7

Power and Protest

Facial Recognition and Public Space Surveillance

Monika Zalnieriute

Political freedom, generally speaking, means the right to be a participator in government, or it means nothing.[1]

7.1 INTRODUCTION

In 2018, police in India reported that the roll out of facial recognition technology (FRT) across New Delhi enabled their identification of 3,000 missing children in just four days.[2] In the United Kingdom, South Wales Police used live FRT to scan over 50,000 faces at various mass gatherings between January and August 2019 and identified nine individuals for arrest.[3] The Chinese Sharp Eyes programme, 'omnipresent, fully networked, always working and fully controllable', can take less than seven minutes to identify and facilitate apprehension of an individual among a population of nearly 5 million people.[4] In Moscow, 105,000 FRT-enabled cameras have

Research for this chapter has been funded by the Research Council of Lithuania (LMTLT) (Government Use of Facial Recognition Technologies: Legal Challenges and Solutions (FaceAI), agreement number S-MIP-21-38); and Australian Research Council Discovery Early Career Research Award (Artificial Intelligence Decision-Making, Privacy and Discrimination Laws, project number DE210101183). The chapter draws on and adapts some arguments developed in M. Zalnieriute, 'Facial Recognition Surveillance and Public Space: Protecting Protest Movements', *International Review of Law, Computers & Technology*, 2024 (forthcoming).

[1] Hannah Arendt, *On Revolution* (Penguin, 1977), p. 218.

[2] PTI, 'Delhi: Facial recognition system helps trace 3,000 missing children in 4 days' (22 April 2018), *Times of India*, https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms.

[3] AFR South Wales, 'Deployments for Live Facial Recognition' (n.d.), www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/deployments-for-live-facial-recognition/.

[4] Ryan Grenoble, 'Welcome to the surveillance state: China's AI cameras see all' (12 December 2017), *HuffPost Australia*, www.huffpost.com/entry/china-surveillance-camera-big-brother_n_5a2ff4dfe4b01598ac484acc.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

monitored and enforced COVID-19 self-isolation orders,[5] with at least 200 violators being identified.[6]

As protest movements are gaining momentum across the world, with Extinction Rebellion, Black Lives Matter, and strong pro-democracy protests in Chile and Hong Kong taking centre stage, many governments – both in the West and in the East – have significantly increased surveillance capacity of the public sphere. City streets and squares, stations, and airports across the globe, and social media and online platforms have become equipped with sophisticated surveillance tools, enabled and made legal through a myriad of complex and ever-expanding 'emergency' laws. Irrespective of whether these events and/or political strategies are framed as 'emergencies' such as the 'war on terror' with its invisible geopolitical enemies for 9/11, or whether they were pro-democracy or anti-racism protests or connected with COVID-19, the state resort to technology and increased surveillance as a tool to control the masses and population has been similar. Examples from varied countries – ranging from China, Russia, and India to the United States and the United Kingdom – tell us that recent technological advances have enabled authoritarian and democratic governments alike to build omnipresent biometric infrastructures that systematically monitor, surveil, predict, and regulate the behaviour of individual citizens, groups, or even entire populations.

In this chapter, I focus on the chilling effect of FRT use in public spaces on the right to peaceful assembly and political protest. While technological tools have transformed protest movements widely, both amplifying and undermining them,[7] in this chapter I only focus how protest movements have been tackled with FRT and my emphasis is on *political protests* and *public spaces*. Pointing to the absence of oversight and accountability mechanisms on government use of FRT, the chapter demonstrates how FRT has significantly strengthened state power. It draws attention to the crucial role of tech companies in assisting governments in public space surveillance and curtailing protests. I argue for hard human rights obligations

[5] Patrick Reevell, 'How Russia is using facial recognition to police its coronavirus lockdown' (30 April 2020), *ABC News*, https://abcnews.go.com/International/russia-facial-recognition-police-coronavirus-lockdown/story?id=70299736; Sarah Rainsford, 'Russia uses facial recognition to tackle virus' (4 April 2020), *BBC News*, www.bbc.com/news/av/world-europe-52157131/coronavirus-russia-uses-facial-recognition-to-tackle-covid-19. One man, having been given a self-quarantine order, was visited by police within half an hour of leaving his home to take out the rubbish.

[6] NtechLab, 'Biometric Solution against COVID-19' (n.d.), https://ntechlab.com/en_au/solution/biometric-solution-against-covid-19/.

[7] V. Barassi, *Activism on the Web: Everyday Struggles against Digital Capitalism* (Routledge, 2015); J. Juris, 'Reflections on #occupy everywhere: Social media, public space, and emerging logics of aggregation' (2012) 39(2) *American Ethnologist* 259–279; P. Gerbaudo, *Tweets and the Streets: Social Media and Contemporary Activism* (Pluto Press, 2012); P. Gerbaudo, *The Mask and the Flag: Populism, Citizenism, and Global Protest* (Oxford University Press, 2017); Alice Mattoni, *Media Practices and Protest Politics How Precarious Workers Mobilise* (Ashgate, 2012); Lucas Melgaco and Jeffrey Monoghan, 'Introduction: Taking to the streets in the information age' in Lucas Melgaco and Jeffrey Monoghan (eds.), *Protests in the Information Age* (Routledge, 2018), pp. 1–17; D. Trottier and Christian Fuchs (eds.), *Social Media, Politics and the State* (Routledge, 2015).

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

to bind these companies and governments, to ensure that political movements and protests can flourish in the post-COVID-19 world.

7.2 UNDERMINING PROTEST MOVEMENTS WITH FRTS

Live automated FRT, rolled out in public spaces and cities across the world, is transforming modern policing in liberal democracies and authoritarian regimes alike. The technology augments traditional surveillance methods by detecting and comparing a person's eyes, nose, mouth, skin textures, and shadows to identify individuals.[8] The live automated facial recognition can instantaneously assess the facial biometric data in the captured images against a pre-existing 'watchlist' and flag it to police officers. Some FRT tools go further, purporting to classify people by gender or race or make predictions about their sexual orientation, emotions, and intent.

