CHAPTER 13

'Not Ready for Prime Time': Biometrics and Biopolitics in the (Un)Making of California's Facial Recognition Ban

Asvatha Babu and Saif Shahin

Introduction

On 8 October 2019, Governor Gavin Newsom signed a law forbidding California police departments from using facial recognition (FR) software on body cameras. The decision was welcomed widely, especially by civil society groups that have long called for outlawing 'an invasive and dangerous tracking technology that undermines our most fundamental civil liberties and human rights' (ACLU 2019a). AB-1215, or The Body Camera Accountability Act, came on the heels of bans on government use of FR in five US cities earlier that summer: San Francisco, Berkeley, and Oakland in California, and Cambridge and Somerville in Massachusetts (Cagle 2020).

FR is a form of biometric artificial intelligence that involves 'the automated process of comparing two images of faces to determine whether they represent the same individual' (Garvie, Bedoya and Frankle 2016, 9). Attempts to use computers to identify human faces go back at least half a century (Goldstein, Harmon and Lesk 1971) and FR technology has become commonplace in recent years. We use it every day to unlock our mobile phones or tag friends on social media. Companies employ it to improve user profiles for targeted

How to cite this book chapter:
Babu, A. and Shahin, S. 2021. 'Not Ready for Prime Time': Biometrics and Biopolitics in the (Un)Making of California's Facial Recognition Ban. In: Verdegem, P. (ed.) *AI for Everyone? Critical Perspectives.* Pp. 223–245. London: University of Westminster Press. DOI: https://doi.org/10.16997/book55.m.

advertising. Law enforcement agencies mostly rely on FR for two purposes: *face verification* to confirm a claimed identity and *face identification* to 'identify an unknown face' (Garvie, Bedoya and Frankle 2016, 10).

Although both are contentious, it is the latter application that has raised the most eyebrows. Back in 2016, the Georgetown Law Center on Privacy & Technology reported that FBI searches for identity using FR were 'more common than federal court-ordered wiretaps' (Garvie, Bedoya and Frankle 2016, 25). The faces of nearly 117 million Americans were already in federal law enforcement databases and every other American adult had had their photos searched in this manner. Law enforcement agencies in the United States have dabbled in FR-based surveillance projects since 2001 (Gates 2011). Now, with advances in technology, police departments in various cities in the US, in conjunction with technology corporations, have initiated FR-based surveillance programs that use existing infrastructure like CCTV cameras such as Detroit's Project Greenlight, under which 'cameras all over the city keep an eye on the populace' (Colaner 2020). Others are experimenting with using FR on body cameras and mobile phones (Naughton 2020). The US Customs and Border Protection agency began deploying FR cameras at airports in 2017 (Oliver 2019) while immigration officers started running FR searches on driving license photos to identify undocumented immigrants since at least 2019 (Chappell 2019).

There is no federal law regulating the collection and use of biometric data in the United States. Illinois, Texas and Washington are the only states so far to pass comprehensive legislation regulating state and private collection of biometric information (Pope 2018). At the same time, facial data has become ubiquitous on the internet with the sharing of photos and videos on social media. An ecosystem of businesses, such as the controversial Clearview AI, have sprung up that take advantage of this ubiquity and regulatory lag to build massive databases and cheap tools for the state to use (Mann and Smith 2017; Naughton 2020; Hill 2020; Kak 2020).

California's AB-1215 law, which came into effect in January 2020, is part of a slew of local, state and federal attempts to check this proliferation. In 2019, San Francisco, home to global tech giants and one of the most technologically advanced cities in the world, became the first US city to ban FR use by law enforcement. It was quickly followed by Somerville, Massachusetts and Oakland, California (Metz 2019). In October 2019, California became the third state to issue a ban, following Oregon and New Hampshire (Thebault 2019). As the namesake of the Californian Ideology (Barbrook and Cameron 1996), an uncritical 'technological solutionism' (Morozov 2012) and belief in 'dotcom' neoliberalism, it is particularly interesting that California has been one of the earliest movers in attempting to regulate this emerging technology.

In the wake of nationwide – indeed global – protests after the killing of 46-year-old George Floyd in May 2020 by the Minneapolis Police, reports of FR use by law enforcement to identify and arrest protestors has further fuelled

demands to remove the technology from the arsenal of law enforcement agencies around the country (Colaner 2020). In June 2020, the Detroit police came under fire for arresting an innocent Black man after FR technology flagged him as a shoplifting suspect. As activists mounted pressure on the city council to reject the proposed extension of the police FR contract, the Detroit Police Chief admitted that the FR system fails to accurately identify faces approximately 95% of the time (Cameron 2020; Colaner 2020; Ferretti 2020). Around the same time, Boston became the biggest city on the US East Coast to ban FR for municipal use. Two US senators have proposed federal legislation calling for 'a full stop to facial recognition use by the government' at all levels nationwide (Ng 2020b). Even companies such as Amazon, IBM and Microsoft announced that they would not be selling the technology to law enforcement (NPR 2020).

And yet, it may still be too early for critics of FR and other forms of algorithmic surveillance to rejoice. Widespread calls to abolish carceral technologies and practices that disproportionately affect Black Americans (Benjamin 2016) have put pressure on private industry, not necessarily to stop building FR for the government but to at least manage the optics of their involvement. Seen in that light, some of these moves appear to be little more than short-lived attempts at corporate image management. Amazon, for instance, made it clear that its moratorium on the sale of its FR tool Rekognition to law enforcement would only be for a year.

Without the visibility provided by these protests and the sustained pressure of activists, it is possible that some of these uses may have gone on unchecked and unexamined. Indeed, many of these companies continue to sell FR technology to governments outside of the United States where there is little pressure from civil rights groups or movements like Black Lives Matter (Barik 2020). Documents released a week after Microsoft's announcement revealed it had previously been trying to sell FR technology to federal agencies without any regard for human rights, contrary to sentiments expressed by the company's president (Ng 2020a).

Even AB-1215 may not be the 'victory' (Guariglia 2019) it seems at first glance. Initially intended to prohibit Californian police's use of FR on body cameras permanently, the bill was gradually diluted and defanged. The version that was passed into law proscribes FR use for only three years. In this chapter, we adopt a *law and society* approach – which views legislation as a social phenomenon (Ewick and Silbey 1998) – to explain how and why this came about. In this approach, researchers study law and *legality* as situated in society and laced through its culture by examining both the 'formal and informal settings where legal activity – in all its guises – may unfold' (Seron and Silbey 2004, 30). Our study traces the trajectory of AB-1215 from its introduction as a 'spot bill' on 21 February 2019 through its signing into law eight months later – both as legislative action within the state assembly and as public deliberation outside the corridors of the capitol. We critically examine legal documents as well as

reports from the civil society and news media as a social discourse with a view to understanding (1) how FR technology was perceived and presented by different stakeholders, specifically in terms of its benefits and harms and (2) what factors and actors contributed to the diminution of the law.

