments exist that that could enable a ban on this technology, particularly as Robert Williams, the man wrongfully arrested because of a fault in the system, seeks a ban in the US.[204]

Having said that, it is interesting to note that Liberty, in advocating for Ed Bridges at trial, falls short in asking the Court to issue a ban. In their submissions before the courts they write: "The Claimant does not suggest that the Defendant or other police forces could never lawfully deploy AFR".[205] In fact, the legal arguments in the courts often evolve around the need to develop legal regimes to

[201] Evan Selinger and Woodrow Hartzog, 'The Inconsentability of Facial Surveillance' (2020) 66 Loyola Law Review 101, 117.

[202] Liberty, 'I Resist Facial Recognition' (*Liberty Human Rights*, 2020). <https://www.libertyhumanrights.org.uk/campaign/resist-facial-recognition/> accessed 28 July 2021. See also, Big Brother Watch, 'Stop Facial Recognition' (*Big Brother Watch*, 2020) <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>.

[203] Paul Kari, 'Amazon to ban police use of facial recognition software for a year' (*The Guardian*, 11 June 2020) <https://www.theguardian.com/technology/2020/jun/10/amazon-rekognition-software-police-black-lives-matter> accessed 28 July 2021; BBC, 'IMB abandons "biased" facial recognition tech' (*BBC News*, 9 June 2020) <https://www.bbc.co.uk/news/technology-52978191> accessed 28 July 2021; Louise Matsakis, 'Amazon Won't Let Police Use Its Facial-Recognition Tech for One Year' (*Wired*, 10 June 2020) <https://www.wired.com/story/amazon-facial-recognition-police-one-year-ban-rekognition/> accessed 28 July 2021; Karen Weise 'Amazon indefinitely extends a moratorium on the police use of its facial recognition software' (*The New York Times*, 18 May 2021) <https://www.nytimes.com/2021/05/18/business/amazon-police-facial-recognition.html> accessed 28 July 2021.

[204] ibid (n 6).

[205] Squires QC (n 85) 2.

protect privacy and data protection rights. In this way, both the political and social struggles for privacy and data protection are to a certain degree "losing strategies:" they tend to favour a highly procedural method instead of asking why collecting mass data is a necessity in the first instance, an approach that perhaps is better suited to understanding the position of the individual within the facial recognition debate.

For these reasons, we should recognise that the Court of Appeal's judgment paves the way for new regulation and Parliamentary scrutiny, which may indicate why police forces did not want to dispute the judgment further.[206] In fact, at the time of writing, the Police, Crime, and Sentencing Bill is making its way through the Commons, and although there is no specific law on facial recognition, Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), a body responsible for assessing effective policing (amongst other things), has published a report outlining a '"need to develop" covert intelligence gathering methods and an expectation of increased use of facial recognition technology.[207]

Shortly after the Court of Appeal's judgement was published, the SWP noted that they would remain "completely committed to its careful […] deployment" stating they were "proud of the fact there has never been an unlawful arrest"[208] – and labelled the final decision as "a judgment that we can work with".[209] By contrast, the London Metropolitan Police publicly stated that whilst the judgment will be taken into consideration, London's policing needs are "different" from the issues raised in the appeal against the SWP. To their mind, so long as their use of the technology is "intelligence-led" it can be used as a tool to fight "serious crime" in the capital, an approach that could also bring about future legal challenges.[210] And yet, for all its weaknesses, the *Bridges* judgment still demonstrates the paramount

[206] Keenan (n 144) 19; Dan Sabbagh, 'South Wales Police lose landmark facial recognition case' (*The Guardian,* 11 August 2020) <https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case> accessed 28 July 2021.

[207] Haroon Siddique, 'Civil liberties groups call police plans for demos an "assault" on right to protest' (*The Guardian*, 11 March 2021) <https://www.theguardian.com/law/2021/mar/11/civil-liberties-groups-call-police-plans-for-demos-an-assault-on-right-to-protest> accessed 28 July 2021.

[208] Jenny Rees, 'Facial Recognition use by South Wales Police ruled unlawful' (*BBC*, 11 August 2020) <https://www.bbc.co.uk/news/uk-wales-53734716> accessed 28 July 2021.

[209] ibid.

[210] Metropolitan Police, 'Live Facial Recognition' (*Metropolitan Police*, 2020) <https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/> (accessed 28 July 2021).

importance of an independent judiciary – particularly at a time where there are signs it may come under attack from the state.[211]

In many ways, facial recognition serves as a metaphor for the potential of increased surveillance – given that it forms part of our "invisible visual culture".[212] Interestingly, through the coronavirus pandemic we have witnessed quick changes to the monitoring of our everyday lives: the need to "track and trace" or "vaccine passports" was largely unthinkable prior to the pandemic. And yet, as Deleuze eloquently reminds us: "There is nothing to fear or hope, but only to look for new weapons".[213] To that end, we need to reflect on how the law can work to achieve much greater transparency to support the individual, rather than allow AFR – and technology in general – to become a tool that develops a perpetual state of surveillance.

[211] Tom Clark and Alex Dean, 'Judges in the dock: the inside story of the battle for Britain's Courts' (*Prospect*, 24 January 2020) <https://www.prospectmagazine.co.uk/magazine/judges-in-the-dock-battle-britain-courts-boris-johnson-prorogation-supreme-court-hale-miller-constitution> accessed 28 July 2021. See also, Editorial. 'The Guardian view on Boris Johnson in court: Brexit's war on the law' (*The Guardian*, 12 February 2020); Haroon Siddique, 'Judicial review changes will make government "untouchable", warns Law Society' (The Guardian, 30 April 2021) <https://www.theguardian.com/law/2021/apr/30/judicial-review-changes-will-make-government-untouchable-warns-law-society> accessed 28 July 2021.

[212] Paglen (n 186).

[213] Deleuze (n 32) 4.