This FRT has been used to tackle protest movements globally. For example, the US company Geofeedia has been marketed to law enforcement 'as a tool to monitor activists and protestors',[9] incorporating FRT use with Twitter, Facebook, and Instagram databases.[10] Rasheed Shabazz, an activist and journalist, believes that his arrest near the Black Lives Matter protests in Oakland in 2014 was as a result of the Geofeedia software.[11] This same software was also used to monitor civil unrest after the police killing of Freddie Grey and link protesters with their social media profiles.[12] Similarly, in 2020, during the protests following the killing of George Floyd in Minneapolis, Minnesota, several people were arrested and charged after being

[8] Andrew Guthrie Ferguson, 'Facial recognition and the Fourth Amendment' (2021) 105 *Minnesota Law Review* 1105–1106; Jagdish Chandra Joshi and K. K. Gupta, 'Face recognition technology: A review' (2016) 1 *The IUP Journal of Telecommunication* 53–54, at 53; Relly Victoria Virgil Petrescu, 'Face recognition as a biometric application' (2019) 3 *Journal of Mechatronics and Robotics* 240; Mary Grace Galterio, Simi Angelic Shavit, and Thaier Hayajneh, 'A review of facial biometrics security for smart devices' (2018) 7 (37) *Computers* 3; Ian Berle, *Face Recognition Technology: Compulsory Visibility and Its Impact on Privacy and the Confidentiality of Personal Identifiable Images* (Springer, 2020), p. 1

[9] ACLU of Northern CA, 'Police use of social media surveillance software is escalating, and activists are in the digital crosshairs' (22 September 2016), *Medium*, https://medium.com/@ACLU_NorCal/police-use-of-social-media-surveillance-software-is-escalating-and-activists-are-in-the-digital-d29d8f89c48.

[10] Matt Cagle, 'Facebook, Instagram, and Twitter provided data access for a surveillance product marketed to target activists of color' (11 October 2016), ACLU of Northern California, www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target; Russell Brandom, 'Facebook, Twitter, and Instagram surveillance tool was used to arrest Baltimore protestors' (11 October 2016), *The Verge*, www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api; Kalev Leetaru, 'Geofeedia is just the tip of the iceberg: The era of social surveillance' (12 October 2016), *Forbes*, www.forbes.com/sites/kalevleetaru/2016/10/12/geofeedia-is-just-the-tip-of-the-iceberg-the-era-of-social-surveillence/.

[11] Ali Winston, 'Oakland cops quietly acquired social media surveillance tool' (13 April 2016), *East Bay Express*, www.eastbayexpress.com/oakland/oakland-cops-quietly-acquired-social-media-surveillance-tool/Content?oid=4747526.

[12] Shira Ovide, 'A case for banning facial recognition' (9 June 2020), *New York Times*, www.nytimes.com/2020/06/09/technology/facial-recognition-software.html.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

identified through the use of FRT.[13] In another case, the Detroit Police Department used FRT to identify a Black Lives Matter protester who was arrested and charged with reckless driving and resisting arrest.

Similarly, FRT has been used in many other countries. For example, 'habitual protesters' in India are included in a dataset used to monitor large crowds,[14] which is composed of 'miscreants who could raise slogans and banners'.[15] This database was used to identify dissidents at a prime ministerial rally in December 2019,[16] and also resulted in the detention of a 'handful' of individuals charged with violent crimes when it surveyed protests in New Delhi and Uttar Pradesh.[17] The Hong Kong police used FRT cameras to identify protesters and track their movements during the 2019 pro-democracy protests, which drew criticism from human rights advocates who argued that it violated the protesters' right to privacy and could lead to their persecution.[18] In 2019–2020, FRT cameras were also used in Chile to monitor and identify protesters participating in demonstrations and civil unrest, known as the *Estallido Social*.[19] The cameras were installed in public areas, including train stations and street corners, by the Chilean government to track individuals who were suspected of participating in protests or other forms of civil disobedience. In the face of mounting criticism and protests against the use of this technology, the Chilean government announced that it would suspend the use of facial recognition cameras in public spaces in early 2020.

In all these cases, FRT allowed the authorities to quickly identify individuals who were wanted for questioning or arrest. The cameras were linked to a central database containing photos and personal information of individuals who were known to have participated in previous protests or other activities that the government deemed to be illegal. Such use of FRT cameras sparked controversy and concern among civil liberties groups and privacy advocates, who argued that the technology was being used to stifle dissent and violate the rights of protesters to peacefully assemble and express their opinions. Despite these concerns, governments typically defend FRT use by framing it as a necessary measure to maintain 'public safety' and order during a time of civil unrest.

[13] Tate Ryan-Mosley and Sam Richards, 'The secret police: Cops built a shadowy surveillance machine in Minnesota after George Floyd's murder' (3 March 2020), *MIT Technology Review*, www.technologyreview.com/2022/03/03/1046676/police-surveillance-minnesota-george-floyd/.

[14] Jay Mazoomdaar, 'Delhi police film protests, run its images through face recognition software to screen crowd' (28 December 2019), *Indian Express*, https://indianexpress.com/article/india/police-film-protests-run-its-images-through-face-recognition-software-to-screen-crowd-6188246/.

[15] Vidushi Marda, 'View: From protests to chai, facial recognition is creeping up on us' (7 January 2020), *Carnegie India*, https://carnegieindia.org/2020/01/07/view-from-protests-to-chai-facial-recognition-is-creeping-up-on-us-pub-80708.

[16] Mazoomdaar, 'Delhi police film protests'.

[17] Alexandra Ulmer and Zeba Siddiqui, 'Controversy over India's use of facial recognition technology' (17 February 2020), *Sydney Morning Herald*, www.smh.com.au/world/asia/controversy-over-india-s-use-of-facial-recognition-during-protests-20200217-p541pp.html.

[18] Richard Byrne and Michael C. Davis, 'Protest tech: Hong Kong' (2020), *Wilson Quarterly*, http://wq.proof.press/quarterly/the-power-of-protest/protest-tech-hong-kong/.