We next discuss a range of socio-political concerns raised by FR and outline a conceptual framework for thinking about FR regulation in the light of these concerns. Then, following a brief discussion of the passage of AB-1215, we turn attention to our empirical analysis of the bill as a social discourse. We conclude with an assessment of how and why the bill was defanged and consider how it can inform future research and resistance against algorithmic governance.

Inaccuracy and Mass Surveillance

The application of FR for law enforcement raises three interrelated concerns. The first is the *inaccuracy* of the technology itself, or the possibility that an individual is not who the FR algorithm identifies them as. That is because 'biometric recognition is an inherently probabilistic endeavour' (Pato and Millett 2010, 9). FR technology doesn't *see* faces – the way humans do – but offers probable *matches* based on geometric representations of facial features. Making computers 'see' – i.e. engineering computer vision – is a difficult task that scientists and engineers have mulled over for decades. Advances in the ability to store and crunch large amounts of data as well as in machine learning algorithms have led to breakthroughs in recent years (Demush 2019). At first, the algorithm is trained to recognise which facial features are more likely than others to indicate similarity by analysing different images of the same person from a large training data set. This is known as machine learning. It then applies this learning to identify images of the same individual in real-life law-enforcement scenarios (Huang et al. 2008). But this machine learning involves 'millions of variables' – such as lighting, picture quality, and subject distance, for example – and is never perfect (Garvie, Bedoya and Frankle 2016). The FR algorithm, therefore, does not produce the 'right' match for an image but a series of more or less likely matches.

In 2018, ACLU – the American Civil Liberties Union – tested the accuracy of Amazon's Rekognition, a top FR platform used by government agencies throughout the United States. The FR tool failed spectacularly: 'the software incorrectly matched 28 members of Congress, identifying them as other people who have been arrested for a crime' (Snow 2018). ACLU repeated the test in August 2019. This time, Rekognition misidentified 26 California legislators as criminals – among them Phil Ting, the author of AB-1215 (Chabria 2019). This lack of accuracy means that when law enforcement uses FR uncritically, many innocent people could end up on their radar, go to jail, be deported or, in countries such as the US, face the death penalty.

The second concern is their propensity for *mass surveillance and violation of privacy*. This happens in two ways. One, law enforcement agencies collect photographs of people to populate their FR databases – and they do so indiscriminately. Referring to the FBI program, the Georgetown Law report noted, 'Never before has federal law enforcement created a biometric database – or network of databases – that is *primarily* made up of law-abiding Americans' (Garvie, Bedoya and Frankle 2016, 20, emphasis added). So far, these photographs have been mined from people's driving licences, ID cards and even social media accounts. As FR is employed via cameras at airports, on police personnel and so on, people will be subjected to facial 'tracking from far away, in secret' and en masse (10). This makes it nearly impossible for people to manage their boundaries, a key practice in maintaining dynamic privacy relationships. This, in turn, makes it difficult to practice critical citizenship and aspire to the ideals of liberal democracy (Cohen 2012).

Two, a significant feature of 'high-dimensional' – or individualised – data collection is that it allows cross referencing of multiple data sets (boyd and Crawford 2012). In other words, information about an individual in one data set can be used to find more about that individual by linking it with other data sets. So, while law enforcement agencies might compile FR databases putatively for identifying individuals in situations where a law is violated, they could easily use the photographs to track various other activities of the individual – including activities that may be perfectly legal but politically undesirable for authorities, such as participating in protests against police violence. As was revealed by NSA whistle-blower Edward Snowden, this information can be easily obtained by the US government through social media and phone records (Greenwald, MacAskill and Poitras 2013). When this issue is coupled with FR's inaccuracy, it means that '[e]ven if you're sitting at home on your couch, there's a chance you could be arrested for protesting' (Shwayder 2020).

Biopolitics of Facial Recognition

A third problem with FR systems is their proclivity to perpetuate and amplify *social discrimination* against marginalised communities. This is only partly a consequence of its technical flaws, which are also not arbitrary: 'if a training [data] set is skewed towards a certain race, the algorithm may be better at identifying members of that group as compared to individuals of other races' (Garvie, Bedoya and Frankle 2016, 9). The Silicon Valley's whiteness and apparent 'colour blindness' means FR training data are overwhelmingly White and therefore several times more likely to misidentify Black people (Buolamwini and Gebru 2018; Simonite 2019) – driving up their already disproportionate rates of incarceration.

But social discrimination is not solely a function of machine learning or technology design. Immigrants and minorities – Black, Latinx and Muslim people

in particular – are already much more likely than White people to be singled out for surveillance via FR at the level of policymaking (Bedoya 2019) and disproportionately represented in law enforcement and intelligence watchlists (Devereaux 2019). Browne (2010) argues that the practice of making a body visible – or 'legible' – has always been an exercise in power, with political and economic ramifications. The branding of enslaved Africans on American plantations, for instance, was a means of 'accounting and of making the already hyper-visible body legible' – not exactly the same, but also not altogether different from the contemporary practice of making 'bodies informationalized by way of biometric surveillance' (139). Biometric technology reimagines the body as flows of data and patterns of communication (van der Ploeg 2002). Objectified and digitized 'individuals are broken down and reinterpreted in terms of the information provided by their body, instead of as agential social beings' (Hood 2020, 158). These data points are logged in a virtual register, making the bodies themselves legible, accountable, and thus controllable (Andrejevic, 2019).

Considered from this perspective, FR is only the latest chapter in a long history of authorities using technology to subjugate, racialise and dehumanise people by acting upon their bodies – the newest arena of 'biopolitics'. A biopolitical view (Foucault 2003) brings to surface the *systemic* nature of social discrimination. In this view, the technological inaccuracy of FR is itself a consequence of institutionalised racism and classism – evident in everything from education to hiring practices to law enforcement – that keeps marginalised bodies outside of Silicon Valley offices and inside of prisons. This view is at once micro and macro: it segues from the datafication of human body to map the geography of social belonging that such data enables. Gandy Jr. (1993) showed how the economic value of a person's data differed depending on the social group they belonged to and how this differentiation reproduced social inequalities. As he noted, surveillance goes beyond social control and into the realm of sorting and differentially targeting people based on their positionality in the socio-economic hierarchy.

Petit (2017) makes a distinction between discrete and systemic 'externalities' that accrue from artificial intelligence systems. Externalities could be either harms or benefits to third parties. *Discrete externalities* are 'personal, random, rare or endurable' (26). They take place at the level of the individual, may affect anyone with an equal chance, are low in frequency and neither ruin nor radically improve the affected individual's life. Examples include a malfunctioning robot mistaking a garden-variety rodent for a parasite and spraying it with pesticide. *Systemic externalities* are 'local, predictable, frequent or unsustainable' (26). In other words, they are foreseeable, take place repeatedly, affect 'a non-trivial segment of the population' and can cause a long-term 'reduction or increase in well-being of the local population class under consideration' (26). For instance: China's reported use of automation and cutting-edge technological tools to surveil and detain its largely Muslim Uighur population (Taddonio 2019).