[19] Michelle Corinne Liu, Jaime R. Brenes Reyes, Sananda Sahoo, and Nick Dyer-Witheford, 'Riot platforms: Protest, police, planet' (2022) 54(6) *Antipode* 1901.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

In addition to such 'top-down' surveillance by public authorities in USA, India, Hong Kong, and Chile, 'horizontal' modes of surveillance have become increasingly popular.[20] This involves partially outsourcing surveillance functions to individuals and/or tech companies. A vivid example of such outsourced surveillance was the 2020 Black Lives Matter protests in Dallas, during which the police department asked individuals on Twitter to send them videos from protests that showed 'illegal activity'.[21] A larger-scale example was seen in the aftermath of the 2010 Canadian Winter Olympics riots, in which closed-circuit television (CCTV) footage was used to identify offenders, and private individuals sent the Vancouver Police Department thousands of images and helped them scour social media.[22] Similarly, tech companies such as Facebook, Twitter, and Instagram have been crucial in surveillance of protesters, as the widespread use of social media has made the monitoring of protest and dissident activities significantly easier.[23] For example, in 2014 and 2016, the US government obtained two patents that may facilitate its ability to use social-media to predict when a protest will break out.[24]

Protest movements in USA, Hong Kong, Chile, and beyond have also operated in the shadow of the global COVID-19 pandemic, and together raised questions about unprecedented levels of government power and the expanding regime of mass surveillance in public spaces. The COVID-19 pandemic has given governments a further impetus to explore FRT's health-related uses – from monitoring compliance with quarantine or social-distancing requirements to tracking (in conjunction with other biometric technologies such as thermal scanning) those who are potentially infected. COVID-19 and the latest protests in Hong Kong, Chile, and the United States have redefined the boundaries of mass surveillance and biometric tracking globally, with irreversible implications for the future exercise of government power and surveillance.

7.3 LACK OF REGULATION AND DANGERS OF FRT

Despite the increasing deployment of FRT in many city squares and streets across the globe, as many chapters in this book demonstrate, FRT use is not yet regulated.

[20] D. Trottier, 'Crowdsourcing CCTV surveillance on the internet' (2014) 15(5) *Information Communication and Society* 609; D. Trottier, 'Digital vigilantism as weaponisation of visibility' (2017) 30(1) *Philosophy and Technology* 55.

[21] Heather Kelly and Rachel Lerman, 'America is awash in cameras, a double-edged sword for protesters and police' (3 June 2020), *Washington Post*, www.washingtonpost.com/technology/2020/06/03/cameras-surveillance-police-protesters/. In protest at the request, individuals reportedly sent the police videos and images of K-pop stars.

[22] Debra Mackinnon, 'Surveillance-ready-subjects: The making of Canadian anti-masking law' in Lucas Melgaco and Jeffrey Monoghan (eds.), *Protests in the Information Age* (Routledge, 2018), pp. 151, 162.

[23] Rachel Levinson-Waldman, 'Government access to and manipulation of social media: Legal and policy challenges' (2018) 61(3) *Howard Law Journal* 531–562, at 526–531.

[24] 'U.S. Patent No. 9,892,168 BI' filed on 24 May 2016; 'U.S. Patent No. 9,794,358 BI' filed on 13 March 2014; Farrah Bara, 'From Memphis, with love: A model to protect protesters in the age of surveillance' (2019) 69 *Duke Law Journal* 197–229, at 206.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

Law enforcement agencies around the world are experimenting with FRT with discretion and on an ad hoc basis, without appropriate legal frameworks to govern its use nor sufficient oversight or public awareness.[25] For example, there are currently no federal regulations in the United States governing the use of FRT by law enforcement.[26] In March 2019, two US senators introduced the Commercial Facial Recognition Privacy Act, intended to ban developers and providers of commercial FRT from collecting and sharing data for identifying or tracking consumers without their consent.[27] However, this only focussed on the commercial use of FRT. Similarly, in the EU, regulation of FRT has been very limited. In February 2020, a draft EU White Paper on Artificial Intelligence appeared to call for a discussion about a temporary five-year ban on facial recognition. However, the final draft of this paper removed mention of such a moratorium.[28]

This lack of oversight of FRT use by public bodies can lead to abuses of power and violations of fundamental rights and civil liberties. As many chapters in this book demonstrate, FRT use can result in discriminatory treatment and undermining of privacy and due process, as well as other concerns. Indeed, the dangers of FRT are gradually being recognised by courts. For example, law enforcement's use of automated FRT was successfully challenged in 2020 in R *(on the application of Bridges)* v. *Chief Constable of South Wales Police ([2020] EWCA Civ 1058) ('Bridges*') case, where the Court of Appeal held that the use of automated FRT by South Wales Police was unlawful because it was not 'in accordance with law' for the purposes of Article 8 of the European Convention on Human Rights.[29] In addition, South Wales Police had failed to carry out a proper Data Protection Impact Assessment and had not complied with the public sector equality duty.[30] While *Bridges* is the first successful legal challenge to police use of automated FRT worldwide, fresh lawsuits brought by non-governmental organisations in the United States and France are still pending, and they might provide different judicial responses to regulation of police FRT use.[31]

[25] Monika Zalnieriute, 'Burning bridges: The automated facial recognition technology and public space surveillance in the modern state' (2021) 22(2) *Columbia Science and Technology Review* 314, 284.

[26] Katja Kukielski, 'The First Amendment and facial recognition technology' (2022) 55(1) *Loyola of Los Angeles Law Review* 231.

[27] Charlotte Jee, 'A new face recognition privacy bill would give us more control over our data' (8 October 2019), *MIT Technology Review*, www.technologyreview.com/f/613129/a-new-face-recognition-privacy-bill-would-give-us-more-control-over-our-data/; Security Newswire, 'Commercial facial recognition Privacy Act of 2019 introduced' (n.d.), *Security*, www.securitymagazine.com/articles/90097-commercial-facial-recognition-privacy-act-of-2019-introduced?v=preview.

[28] Amrita Khalid, 'The EU's agenda to regulate AI does little to rein in facial recognition' (20 February 2020), Quartz, https://qz.com/1805847/facial-recognition-ban-left-out-of-the-eus-agenda-to-regulate-ai/.