This distinction helps us think normatively about AI regulation. Petit (2017) recommends that discrete externalities 'should be left to the basic legal infrastructure' (28). That is, emergent problems could be resolved on a case-by-case basis in an *ex-post* manner – or after they occur – by applying specific laws that are already in place. But systemic externalities require *ex-ante* consideration. As they are not only predictable but also significant in the scale of their impact, their repercussions need to be anticipated and lawmakers ought to institute regulations to mitigate the harms they might cause.

Are FR's externalities discrete or systemic? A purely technological view that is restricted to FR's inaccuracy would consider them to be discrete – random, rare and occurring at the level of the individual. But a biopolitical view, as outlined above, enables us to see that FR's externalities are in fact *systemic* in nature – causing frequent and permanent harms to large and identifiable populations. FR therefore requires ex-ante regulation that anticipates these harms and prevents them.

A Brief History of AB-1215

In a blogpost about ACLU's 2018 test on Rekognition which demonstrated its fallibility, Jacob Snow, Technology and Civil Liberties Attorney with the ACLU, wrote: 'These results demonstrate why Congress should join the ACLU in calling for a moratorium on law enforcement use of face surveillance' (Snow 2018). This test from ACLU, combined with mounting academic research on the discrete and systemic harms of FR, has become a cornerstone for calls to ban the use of facial recognition technology by government agencies and law enforcement organisations (Metz 2019). AB-1215, in California, was one such call.

AB-1215 was signed into law in October 2019 and came into effect in January 2020 for a three-year period. It states that: '[a] law enforcement agency or law enforcement officer shall not install, activate, or use any biometric surveillance system in connection with an officer camera or data collected by an officer camera' (Body Camera Accountability Act 2019e, 3).

The spot bill for AB-1215 was introduced in February 2019 by Democratic member of California's State Assembly, Phil Ting. With the support of ACLU of Northern California and several other civil society organisations, Ting introduced the first substantive draft of the bill in the State Assembly on 8 April. This version of the bill was considerably different from the final version that would eventually be passed. For instance, it prohibited the installation, activation or use of biometric surveillance in connection with an officer camera *indefinitely*. It also made the law enforcement agency or official liable for damages up to US$4000 in addition to attorneys' fees (Body Camera Accountability Act 2019a). The bill made its arguments for a ban by drawing attention to the threat to civil liberties and the constitutional right to privacy and anonymity posed by FR, the possible chilling effect on free speech in public spaces,

FR's lack of accuracy in identifying people of colour and women, and the disproportionate impact of this technology on overpoliced communities. The bill also repudiated law enforcement's co-optation of tools meant to ensure their accountability (body cameras) into tools of dragnet surveillance (Body Camera Accountability Act 2019a).

On 23 April, the bill was debated and amended in the Assembly Public Safety Committee with the recorded support of 24 civil society organisations (including the ACLU of Northern California) and opposition from law enforcement groups including the California Police Chiefs Association and California State Sheriffs' Association. It passed through to the next stage with an amendment removing the specific amount that had to be paid in damages. When it passed with a 45–17 vote in the California State Assembly on 25 April, the ban on the use of FR in police body cameras was still indefinite (Body Camera Accountability Act 2019b).

In June, it was taken up in the California State Senate Committee on Public Safety, where it passed 5–2 without amendment. A couple of months later, while the bill was still on the backburner at the Senate, the ACLU of Northern California ran its second test using Rekognition which matched 26 California lawmakers including Phil Ting with criminal mugshots (Gardiner 2019a). Almost two weeks later, on 27 August, the bill was amended to include a sunset clause that repealed the bill on 1 January 2027. The amendments also excluded from the ban 'internal editing procedures for redaction purposes'; and the 'lawful use of mobile fingerprint scanning devices' (Body Camera Accountability Act 2019c, 3–4). In September, at its final reading before passage, the bill was amended to shorten the sunset period from seven to just three years and was set to expire on 1 January 2023 (Body Camera Accountability Act 2019d).

Thus, when the bill was signed into law, it was not so much a *ban* on the use of FR by law enforcement as a relatively short *moratorium* on a very specific use of the technology. While this was still considered a win by civil rights groups around the country, ACLU and Assembly member Ting's original intent to keep FR out of the arsenal of law enforcement in perpetuity was thwarted. How, and why, did this happen? And what can we learn from this qualified success to guide future attempts for regulating FR and other forms of algorithmic governance?

Research Design

To answer the questions above, we used the law and society approach (Seron and Silbey 2004) to track AB-1215 as social discourse, taking place both within and without the corridors of the state assembly, involving lawmakers as well as civil society groups, technology companies, police unions and the mass media. The passage of AB-1215 was a months-long process that involved these multiple stakeholders engaged in shaping the conversation

through reports, blog posts, press releases, media presence and participation in the legislative process. These artefacts offer important insight into the way the social discourse surrounding FR and its regulation evolved. Keeping in mind our objective to track this evolution, we conducted a qualitative content analysis of these artifacts.

We triangulated data from three sources: legislative documents such as bill and floor analyses; communication materials from organisations listed in legislative documents as supporting or opposing the bill; and local news coverage on AB-1215 between February (the introduction of the spot bill) and October 2019 (the signing of AB-1215 into act by the California governor). Although not exhaustive, these sources provided us with a comprehensive and diverse collection of stakeholders and their contributions to the conversation around AB-1215. They allowed us to examine the stakeholders' primary participation in the discourse through their own publications and statements as well as what was picked up by the media.

News reports were collected and combined from three databases – Access World News, LexisNexis and Factiva – using the search phrase: ['ab 1215' OR 'ab1215' OR 'ab-1215' OR 'a.b. 1215' OR California AND ('face recognition' OR 'facial recognition') AND ('police' OR 'law enforcement')]. Only articles published in the United States between 1 February 2019 and 31 October 2019, mentioning these terms in the headline or lead paragraphs were included in the corpus. Next, legislative documents were downloaded from the official California Legislative Information website. This included: the multiple versions of the bill from 21 February to 8 October (7 documents), bill and floor analyses at each stage (7 documents), and vote information. Finally, we manually downloaded any communications material mentioning 'AB-1215' from the websites of the civil society organisations mentioned as supporting and opposing the legislation. If there was no mention of the bill, we chose any materials that discussed 'facial recognition' within our target dates. This yielded a total of 38 documents for analysis. After discarding duplicate and irrelevant articles from the media coverage, we had a total of 148 documents (96 news articles, 14 legislative documents and 38 outreach materials).

Following Mayring (2004), analytical criteria were determined based on our research question as: arguments made in support of facial recognition use by law enforcement; arguments made against facial recognition use in body cameras by law enforcement; actors making these arguments; and social and political values present. These documents were then read line-by-line to develop inductive codes. In the first cycle of coding, we used the 'in-vivo' or 'literal' coding technique (Saldaña 2009) wherein exact phrases from the actual language of the documents can be used as code. According to Charmaz (2006), this technique helps preserve the meaning of actors' views and actions within the code, making it easier to analyse while and after coding. Using this technique, we developed a set of codes that were arguments for and against the use of facial recognition on police body cameras. We also noted the actors

making these arguments. In the second cycle of coding, similar in-vivo codes were grouped together under a summative 'value' to discern patterns in the data. Taebi et al. (2014), in their study of public values in technology and innovation, cite Talbot (2011) to suggest that the term refers to the public view of what may be considered valuable or worth striving for.

AB-1215 as a Social Discourse

The coding, categorization and organisation of data revealed that the main arguments for and against the use of facial recognition in police body cameras in California could be filed under three themes: (1) privacy, surveillance and liberty; (2) public safety; and (3) discrimination as technological artefact. Interestingly, both the pro- and anti-FR factions were able to use the concepts underlying these three themes to their advantage in their arguments. These themes are discussed below.

Media discussions about the bill were dominated by civil society organisations (especially ACLU), and lawmakers (especially Assembly member Phil Ting, the author AB-1215), followed by representatives of police unions and organisations. To a much lesser extent, comments and statements from technology manufacturers such as Amazon, Axon and Microsoft were also featured in news coverage. Most media coverage was local, with city and county news organisations contributing the bulk of the articles in the corpus. A lot of the coverage was based almost entirely on press statements from Assembly member Ting, congressional and senate floor analyses and press statements from organisations with involvement in the political process such as ACLU, Electronic Frontier Foundation, Fight for the Future, or, from the other side, the Riverside Sheriffs' Association, the California Peace Officers' Association and the California Police Chiefs Association. As a result, arguments tended to repeat themselves across the dataset. But as our corpus was multi-pronged, this enabled us to understand what arguments were more likely to be picked up from legislative debates and outreach materials and become popularised in the media – and what arguments were not. In addition, we were able to track how the discourse changed over time.

Privacy, Surveillance and Liberty

Fears that arming police body cameras with FR systems would lead to mass surveillance and intrusions of privacy were prominent in statements from civil rights groups and lawmakers supporting AB-1215, especially in the weeks and months following the introduction of the bill. For instance, Ting, the assembly member who wrote the bill, said on 9 May, when the bill went to the Senate: 'Without my bill, face recognition technology can subject law-abiding citizens to perpetual police line-ups, as their every movement is

tracked without consent. Its use, if left unchecked, undermines public trust in government institutions and unduly intrudes on one's constitutional right to privacy' (Office of Assembly member Ting, 2019a). Similarly, ACLU representatives repeatedly brought up the 'invasive' nature of FR. Matt Cagle, an attorney for ACLU of Northern California, said, 'AB-1215 helps ensure Californians don't become test subjects for an invasive and dangerous tracking technology that undermines our most fundamental civil liberties and human rights' (ACLU 2019a).

The idea that FR would violate not some arbitrary notion of privacy but the constitutionally ordained rights of American citizens was important in these claims. The Fourth Amendment to the US Constitution protects citizens from unreasonable search and seizures. In effect, this allows citizens to be present in public without having to show any form of identification to authorities (Body Camera Accountability Act: Hearing 2019a). This protection would vanish with the widespread adoption and use of FR by law enforcement to scan civilians on the street. As described in the text of AB-1215, this is the 'functional equivalent of requiring every person to show a personal photo identification card at all times in violation of recognized constitutional rights'. (Body Camera Accountability Act: Hearing 2019a, 3).

In addition, critics warned of the technology's potential to 'chill' free speech in public spaces. The case of China was brought up as an example, such as in this news report:

> If there is one cautionary tale that surfaces in discussions of this technology, it is the case of China's policing through an array of cameras equipped with facial recognition software of the Uighurs, a largely Muslim minority in the western part of the country. (della Cava, 2019)

Pushback against these arguments was divided. Some proponents of FR in law enforcement, such as Ron Lawrence of the California Police Chiefs Association, asserted that privacy would be respected and technology won't be misused. 'Let me be clear, law enforcement respects and understands the importance of protecting a person's right to privacy', he said. 'We believe a person's privacy should not be violated unless that person is a threat to themselves or to others. We stand by this and will continue to do so in the future' (Lawrence 2019). But others, such as the Riverside Sheriffs' Association in its official opposing argument on the legislative floor, argued that citizens *did not* have a reasonable expectation of privacy in public. They also questioned why 'civil libertarians' were only concerned about privacy now and did not speak up for the privacy of law enforcement officers when an earlier law mandated the public disclosure of body camera video (Body Camera Accountability Act: Hearing 2019b).

The contradictory claims of FR proponents serve to justify the fears of FR's critics. Even if one takes the assurances of officers such as Lawrence at face value, there would be others in law enforcement who simply do not respect or

recognise people's privacy – nor the basic rights guaranteed to them in the law they are claiming to enforce.

Public Safety

The most common argument proffered by proponents of FR in policing was that it would improve public safety. To do so, they cited the 'success' of FR in other states and countries. Two frequently quoted examples included: the reported use of FR to capture the perpetrator of the *Capital Gazette* shooting in Maryland in 2018 (della Cava 2019); and a supposed 60% reduction in carjackings in Detroit after the installation of a citywide FR system (Lawrence 2019).

In addition, law enforcement groups such as the Riverside Sheriffs' Association frequently brought up California's plans to host mega events – including the annual Coachella Arts and Music Festival and the 2028 Summer Olympics – and the need to ensure public safety at these events. A ban on FR, they claimed, would signal the state's inability to protect participants and visitors and could potentially mean the events would move elsewhere. This argument, first made in official comments to the legislature in opposition of AB-1215 (Body Camera Accountability Act: Hearing 2019b, 10), was picked up and amplified by media coverage.

But critics of FR turned the argument on its head. They claimed that the technology would undermine rather than improve public safety – especially for minorities. If law enforcement officers were to police these communities while wearing FR-enhanced body cameras, members of the public would likely hesitate to interact with officers, even as victims or witnesses of crimes, for fear of having their faces caught on camera and stored in a database in perpetuity. This would make the job of law enforcement more difficult and also put these communities in greater danger (Body Camera Accountability Act 2019a). They also argued that public safety can be undermined by law enforcement officers suspecting or arresting innocent civilians.

Discrimination as Technological Artefact

Indeed, the disproportionately negative impact of FR on marginalised communities – minorities and immigrants – was a theme that surfaced in many different ways. Lawmakers and civil rights groups made this a key part of their argument against FR from the outset. In his 9 May statement when the bill went to the Senate, for instance, Ting noted that 'AB-1215 is an important civil rights measure that will prevent exploitation of vulnerable communities' (Office of Assembly member Ting 2019a).

Albert Fox Cahn, who founded The Surveillance Technology Oversight Project at the New York-based Urban Justice Center, wrote in a commentary,

'There's something unbearable about thinking that our country's largest investment ever in police accountability' – referring to body cameras – 'would be turned into a weapon against the very communities of colour that it was supposed to protect' (Cahn, 2019). Similarly, the Electronic Frontier Foundation noted that FR 'exacerbates historical biases born of, and contributing to, overpolicing in Black and Latinx neighbourhoods' (EFF 2019).