[29] *[2020] EWCA Civ 1058.*

[30] *R (on the application of Edward Bridges)* v. *The Chief Constable of South Wales Police* [2020] Court of Appeal (Civil Division) C1/2019/2670; EWCA Civ 1058, 210 ('*Bridges (Appeal)*').

[31] *American Civil Liberties Union* v. *United States Department of Justice* (United States District Court, 31 October 2019). In October 2019 the American Civil Liberties Union (ACLU) brought an action

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

Some jurisdictions have already regulated and limited FRT use by law enforcement. In the United States, for example, the cities of San Francisco and Berkeley have banned local agencies (including transport authorities and law enforcement) from using FRT,[32] some municipalities in Massachusetts have banned government use of facial recognition data in their communities,[33] and other US states (California, New Hampshire, and Oregon) have instituted bans on facial-recognition technology used in conjunction with police body cameras.[34] The United Kingdom also has an Automated Facial Recognition Technology (Moratorium and Review) Bill,[35] proposing to ban the use of technologies. Yet its future remains uncertain.

Therefore, not only civil right advocates, but also the courts and politicians widely recognise that FRT can be easily misused by law enforcement to target certain groups of people, such as political activists or marginalised communities, and such targeting often leads to further discrimination and injustice. Importantly, the growing prevalence of surveillance through FRT has a chilling effect on public discourse by threatening the right to protest anonymously; a notion fundamental to protest movements.

7.4 PROTEST MOVEMENTS, PUBLIC SPACE, AND THE IMPORTANCE OF ANONYMITY

Protest movements are collective actions undertaken by a group of people who come together to express their dissent, raise awareness, and advocate for change around a

against the US Department of Justice, the FBI, and the Drug Enforcement Agency, claiming that the public had a right to know when facial recognition software was being utilised under the Freedom of Information Act. The case was filed after the ACLU made a freedom of information request in January 2019. The DoJ, FBI, and DEA failed to produce any responsive documents. ACLU, 'ACLU challenges FBI face recognition secrecy' (31 October 2019), www.aclu.org/press-releases/aclu-challenges-fbi-face-recognition-secrecy; Conseil d'Etat, Décision n 442364 (26 April 2022), www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364.

[32] Kate Conger, Richard Fausset, and Serge Kovaleski, 'San Francisco bans facial recognition technology' (14 May 2019), *New York Times*, www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. The decision was made by the Board of Supervisors, who stated that the responsibility to regulate FRT will lie first with local legislators who have the capacity to move more quickly than the Federal government.

[33] Christopher Jackson, Morgan Livingston, Vetri Velan, Eric Lee, Kimberly Huynh, and Regina Eckert, 'Establishing privacy advisory commissions for the regulation of facial recognition systems at the municipal level' (2020), Science Policy Group, University of California, Berkeley, https://escholarship.org/uc/item/7qp0w9rn.

[34] Max Read, 'Why we should ban facial recognition technology' (30 January 2020), *Intelligencer*, https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html; ACLU, 'California governor signs landmark bill halting facial recognition on police body cams' (8 October 2019), ACLU Northern California, www.aclunc.org/news/california-governor-signs-landmark-bill-halting-facial-recognition-police-body-cams.

[35] Lord Clement-Jones, 'Automated Facial Recognition Technology (Moratorium and Review) Bill [HL]2019–20' (2019), https://services.parliament.uk/bills/2019-20/automatedfacialrecognitiontechnologymoratoriumandreview.html/.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

particular issue or cause.[36] These movements can take many different forms, ranging from peaceful demonstrations, marches, and rallies to civil disobedience, strikes, and other forms of non-violent resistance. Protest movements can emerge in response to a wide range of social, economic, political, and environmental issues. Some of the most common causes of protest movements include discrimination, injustice, corruption, inequality, environmental degradation, and war. Contemporary examples are Occupy Wall Street (2011), Arab Spring (began in 2010), Black Lives Matter (began in 2013), and the Hong Kong pro-democracy movement (began in 2019). Protest movements can also be motivated by a desire to promote social change, challenge existing power structures, and hold those in authority accountable for their actions.

Throughout history, protest movements have played a critical role in advancing social progress and promoting human rights. They have helped to raise awareness of important issues, mobilise public opinion, and influence policy and legislative changes. Examples of protest movements from history include the civil rights movement of the 1950s–1960s, the women's suffrage movement of the late nineteenth and early twentieth centuries and Vietnam anti-war protests (1960s). Today, protest movements continue to be an important tool for promoting social change and advocating for a more just and equitable world.

Protests movements require a tangible and accessible location, typically in the streets and other public places. Public space has always been central to social movements and political protests as a practical place for citizens to gather and as a symbolic place connected to wider democratic values. It provides a physical location where individuals can come together to voice their dissent, express their grievances, and demand change.[37] By occupying public spaces, protesters can create a visible and disruptive presence that draws attention to their cause, and can also serve as a symbolic representation of their struggle.

Public spaces, such as city squares, parks, and streets, are often central to the social and cultural life of a community, and their use for protests can be a powerful statement of the collective will of a group of people. Thus, public spaces are the 'ultimate area of societal interaction' and occupy a symbolic place in society given their accessibility, openness, and, according to Jens Kremer, inherent freedom.[38] When protesters occupy public spaces, they are asserting their right to participate in the democratic process and to be heard by those in power. In interrupting these public spaces, protesters 'touch upon the very core of the current structure and organization of social systems, namely the balance of power, rule of law and democratic

[36] John Scott and Gordon Marshall, *A Dictionary of Sociology* (Oxford University Press, 2009).

[37] Daniel Trottier and Christian Fuchs, 'Theorising social media, politics and the state: An introduction' in Daniel Trottier and Christian Fuchs (eds.), *Social Media, Politics and the State* (Routledge, 2015), pp. 3, 33; Alberto Melucci and Leonardo Avritzer, 'Complexity, cultural pluralism and democracy: Collective action in the public space' (2000) 39(4) *Social Science Information* 507.