Curiously, a few months into the bill's passage, there was an important shift in this argument. Social discrimination moved from being a consequence of 'historical biases' to being a function of the inaccuracy of the FR technology itself. The shift was especially evident after Rekognition failed the ACLU's test on 13 August 2019, during which it misidentified 26 California lawmakers as criminals – many of them, including Ting, being people of colour. This technological failure quickly became central to Ting's statements against FR and justification for AB-1215. As he said after the experiment: 'This experiment reinforces the fact that facial recognition software is not ready for prime time – let alone for use in body cameras worn by law enforcement' (ACLU Northern California 2019).

To be sure, FR's inaccuracy when it came to identifying people of colour, had been known for long. ACLU had run a similar test a year earlier, with similar results. However, as the new experiment, and Ting's mobilisation of its results to back his push for the bill, began to dominate the news, the discourse about social discrimination shifted subtly yet recognisably. Journalists increasingly began to associate FR's potential for exacerbating marginalisation to what Ting called its 'dangerous inaccuracies' as a technological artefact (Office of Assembly member Ting 2019b).

Ironically, scientific support for the arguments of FR's detractors soon became the bill's undoing – at least in terms of what it was initially intended to be. Amazon disputed the findings of the experiment, claiming the researchers purposefully used a lower confidence threshold than recommended (they used the default settings in the Rekognition software) (Gardiner 2019a). The Information Technology and Innovation Foundation argued FR was, in fact, more accurate than human recognition and so was an improvement to existing techniques in terms of accuracy (Information Technology and Innovation Foundation 2019). Even those who acknowledged that the ACLU experiment revealed a significant problem added that the problem, being technological, could – and eventually would – be resolved. Both Axon, one of the largest manufacturers of body cameras in the US, and Microsoft, which has its own FR software, agreed that FR had an accuracy and fairness problem – in its *current* state. As an Axon report said, 'At the least, face recognition technology should not be deployed until the technology performs with far greater accuracy and performs equally well across races, ethnicities, genders and other identity groups' (Sumagaysay 2019). The idea that the main problem with FR was a technological flaw that needed to be and *could be* fixed given time became dominant.

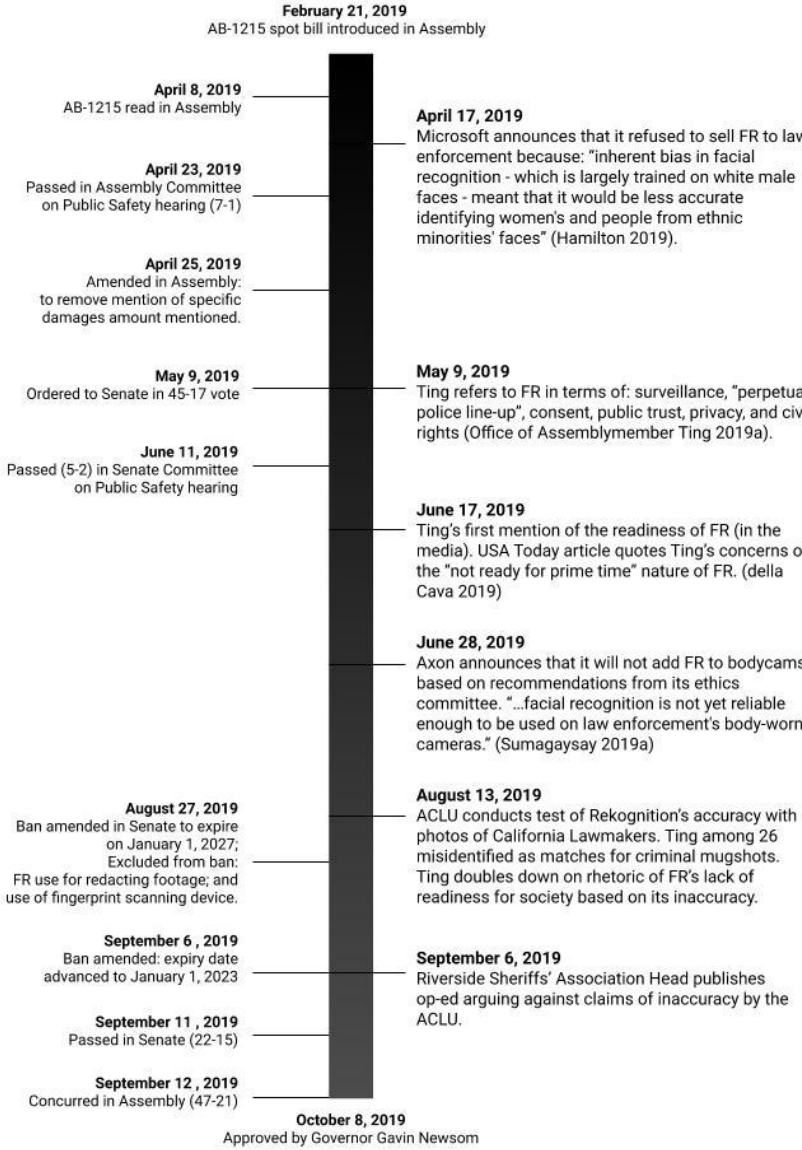

Figure 13.1: A Brief History of AB-1215.

This discursive shift came as a shot in the arm for FR proponents on the assembly floor, such as the Riverside Sheriffs' Association. They had already been arguing that, as a world leader in technology development, California was not the kind of state that would ban a technology simply because it wasn't perfect. 'Could any of us imagine a statutory ban on Microsoft Office or Apple's

iOS until the software was able to be certified as 100% flawless?' they had asked in their official comments to the legislature in June (Body Camera Accountability Act: Hearing 2019b, 10).

Two weeks after the 13 August experiment, the bill was amended to include a sunset clause (see Figure 13.1). The indefinite ban on FR was now set to expire after seven years. On 6 September, the expiry was further reduced to three years. Days after these amendments, the bill was passed in both houses – and signed by Governor Newsom a month later.

Conclusion: Why Biopolitics Matters

Our study has examined AB-1215 as a social discourse, adopting a *law and society* approach that views legislations as socially negotiated and focuses, among other things, on the 'construction of meanings' of the law and how it influences the legal/regulatory process (Ewick and Silbey 1998). Our analysis leads us to two broad conclusions to guide future social research and social action vis-à-vis FR and algorithmic governance in general. Firstly, the discourse comprised both 'particular' and 'universal' features – arguments and claims that were rooted in the political and cultural contexts in which they were made but also drew on ideas and concepts that transcended those contexts. For instance, the concern with FR systems infringing upon citizens' privacy is universal, but in this discourse, this concern was hybridised with guarantees of personal freedom that were specific to the US constitution. Meanwhile, FR's proponents, while echoing universalist claims about enhancing public safety with the aid of technology, also mobilised California's identity as a forward-looking and technology-friendly state – home to the Silicon Valley – to delegitimise calls for banning FR from law enforcement. A *hybrid* analytical lens that is sensitive to both universal and particular characteristics of FR as a social discourse is therefore vital for producing a nuanced picture.