[38] Jens Kremer, 'The end of freedom in public places? Privacy problems arising from surveillance of the European public space' (2017), PhD thesis, University of Helsinki, p. 5.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

governance'.[39] It questions the ability of government authorities to maintain the integrity of these shared spaces,[40] thus challenging existing power structures.

Historically, protesters have taken the right to protest anonymously largely for granted; a right that is now becoming increasingly more fragile. The right to anonymity has been fundamental to social movements and protesting, as these events require the population to feel confident and safe in their ability to gather in public spaces and manifest their disagreement with the status quo. This is impossible if they fear surveillance tools can be weaponised against them to suppress and punish their dissent. The sense of safety necessary to facilitate robust democratic participation stems from an understanding that an individual, in the act of demonstrating, is expressing something larger than themselves by joining in a collective. They thus sacrifice their individual voice for the benefit of social disruption, and in return are granted the key right that protesters have enjoyed for centuries; the right of anonymity. The anonymity earned by protesters in public spaces has been increasingly challenged and eroded by surveillance infrastructure.

While the relative anonymity of the individual during protest gatherings has typically 'neutralised' the effect of surveillance, they have been increasingly subject to 'counter-neutralization technologies' that require those individuals to take more active steps to circumvent identification.[41] Of course, protest movements have long devised resistance strategies against surveillance. For example, protesters can break a system a surveillance system by flooding it, rendering surveillance inoperable or impractical.[42] Typical examples include crude forms of neutralisation such as disabling phone lines, wearing masks, and destroying cameras. For example, Hong Kong protesters in 2019 used lasers and broke smart lampposts that they believed contained FRT software.[43] With FRT, protestors are given two choices: first, they can wear a mask and risk arrest and the collection of biometric information in the form of criminal records, or second, they can do without a mask and risk collection of biometric data through FRTs.[44]

Surveillance technologies dealing with political protests have become the norm in many countries, and scholars have theorised about the chilling effect of surveillance on dissent.[45] Monitoring, tracking, and detaining individual protesters for

[39] Ibid., p. 73.

[40] Christoph Burgmer, 'Protestbewegung: Warum einen öffentlichen Platz besetzen?' [Why occupy a public space?] (3 October 2014), *Deutschlandfunk*, www.deutschlandfunk.de/protestbewegung-warum-einen-oeffentlichen-platz-besetzen.1184.de.html?dram:article_id=299327.

[41] G. T. Marx, 'Security and surveillance contests: Resistance and counter- resistance' in T Balzacq (ed.), *Contesting Security. Strategies and Logics* (Routledge, 2015), pp. 15, 23.

[42] G. T. Marx, *Windows into the Soul: Surveillance and Society in an Age of High Technology* (University of Chicago Press, 2016), p. 160.

[43] Byrne and Davis, 'Protest tech'.

[44] Mackinnon, 'Surveillance-ready-subjects', p. 161.

[45] Melgaco and Monoghan, 'Introduction', p. 7; Luis Fernandez, *Policing Dissent: Social Control and the Anti- Globalization Movement* (Rutgers University Press, 2008); P. Gillham, 'Securitizing America: Strategic incapacitation and the policing of protest since the 11 September 2001 terrorist attacks' (2011)

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

their actions in public places significantly shifts the power balance between the state and individuals. Surveillance of political protests undermines the individual as a 'free autonomous citizen', and negatively impacts democracy and the rule of law.[46] Protestors become disempowered in relation to their body and biological information,[47] which is not only threatening, in one sense, to discrete individuals,[48] but in another to discretise protesters, breaking down their collective image. Pervasive surveillance tools can be understood as disciplinary, as they are able to threaten and realise retribution against individual protesters who would otherwise have been lost in a sea of voices, but it is in another sense indicative of a 'controlled' society in which surveillance is ubiquitous.[49]

7.5 PROTECTING PROTESTERS FROM ABUSE: POTENTIAL WAYS TO REGULATE

Given the danger that FRT surveillance in public spaces poses to political protests, the rights to peaceful assembly and association, and wider democratic participation, legislatures should regulate or entirely ban the use of FRT in policing and law enforcement. Regulation of FRT use is a necessary step to ensure the chilling effect of FRT on political expression and freedom of assembly is eliminated.

The chilling effect on freedom of speech and assembly is even stronger in some jurisdictions, such as Australia. This is because, unlike many other jurisdictions discussed in this book, Australia has no human rights protection enshrined in its Constitution and no national human rights legislation.[50] Only three out of eight Australian states and territories have state-level human rights Acts. For this reason, in its recent report, the Australian Human Rights Commission has urged Australia's federal, state, and territory governments to enact legislation regulating FRT.[51]

What are the ways to protect protesters and protest movements from abuse by public authorities? Recent literature related to AI and accountability has recommended

5(7) *Sociology Compass* 636; P. Gillham, B. Edwards, and J. Noakes, 'Strategic incapacitation and the policing of Occupy Wall Street protests in New York City, 2011' (2013) 23(1) *Policing and Society* 81; Jeffrey Monoghan and K. Walby, 'Making up "terror identities": Security intelligence, Canada's integrated Threat Assessment Centre, and social movement suppression' (2012) 22(2) *Policing and Society* 133; Jeffrey Monoghan and K. Walby, '"They attacked the city": Security intelligence, the sociology of protest policing, and the anarchist threat at the 2010 Toronto G20 Summit' (2012) 60(5) *Current Sociology* 653.

[46] Irena Nesterova, 'Mass data gathering and surveillance: The fight against facial recognition technology in the globalized world', *SHS Web of Conferences* 74, 03006, www.shs-conferences.org/articles/shsconf/pdf/2020/02/shsconf_glob2020_03006.pdf, pp. 2–3, 6.

[47] J. Pugliese, *Biometrics: Bodies, Technologies, Biopolitics* (Routledge, 2012).

[48] T Monahan, 'Dreams of control at a distance: Gender, surveillance, and social control' (2009) 9(2) *Cultural Studies – Critical Methodologies* 286; Mackinnon, 'Surveillance-ready-subjects', p. 162.