Secondly, while FR's negative externalities – or the harms to 'third parties' it can cause (Petit 2017) – were initially perceived as *systemic*, they later came to be constructed in more *discrete* terms, albeit with certain systemic elements. Specifically, social discrimination – which FR was expected to reinforce – was discussed in terms of 'historical biases' at first but eventually became a function of machine learning-related inaccuracies of the technology itself. Crucially, this shift also implied that the harms it caused would be individualised and random, rather than affecting large sections of the populace in a predictable manner. The extent of the harm was still deemed unsustainable – wrongly identified individuals could end up being in prison or worse – and thus regulation was still warranted. But because the shortcoming was now perceived as technological, the need for regulation was supposed to be temporary: technology would, after all, improve – as technology is always expected to – and inaccuracies would reduce and eventually go away.

In theoretical terms, we witnessed the discourse transforming from *biopolitical* to technological determinist – foregrounding technology as the cause underlying social phenomena, good or bad, and de-emphasising concerns about institutionalised racism and mass surveillance (see also, Gangadharan and Niklas 2019). Ironically, this shift was precipitated by a well-intentioned scientific experiment carried out by a civil rights group. It is possible the ACLU experiment helped the bill get past the assembly floor by making the harms FR can cause appear more concrete and measurable. However, it simultaneously reduced the concerns with FR to the level of the technology itself – an example of what Selbst et al. (2019) have called a failure of abstraction. The social discourse lost its biopolitical magnitude – and so did the bill.

Shahin (2019) has drawn attention to the theoretical significance of 'critical junctures' – emergent conditions in which a social discourse takes on a new direction without the principal stakeholders intending it to – in shaping regulations about technology. The ACLU experiment in August 2019 was such a critical juncture in the discourse about AB-1215. Even though ACLU's own position on why FR had no place in law enforcement did not shift after the experiment – its press releases, for instance, retained their focus on systemic issues – both Assembly member Ting and the media latched on to Rekognition's manifest failure as a piece of technology. This quickly undermined the original intent of the bill. To be sure, other factors may have also played a role in the willingness shown by Ting and other supporters of the bill to accept a sunset clause – twice – and change the character of the bill from a permanent ban on the use of FR in police body cameras to a three-year moratorium. But the noticeable change in the social discourse following the experiment, coinciding with changes in the bill itself, does indicate that the experiment weakened the bill even as it became instrumental for its passage.

Our analysis is significant not only for future research on FR but also for future efforts to check algorithmic governance, legislative or otherwise, in the US and around the world. Firstly, it underlines the significance of a biopolitical approach to understanding – and resisting – algorithmic governance. That does not mean technological flaws are not important to point out. But those flaws are themselves the consequence rather than the cause of institutionalised racism: they don't produce but serve to *re*-produce discrimination and marginalisation.

Research and resistance therefore need to press forward with an agenda in which FR and other forms of artificial intelligence are viewed as sociotechnical artefacts interpellated in relations of power – produced by them even as they serve to reproduce those relations. Moreover, a technologically determinist outlook, where activists focus only on the machine, its algorithms, input and output, and not as much on the social contexts of its design and use, is not only a failure of abstraction (Selbst et al. 2019) – it is also a failure of strategy. Blaming the technology alone might appear attractive in the short-term but, as our analysis indicates, it does not aid the long-term goal of regulating algorithmic governance as a means of achieving social justice.

Secondly, these relations of power increasingly have both universal and particular – or global and local – dimensions. Being sensitive to such hybridity is important for research on and resistance to algorithmic governance in countries like the US, as our analysis indicates, but even more so in the Global South. That is partly because sociotechnical artefacts such as FR are constructed in North America and Western Europe, along with certain norms and practices of governance, and are often then 'localized' (Zaugg 2019) in the Global South amidst different forms of social hierarchy.

Understanding these hybridised dynamics opens new avenues for research and resistance aimed at exposing and destabilising such hierarchies. For instance, how are algorithms trained to discriminate against people of colour implicated in the biopolitics of societies where the entire population is 'of colour'? If algorithms for governance are coded and trained from scratch rather than copied and pasted, what kinds of power and norms of control do they reflect and reproduce? Comparative research across countries, and empirical research focusing on specific countries and contexts of design and use of these technologies are important. As new legal instruments are developed to regulate this technology, collaborations between legal scholars and scholars of social science are key in understanding how we can negotiate these technologies as a society.

In conclusion, we emphasise the main argument of our study. Scholars and activists have long been aware of the role of algorithms and artificial intelligence in marginalising minorities and immigrants and reinforcing relations of power (boyd and Crawford 2012; Eubanks 2018). Biometric technologies, such as FR, are particularly insidious examples as they can act at the level of both the 'body' and the 'body politic'. They reduce human beings into data points that may be stored, manipulated and controlled en masse (Browne 2010; Hood 2020). At the same time, they enable forms of domination that are *systemic* in nature: they have a long history and they are institutionalised in a variety of social practices. Indeed, algorithms themselves represent one such social practice. The prejudices they exhibit are a consequence of the systemic bias they are produced by – even as the algorithms help re-enact and reproduce that bias. Research on and resistance to algorithmic governance should, therefore, avoid the trap of technological determinism and not lose sight of the systemic nature of their subject matter – the biopolitics of discrimination and domination.

References

ACLU. 2019a. California Senate Votes to Block Face Recognition on Police Body Cameras [PRESS RELEASE], 11 September 2019. https://www.aclunc.org/news/california-senate-votes-block-face-recognition-police-body-cameras.

ACLU. 2019b. California Governor Signs Landmark Bill Halting Facial Recognition on Police Body Cams [PRESS RELEASE], 8 October 2019. https://

www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams.

ACLU Northern California. 2019. Facial Recognition Technology Falsely Identifies 26 California Legislators with Mugshots [PRESS RELEASE], 13 August 2019. https://www.aclunc.org/news/facial-recognition-technology-falsely-identifies-26-california-legislators-mugshots.

Anderson, B. 2019. California Considers Plan to Ban Facial Recognition Technology. *The Fresno Bee*. 16 May 2019. https://www.fresnobee.com/news/california/article230437789.html.

Andrejevic, M. 2019. Automating Surveillance. *Surveillance & Society* 17 (1/2): 7–13.

Barbrook, R. and Cameron, A. 1996. The Californian Ideology. *Science as Culture* 6 (1): 44–72. DOI: https://doi.org/10.1080/09505439609526455.

Barik, S. 2020. Microsoft Will Not Sell Facial Recognition Tech to Police in the US without Federal Law. *Medianama*, 12 June 2020. https://www.medianama.com/2020/06/223-microsoft-facial-recognition

Bedoya, A.M. 2019. The Color of Surveillance. *Slate*. 18 January. https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html.

Benjamin, R. 2016. Catching Our Breath: Critical Race STS and the Carceral Imagination. *Engaging Science, Technology, and Society* 2: 145–156.

Body Camera Accountability Act, A.B. 1215. 2019a. Amended in Assembly. 8 April 2019.

Body Camera Accountability Act, A.B. 1215. 2019b. Amended in Assembly. 25 April 2019.

Body Camera Accountability Act, A.B. 1215. 2019c. Amended in Senate. 27 August 2019.

Body Camera Accountability Act, A.B. 1215. 2019d. Amended in Senate. 6 September 2019.

Body Camera Accountability Act, A.B. 1215. 2019e. Enrolled, 8 October 2019.

Body Camera Accountability Act: Hearing on A.B. 1215 Before the Sen. Comm. on Public Safety. 2019a. (statement of the American Civil Liberties Union). http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB1215

Body Camera Accountability Act: Hearing on A.B. 1215 Before the Sen. Comm. on Public Safety. 2019b. (statement of the Riverside Sherriffs Association). http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB1215

boyd, d. and Crawford, K. 2012. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. *Information, Communication & Society* 15 (5): 662–679.

Browne, S. 2010. Digital Epidermalization: Race, Identity and Biometrics. *Critical Sociology* 36 (1): 131–150.

Buolamwini, J. and Gebru, T. 2018. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: *Conference on Fairness, Accountability and Transparency*, 77–91.

Cagle, M. 2020. California Just Blocked Police Body Cam Use of Face Recognition. *ACLU Free Future* (blog). 11 October 2020. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/california-just-blocked-police-body-cam-use-face.

Cahn, A.F. 2019. Facial Recognition Tech Is a Blatant Misuse of Police Bodycams. *The Daily Beast*. 17 October 2019. https://www.thedailybeast.com/facial-recognition-tech-is-a-blatant-misuse-of-police-bodycams.

Cameron, D. 2020. Detroit Police Chief Admits Face Recognition Doesn't Work '95–97% of the Time'. *Gizmodo*, 29 June 2020. https://gizmodo.com/detroit-police-chief-admits-face-recognition-doesnt-wor-1844209113.

Chabria, A. 2019. Facial Recognition Software Mistook 1 in 5 California Lawmakers for Criminals, Says ACLU. *Los Angeles Times*, 13 August 2019. https://www.latimes.com/california/story/2019-08-12/facial-recognition-software-mistook-1-in-5-california-lawmakers-for-criminals-says-aclu.

Chappell, B. 2019. ICE Uses Facial Recognition to Sift State Driver's License Records, Researchers Say. *NPR*, 8 July 2019. https://www.npr.org/2019/07/08/739491857/ice-uses-facial-recognition-to-sift-state-drivers-license-records-researchers-sa.

Charmaz, K. 2006. *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. Thousand Oaks, CA: Sage.

Cohen, J.E. 2012. What Privacy Is For. *Harv. L. Rev*. 126: 1904.

Colaner, S. 2020. Detroit's Fight over Policing and Facial Recognition Is a Microcosm of the Nation. *VentureBeat*, 25 June 2020. https://venturebeat.com/2020/06/25/detroits-fight-over-policing-and-facial-recognition-is-a-microcosm-of-the-nation

della Cava, M. 2019. Face-Recognition Technology Has Heads Spinning in Calif. *USA Today*, 17 June 2019. https://www.pressreader.com/usa/usa-today-us-edition/20190617/281500752769807

Demush, R. 2019. A Brief History of Computer Vision (and Convolutional Neural Networks). *HackerNoon*, 26 February 2019. https://hackernoon.com/a-brief-history-of-computer-vision-and-convolutional-neural-networks-8fe8aacc79f3.

Devereaux, R. 2019. Secret Terrorism Watchlist Found Unconstitutional in Historic Decision. *The Intercept*, 6 September 2019. https://theintercept.com/2019/09/06/terrorism-watchlist-lawsuit-ruling

EFF. 2019. Hearing Tuesday: EFF Will Voice Support for California Bill Reining in Law Enforcement Use of Facial Recognition [PRESS RELEASE], 10 June 2019. https://www.eff.org/press/releases/hearing-tuesday-eff-will-voice-support-california-bill-reining-law-enforcement-use.

Eubanks, V. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.

Ewick, P. and Silbey, S.S. 1998. *The Common Place of Law: Stories from Everyday Life*. Chicago, IL: University of Chicago Press.

Ferretti, C. 2020. Residents Urge City Council to Reject Proposed Facial Recognition Contract Extension. *The Detroit News*, 16 June 2020. https://www.detroitnews.com/story/news/local/detroit-city/2020/06/16/residents-urge-city-council-reject-proposed-facial-recognition-contract/3197917001/.

Foucault, M. 2003. *Society Must Be Defended: Lectures at the Collège de France 1975–1976*, trans. David Macey. New York: Picador, 242.

Gandy Jr, O.H. 1993. *The Panoptic Sort: A Political Economy of Personal Information.* Critical Studies in Communication and in the Cultural Industries. Boulder, CO: Westview Press/ERIC.

Gangadharan, S.P. and Niklas, J. 2019. Decentering Technology in Discourse on Discrimination. *Information, Communication & Society* 22 (7): 882–899.

Gardiner, D. 2019a. Facial ID Misses Mark, Test by ACLU Reveals. *San Francisco Chronicle*, 13 August 2019. https://www.sfchronicle.com/politics/article/Facial-recognition-misidentified-26-California-14301190.php.

Gardiner, D. 2019b. Lawmakers OK Ban on Police Use of Facial Recognition. *San Francisco Chronicle*, 13 September 2019. https://www.sfchronicle.com/politics/article/California-lawmakers-vote-for-3-year-ban-on-14436245.php.

Gardiner, D. 2019c. California Blocks Police from Using Facial Recognition in Body Cameras. *San Francisco Chronicle*, 7 October 2019. https://www.sfchronicle.com/politics/article/California-blocks-police-from-using-facial-14502547.php.

Garvie, C., Bedoya, A. and Frankle, J. 2016. The Perpetual Line-Up. Unregulated Police Face Recognition in America. Georgetown Law Center on Privacy & Technology, October. https://www.perpetuallineup.org.

Gates, K.A. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. Vol. 2. New York: New York University Press.

Goldstein, A.J., Harmon, L.D. and Lesk, A.B. 1971. Identification of Human Faces. *Proceedings of the IEEE* 59 (5): 748–760. DOI: https://doi.org/10.1109/PROC.1971.8254.

Gomez, J. and Rosenberg, L. 2019. In the Hands of Police, Facial Recognition Software Risks Violating Civil Liberties. *USA Today*, 18 October 2019. https://www.usatoday.com/story/opinion/policing/2019/10/18/hands-police-facial-recognition-tech-violates-civil-liberties/3904469002

Greenwald, G., MacAskill, E. and Poitras, L. 2013. Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations. *The Guardian*, 11 June 2013. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Guariglia, M. 2019. Victory! California Governor Signs A.B. 1215. *Electronic Frontier Foundation* (blog). 9 October 2019. https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215.

Hamilton, I.A. 2019. Microsoft Took an Ethical Stand on Facial Recognition Just Days after Being Blasted for a Sinister AI Project in China. *Business Insider*, 17 April 2019. https://www.businessinsider.in/tech/microsoft-took-an-ethical-stand-on-facial-recognition-just-days-after-being-blasted-for-a-sinister-ai-project-in-china/articleshow/68922085.cms.