[49] Melgaco and Monoghan, 'Introduction', p. 9; Gilles Deleuze, 'Postscript on the societies of control' (1992) 59 October 3; Zygmunt Bauman and David Lyon, *Liquid Surveillance: A Conversation* (Polity Press, 2013).

[50] Australian Human Rights Commission, 'How are human rights protected in Australian law?' (2015) https://humanrights.gov.au/our-work/rights-and-freedoms/how-are-human-rights-protected-australian-law.

[51] Australian Human Rights Commission, 'Human rights and technology: Final report' (March 2021).

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

several avenues, including regulation,[52] the development of technical methods of explanation,[53] the promoting of auditing mechanisms,[54] and the creation of standards of algorithmic accountability in public and private bodies.[55] Law, of course, should also play a role.

7.5.1 *Privacy Law*

Privacy law provides one avenue to regulate police use of FRT in public spaces.

Scholars have long argued that public activities deserve privacy protections, and that the simple act of being 'in public' does not negate an individual's expectation of privacy.[56] However, as Jake Goldenfein in Chapter 5 of this book suggests, privacy law has severe limitations when regulating the use of FRT. For example, the US Fourth Amendment, under current Supreme Court jurisprudence, has been viewed as an unlikely protection against FRT for two reasons: first, jurisprudence has typically ignored pre-investigatory surveillance,[57] and secondly, it has failed to encompass identification of information already exposed to the public.[58] In relation to the Fourth Amendment, Douglas Fretty questions whether Constitutional protection will require the Supreme Court to confirm the 'right of the people to be secure' or simply display how insufficient the Fourth Amendment is in safeguarding individuals beyond the scope of their private spaces.[59] Drawing on recent US Supreme Court cases concerning GPS tracking and other technologies and

[52] Marion Oswald, 'Algorithm-assisted decision-making in the public sector: Framing the issues using administrative law rules governing discretionary power' (2018) 376(2128) *Philosophical Transactions of the Royal Society A*, https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2017.0359; Andrew Tutt, 'An FDA for algorithms' (2017) 69 *Administrative Law Review* 83.

[53] Brent D. Mittelstadt, Chris Russell, and Sandra Wachter, 'Explaining explanations in AI', *Proceedings of FAT* '19: Conference on Fairness, Accountability, and Transparency (FAT* '19)*, Atlanta, GA, ACM, New York (29–31 January 2019).

[54] Brent Mittelstadt, 'Auditing for transparency in content personalization systems' (2016) 10 *International Journal of Communication* 4991; Pauline T. Kim, 'Auditing algorithms for discrimination' (2017) 166 *University of Pennsylvania Law Review Online* 189.

[55] Corinne Cath et al., 'Artificial intelligence and the "good society": The US, EU, and UK approach' (2018) 24 *Science and Engineering Ethics* 505.

[56] Tjerk Timan, Bryce Clayton Newell, and Bert-Jaap Koops (eds.), *Privacy in Public Space: Conceptual and Regulatory Challenges* (Edward Elgar, 2017); Bryce Clayton Newell, Tjerk Timan, and Bert-Jaap Koops, *Surveillance, Privacy and Public Space* (Routledge, 2019); N. A. Moreham, 'Privacy in public places' (2006) 65(3) *The Cambridge Law Journal* 606; Joel Reidenberg, 'Privacy in public' (2014) 69(1) *University of Miami Law Review* 141; Helen Fay Nissenbaum, 'Towards an approach to privacy in public: Challenges of information technology' (1997) 7(3) *Ethics & Behaviour* 207; Beatte Roessler, 'Privacy and/in the public sphere' (2016) 1 *Yearbook for Eastern and Western Philosophy* 243.

[57] Elizabeth Joh, 'The new surveillance discretion: Automated suspicion, big data, and policing' (2016) 10 *Harvard Law & Police Review* 15, 33.

[58] Orin Kerr, 'The case for the third-party doctrine' (2009) 107 *Michigan Law Review* 561, 566; Ferguson, 'Facial recognition and the Fourth Amendment', pp. 16–17.

[59] Douglas A. Fretty, 'Face-recognition surveillance: A moment of truth for Fourth Amendment rights in public places' (2011) 16(3) *Virginia Journal of Law & Technology* 430, 463.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

the Fourth Amendment,[60] Andrew Ferguson suggests that the Supreme Court is cognisant of the need to adapt Fourth Amendment jurisprudence to emerging technologies.[61] He identifies six key principles in adapting the Fourth Amendment to deal with modern concerns. First, technological searches cannot be viewed as equivalent to pre-technological police investigatory modes.[62] Secondly, there must be a general presumption against the large-scale aggregation of data.[63] Thirdly, there must be a general presumption against the long term storage and ongoing use of aggregated data.[64] Fourthly, the ability to track and trace an individual must be a relevant factor in considering the application of the Fourth Amendment.[65] Fifthly, the concept of anti-arbitrariness must be transposed to a digital setting to act against automated technologies that do not require probable cause.[66] Sixthly, monitoring technologies must not be so over-reaching as to grossly permeate civil society.[67] However, the Fourth Amendment offers limited support in the protection of protest movements from FRT surveillance in public spaces.

7.5.2 *Discrimination Law*

Could discrimination law provide a better avenue to regulate police use of FRT in public spaces? The emerging consensus in an increasing body of academic research is that FRTs are not 'neutral',[68] but instead reinforce historical inequalities.[69] For example, studies have shown that FRT performs poorly in relation to women, children, and individuals with darker skin tones.[70]

[60] *United States* v. *Jones* [2012] US Supreme Court 565 U.S. 400; *Carpenter* v. *United States* [2018] United States Supreme Court 138 S. Ct.; *Riley* v. *California* [2014] United States Supreme Court 573 US 373.

[61] Ferguson, 'Facial recognition and the Fourth Amendment', p. 21.

[62] Ibid., pp. 21–23: 'Anti-equivalence principle'; *Carpenter* v. *United States* 2219.

[63] Ferguson, 'Facial recognition and the Fourth Amendment', pp. 23–24: 'Anti-aggregation principle'.

[64] Ibid., pp. 24: 'Anti-permanence principle'.