Hill, K. 2020. The Secretive Company That Might End Privacy as We Know It. *New York Times*, 18 January 2020. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hood, J. 2020. Making the Body Electric: The Politics of Body-Worn Cameras and Facial Recognition in the United States. *Surveillance & Society* 18 (2): 157–169.

Huang, G.B., Mattar, M., Berg, T. and Learned-Miller, E. 2008. Labeled Faces in the Wild: A Database Forstudying Face Recognition in Unconstrained Environments. In:*Workshop on Faces in 'Real-Life' Images: Detect ion, Alignment, and Recognition*. https://hal.inria.fr/inria-00321923/file/Huang_long_eccv2008-lfw.pdf.

Information Technology and Innovation Foundation. 2019. Information Technology & Innovation Foundation Issues Statement on Facial Recognition Technology for Law Enforcement [PRESS RELEASE], 11 September 2019.

Kak, A. 2020. *Regulating Biometrics: Global Approaches and Urgent Questions*. AI Now. https://ainowinstitute.org/regulatingbiometrics.pdf.

Lawrence, R. 2019. Commentary: Why Law Enforcement Should Use Facial Recognition. *San Diego Union-Tribune*, 6 September 2019. https://www.sandiegouniontribune.com/opinion/story/2019-09-06/commentary-why-law-enforcement-should-use-facial-recognition.

Mann, M. and Smith, M. 2017. Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *UNSWLJ* 40: 121.

Mayring, P. 2004. Qualitative Content Analysis. *A Companion to Qualitative Research* 1 (2004): 159–176.

Metz, R. 2019. Beyond San Francisco, More Cities Are Saying No to Facial Recognition. *CNN Wire*, 17 July 2019. https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

Morozov, E. 2012. *The Net Delusion: The Dark Side of Internet Freedom*. New York: Public Affairs.

Naughton, J. 2020. Quick, Cheap to Make and Loved by Police – Facial Recognition Apps Are on the Rise. *The Guardian*, 25 January 2020. https://www.theguardian.com/technology/commentisfree/2020/jan/25/facial-recognition-apps-are-on-the-rise.

Ng, A. 2020a. Microsoft Pushed Its Facial Recognition to Federal Agencies, Emails Show. *CNET*, 17 June 2020. https://www.cnet.com/news/microsoft-pushed-its-facial-recognition-to-federal-agencies-emails-show/.

Ng, A. 2020b. Lawmakers Propose Indefinite Nationwide Ban on Police Use of Facial Recognition. *CNET*, 25 June 2020. https://www.cnet.com/news/lawmakers-propose-indefinite-nationwide-ban-on-police-use-of-facial-recognition

NPR. 2020. Tech Companies Are Limiting Police Use of Facial Recognition. Here's Why. *Short Wave*, 23 June 2020. https://www.npr.org/2020/06/22/881845711/tech-companies-are-limiting-police-use-of-facial-recognition-heres-why.

Office of Assembly member Ting. 2019a. Ting Proposal Banning Facial Recognition Technology in Body Cams Approved by State Assembly [PRESS RELEASE], 9 May 2019. https://a19.asmdc.org/press-releases/20190509-ting-proposal-banning-facial-recognition-technology-body-cams-approved-state

Office of Assembly member Ting. 2019b. Facial Recognition Technology Falsely Identifies 26 California Legislators, Including Ting, with Mugshots [PRESS RELEASE], 13 August 2019. https://a19.asmdc.org/press-releases/20190813-facial-recognition-technology-falsely-identifies-26-california-legislators.

Oliver, D. 2019. Facial Recognition Scanners Are Already at Some US Airports. Here's What to Know. *USA Today*, 16 August 2019. https://www.usatoday.com/story/travel/airline-news/2019/08/16/biometric-airport-screening-facial-recognition-everything-you-need-know/1998749001/.

Pato, J.N. and Millett, L.I. 2010. National Research Council (US) Whither Biometrics Committee. In: *Biometric Recognition: Challenges and Opportunities*. National Academies Press (US).

Petit, N. 2017. Law and Regulation of Artificial Intelligence and Robots-Conceptual Framework and Normative Implications SSRN, 9 March. DOI: http://dx.doi.org/10.2139/ssrn.2931339

Pope, C. 2018. Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data. *JL & Pol'y* 26: 769.

Saldaña, J. 2009. *The Coding Manual for Qualitative Researchers*. New York: Sage.

Selbst, A.D., boyd, d., Friedler, S.A, Venkatasubramanian, S. and Vertesi, J. 2019. Fairness and Abstraction in Sociotechnical Systems. In: *Proceedings of the Conference on Fairness, Accountability, and Transparency*, pp. 59–68. New York: ACM.

Seron, C. and Silbey, S. 2004. Profession, Science, and Culture: An Emergent Canon of Law and Society Research. In Sarat, A (Ed.)*The Blackwell Companion to Law and Society,* pp. 30–59. Oxford: Blackwell Publishers

Shahin, S. 2019. Facing up to Facebook: How Digital Activism, Independent Regulation, and Mass Media Foiled a Neoliberal Threat to Net Neutrality. *Information, Communication & Society* 22 (1): 1–17.

Shwayder, M. 2020. Police Facial Recognition Tech Could Misidentify People at Protests, Experts Say. *Digital Trends*, 2 June 2020. https://www.digitaltrends.com/news/police-protests-facial-recognition-misidentification

Simonite, T. 2019. The Best Algorithms Struggle to Recognize Black Faces Equally. *Wired*, 22 August 2019. https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally

Snow, J. 2018. Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots. *ACLU* (blog). 26 July 2018. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

Sumagaysay, L. 2019. No More Facial Recognition in Cop Body Cams – Axon Announces New Policy as Concern Grows over Reliability. *The Mercury News*, 28 June 2019. https://www.mercurynews.com/2019/06/27/no-facial-recognition-in-police-body-cams-their-biggest-maker-vows

Taddonio, P. 2019. How China's Government Is Using AI on Its Uighur Muslim Population. *Frontline PBS*, 21 November 2019. https://www.pbs.org/wgbh/frontline/article/how-chinas-government-is-using-ai-on-its-uighur-muslim-population

Taebi, B., Correlje, A., Cuppen, E., Dignum, M. and Pesch, U. 2014. Responsible Innovation as an Endorsement of Public Values: The Need for Interdisciplinary Research. *Journal of Responsible Innovation* 1 (1): 118–124.

Talbot, C. 2011. Paradoxes and Prospects of 'Public Value'. *Public Money & Management* 31 (1): 27–34.

Thebault, R. 2019. California Could Become the Largest State to Ban Facial Recognition in Body Cameras. *The Washington Post*, 12 September 2019. https://www.washingtonpost.com/technology/2019/09/12/california-could-become-largest-state-ban-facial-recognition-body-cameras

van der Ploeg, I. 2002. Biometrics and the Body as Information: Normative Issues of the Socio-Technical Coding of the Body. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, pp. 57–73. London: Routledge.

Zaugg, J. 2019. India is Trying to Build the World's Biggest Facial Recognition System. *CNN*. 18 October 2019. https://www.cnn.com/2019/10/17/tech/india-facial-recognition-intl-hnk/index.html