[65] Ibid., pp. 24–26: 'Anti-tracking principle'.

[66] Ibid., pp. 26–27: 'Anti-arbitrariness principle'.

[67] Ibid., pp. 27–28: 'Anti-permeating surveillance principle'.

[68] Clare Garvie, Alvaro Bedoya, and Jonathan Frankle, '*The perpetual line-up*: Unregulated police face recognition in America' (18 October 2016), Georgetown Law Center on Privacy and Technology, www.perpetuallineup.org/; Brendan F. Klare, Mark J. Burge, Joshua C. Klontz, Richard W. Vorder Bruegge, and Anil K. Jain, 'Face recognition performance: Role of demographic information' (2012) 7 *IEEE Transactions on Information Forensics and Security* 1789; Joy Buolamwini and Timnit Gebru, 'Gender shades: Intersectional accuracy disparities in commercial gender classification' (2018) 81 *Proceedings of Machine Learning Research* 1, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[69] Matthew Schwartz, 'Color-blind biometrics? Facial recognition and arrest rates of African-Americans in Maryland and the United States' (2019), Thesis in partial fulfilment of a Masters in Public Policy, Georgetown University, p. 15.

[70] Salem Hamed Abdurrahim, Salina Abdul Samad, and Aqilah Baseri Huddin, 'Review on the effects of age, gender, and race demographics on automatic face recognition' (2018) 34 *The Visual Computer* 1617–1630; Jacob Snow, 'Amazon's face recognition falsely matched 28 members of Congress with mugshots' (26 July 2018), ACLU, www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

This bias and discrimination can be introduced into the FRT software in three technical ways: first, through the machine learning process, based on the training data set and system design; secondly, through technical bias incidental to the simplification necessary to translate reality into code; and thirdly, through emergent bias that arises from users' interaction with specific populations.[71] Because the training data for FRTs in the law enforcement context comes from photos relating to past criminal activity,[72] minority groups and people of colour are over-represented in FRT training systems.[73] In some jurisdictions, such as the United States, people of colour are at a much higher risk of being pulled over,[74] searched,[75] arrested,[76] incarcerated,[77] and wrongfully convicted than white women.[78] Therefore, police use of FRT to repress political protests can produce a large number of false positives – as it is already functioning in a highly discriminatory environment; and this can impact on the freedom of assembly and association of those already marginalised and discriminated against. However, discrimination law alone offers limited support in the protection of protest movements from FRT surveillance in public spaces.

7.5.3 *Holding Private Companies Accountable for FRT Surveillance of Public Spaces*

Private actors are also playing a role in the increasing surveillance of public spaces by stifling protest movements and political participation worldwide, and we need to

[71] Rebecca Crootof, '"Cyborg justice" and the risk of technological–legal lock-in' (2019) 119(1) *Columbia Law Review* 1, 8; Batya Friedman and Helen Fay Nissenbaum, 'Bias in computer systems' (1996) 14 *ACM Transactions on Information Systems* 330, 333–336.

[72] Henriette Ruhrmann, 'Facing the future: Protecting human rights in policy strategies for facial recognition technology in law enforcement' (May 2019), CITRIS Policy Lab, https://citrispolicylab.org/wp-content/uploads/2019/09/Facing-the-Future_Ruhrmann_CITRIS-Policy-Lab.pdf, p. 46; Garvie, Bedoya, and Frankle, 'The perpetual line-up'.

[73] Ruhrmann, 'Facing the future', p. 63; Garvie, Bedoya, and Frankle, 'The perpetual line-up'.

[74] Nusrat Choudhury, 'New data reveals Milwaukee police stops are about race and ethnicity' (23 February 2018), ACLU, www.aclu.org/blog/criminal-law-reform/reforming-police/new-data-reveals-milwaukee-police-stops-are-about-race-and; Frank R. Baumgartner, Derek A. Epp and Kelsey Shoub, *Suspect Citizens What 20 Million Traffic Stops Tell Us about Policing and Race* (Cambridge University Press, 2018).

[75] 'Choudhury, 'New data reveals'; Camelia Simoiu, Sam Corbett-Davies, and Sharad Goel, 'The problem of infra-marginality in outcome tests for discrimination' (2017) 11(3) *The Annals of Applied Statistics* 1193; Lynn Lanton and Matthew Durose, 'Police behavior during traffic and street stops, 2011' (September 2013), US Department of Justice, www.bjs.gov/content/pub/pdf/pbtss11.pdf.

[76] NAACP, 'Criminal Justice Fact Sheet' (n.d.), www.naacp.org/criminal-justice-fact-sheet/; Megan Stevenson and Sandra Mayson, 'The scale of misdemeanor justice' (2018) 98 *Boston University Law Review* 371.

[77] Ashley Nellis, 'The color of justice: Racial and ethnic disparity in state prisons' (13 October 2021), The Sentencing Project, www.sentencingproject.org/publications/color-of-justice-racial-and-ethnic-disparity-in-state-prisons/.

[78] Samuel Gross, Maurice Possley, and Klara Stephens, *Race and Wrongful Convictions in the United States* (National Registry of Exonerations, 2017), www.law.umich.edu/special/exoneration/Documents/Race_and_Wrongful_Convictions.pdf.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

insist on holding them accountable. Private companies, such as telecommunications service providers and tech giants, have been co-operating with law enforcement agencies and developing the technical infrastructure needed for public space surveillance. This includes police purchasing and using privately developed FRT technology or image databases, both of which often happen in secret. For example, IBM, one of the world's oldest (and largest) technology companies,[79] has recently collaborated with repressive governments by providing FRT software. Best known for its famous personal computers, in recent years the company's focus has shifted to AI and FRT.[80] A detailed report by *The Intercept* published in March 2019 revealed that in 2012 IBM provided police forces in the Philippines with video surveillance technology, which was subsequently used to perpetuate President Duterte's war on drugs through extra-judicial killings.[81] The brutal and excessive crime suppression tactics of the Davao police were well known to local and international human rights organisations.[82]

At the time, IBM defended the deal with Philippines, saying it 'was intended for legitimate public safety activities',[83] but claimed that it had ceased provision of its technology to the Philippines in 2012. However, it took at least several years for IBM to stop providing general purpose FRT software to law enforcement (e.g., IBM mentioned its Face Capture technology in a public disclosure in 2013 and 2014, related to its Davao City project).[84] The company's practice of providing authoritarian regimes with technological infrastructure is not new and dates back to the 1930s, when IBM supplied the Nazi Party with unique punch-card technology that was used to run the regime's censuses and surveys to identify and target Jewish people.[85]

Because of such close (and often secretive) collaboration between private tech companies and governments, we need to think of new ways to hold the companies providing the FRT infrastructure accountable – not just in aspirational language, but in law. Currently, in many countries, the application of human rights laws is limited to government bodies only (anti-discrimination and data protection laws being the primary exceptions of horizontal application).[86] The same is true

[79] Encyclopedia Britannica, 'IBM: Founding, history, & products', www.britannica.com/topic/International-Business-Machines-Corporation.

[80] Eric Reed, 'History of IBM: Timeline and facts' (24 February 2020), *TheStreet*, www.thestreet.com/personal-finance/history-of-ibm.

[81] George Joseph, 'Inside the video surveillance program IBM built for Philippine strongman Rodrigo Duterte' (20 March 2019), *The Intercept*, https://theintercept.com/2019/03/20/rodrigo-duterte-ibm-surveillance/.

[82] Ibid.

[83] Ibid.

[84] Ibid.

[85] Edwin Black, *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation-Expanded Edition* (Crown Publishers, 2001).

[86] Monika Zalnieriute, 'From human rights aspirations to enforceable obligations by non-state actors in the digital age: The case of internet governance and ICANN' (2019) 21 *Yale Journal of Law & Technology* 278.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

of international human rights law. This leaves private companies in the human rights gap. However, as I have argued elsewhere in detail, existing efforts focussing on voluntary 'social and corporate responsibility' and ethical obligations of private tech companies are insufficient and incapable of tackling the challenges that these technologies pose to freedom of expression and association.[87] Moreover, a lot of those efforts have merely been 'transparency washing' – performatively promoting transparency and respect for human rights while acting in ways that undermine both.[88]

The problem of the human rights gap is greater in some jurisdictions, such as Australia, which lacks a federal level human rights framework and where governments often remain unaccountable for public space surveillance. Therefore, we need to demand change and accountability from governments, police, and tech companies. We should not continue to rely on the 'goodwill' of tech companies, when they promise to 'respect' our right to protest and our freedom of association and assembly. We need to demand hard legal obligations for private actors because of the significant role they play in increasing public space surveillance and infrastructure. We need data protection and human rights laws that bind companies, to ensure that political movements and protests can flourish and that communities whose rights to peaceful assembly and association have been curtailed via FRT technologies can access an effective remedy.

7.5.4 *Outright Bans on Police Use of FRT*

Of course, even with all the limits that could be placed by law, police use of FRT in public spaces is problematic in itself – owing to the centrality of public space and anonymity for protest movements. It is thus not surprising that many scholars, activists, regulators, and politicians have turned to arguing for bans on FRT use. For example, US scholar Ferguson advocates for a blanket ban on facial surveillance, a probable cause requirement for facial identification, a ban or probable cause-plus standard for facial tracing, and limitations to facial verification at international borders in addition to increased accountability for error, bias, transparency, and fairness.[89]

Proposals to ban FRT have also been coming from sources outside the academic realm; with informal resistance groups such as the developers of the website Fight for the Future running a project called Ban Facial Recognition, which operates an interactive map of where and how the government is using FRT around the United States.[90] Further, the United Kingdom's Equality and Human Rights

[87] Ibid.

[88] Monika Zalnieriute, '"Transparency-washing" in the digital age: A corporate agenda of procedural fetishism' (2021) 8(1) *Critical Analysis of Law* 39.

[89] Ferguson, 'Facial recognition and the Fourth Amendment', pp. 63–73.

[90] 'Ban Facial Recognition', www.banfacialrecognition.com/.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press

Commission,[91] and the Australian Human Right Commission,[92] have recently called on governments to introduce a moratorium on the use of FRT in policing and law enforcement before legislation regulating the use of FRT and other biometric technology is formally introduced.

7.6 CONCLUSION

If the government and law enforcement can resort to FRT without any restrictions or safeguards in place, the right to protest anonymously will be curtailed and political discourse in our democracies will be stifled. For example, the High Court of Australia – Australia's apex court – has emphasised the centrality of the right to protest to Australian democracy: besides casting their vote in elections, Australians have no other avenues through which to voice their political views.[93] Adapting Hannah Arendt's famous quote used at the beginning of this chapter, political freedom must enable a right to participate in government. And in many instances, the only way to do that, in addition to voting, is through political protest.

Before FRTs develop further and become even more invasive, it is imperative that this public surveillance infrastructure is limited. We need laws restraining the use of FRT in our public spaces, and we need hard legal obligations for those who develop and supply law enforcement with them. The reforms could start with an explicit ban (or at least suspension) on police use of FRT in public spaces, pending independent scrutiny of the discriminatory impacts the technology may have against women and other protected groups.[94] These proposed changes are not drastic. In fact, they are a modest first step in the long journey ahead to push back against escalating surveillance of the public sphere worldwide.

[91] For example, the UK Equality and Human Rights Commission had, in March 2020, called on suspension; see Equality and Human Rights Commission, 'Facial recognition technology and predictive policing algorithms out-pacing the law' (12 March 2020), www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law.

[92] Australian Human Rights Commission, '*Human Rights and Technology Final Report*' (1 March 2021), https://tech.humanrights.gov.au/downloads?_ga=2.200457510.901905353.1624842000-1160604841.1624842000.

[93] *Brown* v. *Tasmania* [2017] HCA 43.

[94] For example, the UK Equality and Human Rights Commission had, in March 2020, called on suspension; see Equality and Human Rights Commission, 'Facial recognition technology'.

https://doi.org/10.1017/9781009321211.009 Published online by Cambridge University Press