How Public Space Surveillance is Eroding Political Protests in Australia

Monika Zalnieriute 2021-12-14T10:38:31

On 24 July 2021, an estimated 3,500 Australians marched through Sydney's Central Business District to protest the city's then month-long COVID-19 lockdown. In response, the New South Wales Police created a taskforce to „forensically investigate" CCTV and social media footage from the protest so that attendees can be identified and punished. But the police has refused to confirm whether facial recognition technology ("FRT") – standard or real-time – was, or would be, deployed to do so. Police has also remained tight-lipped in the past about whether it had used any kind of FRT in policing other high-profile protests. Although the COVID-19 lockdown protests were widely condemned by the general public, the potential use of FRT by the police illustrates the implications of an expanding surveillance infrastructure in Australia after 9/11 and raises serious questions about the future of the Australian public sphere.

The Australian government, just like many others, has significantly increased surveillance of the public sphere following 9/11: Australian city streets and squares, stations, airports, social media and online platforms have become equipped with sophisticated surveillance tools, enabled and made legal through myriad of complex and ever-expanding "emergency" laws. In this short blogpost, I will only cover two such tools: metadata tracking and FRTs. My emphasis will be on *public spaces* and *political protests*.

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. For social movements to function, citizens must feel confident and safe in their ability to gather in public spaces to express their disagreement with the status quo. This is impossible if they fear surveillance tools are weaponized against them to suppress and punish their dissent.

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 are taking centre stage, governments around the world are increasing their surveillance capacities in the name of "protecting the public" and "addressing emergencies". Irrespective of whether these events and/or political strategies framed as "emergencies" were the "war on terror" with its invisible geopolitical enemies for 9/11, or were they pro-democracy or anti-racism protests COVID-19, state resort to technology and increased surveillance as a tool to control the masses and population has been similar.

Australia is not an exception to this trend. In this post, I will focus on metadata tracking and data retention laws, which have expanded significantly after 9.11, in suppressing political protests in Australia. I will also cover the "chilling effect" of

FRT use in Australian public spaces on the right to peaceful assembly and protest, and the absence of oversight mechanisms. I will finish by drawing attention to the crucial role of telecommunications service providers and tech companies in assisting governments in public space surveillance and curtailing protests, and argue that we need hard human rights obligations to bind these companies and Australian governments, to ensure that political movements and protests can flourish twenty years after 9/11.

Using Metadata Tracking to Suppress Political Protests

First, since 9/11, Australian public space and political protests have been significantly and increasingly affected by metadata tracking and data retention laws. The capacity of mobile data tracking has increased considerably in the past decade, and escalated further since the start of the worldwide COVID-19 pandemic in 2020. Australian governments (states and territories), just like many other governments across the world, can now follow citizens' movements through contact tracing apps. These apps and general metadata tracking technology, coupled with Australia's weak metadata legislation (which does not even define the term "metadata"), give the government unprecedented tools to surveill public spaces and find out who has attended protests and take repressive action.

Metadata is "data about data": the location, date, time, duration and form of communications and web browsing activity and other details. While it does not reveal the *content* of communications, metadata can be used to create a detailed digital picture of individuals – their identity, movements, contacts, interests, and associations – continuously, surreptitiously, and automatically through their mobile phones. Access to this data enables law enforcement and intelligence agencies to draw links between people who are organizing, attending or intending on speaking at political protests in public spaces across Australia.

Following the 9/11 terrorist attacks, the Australian government, just like many others across the globe, adopted mandatory data retention and interception laws, compelling private companies to retain customers' personal data and disclose it to national security agencies through state legislation, federal legislation and international agreements. Under Australia's federal metadata access regime, telecommunications providers must retain metadata for two years and provide it on request, not just to law enforcement, but also to the government's welfare, tax, revenue protection, fines enforcement agencies and numerous other professional associations and government bodies. Metadata can be accessed without a warrant, the reporting requirements for police access are incomprehensibly vague, and local government and state health departments need not report access at all.

In a report, released in February 2020, Commonwealth Ombudsman Michael Manthorpe has detailed how telecommunications companies retain and provide data to law enforcement agencies *beyond* what legislation permits, such as users' web

browsing histories. He also revealed that during 2018-2019, numerous agencies accessed metadata "without proper authority" through unauthorized disclosure.

Since the COVID-19 crisis began, this surveillance capacity was further expanded by the Australian governments. First, the federal Biosecurity Act 2015 as well as many state level measures made it easier for data to be shared between even more departments and organisations. Second, additional surveillance measures were adopted under the *Privacy Amendment (Public Health Contact Information) Act 2020* (Cth) ("the COVIDSafe Act"), with justifications of exceptional necessity that also loosened the safeguards for data sharing and access further.

These developments are worrying, given the volume of data collected from the numerous COVID-19 contact tracing apps used in Australia. But even more so, and contrary to government assurances that this data will not be shared with law enforcement, COVID-19 contact tracing data has already been used for police investigations in two out of six Australian states, and has been "incidentally" collected by Australia's intelligence agencies.

It is unknown whether Australian governments and law enforcement have already used the metadata retention scheme and/or COVID-19 contact tracing app data specifically to suppress political protests. It is hard to find out, given the lack of detailed reporting requirements for police access to metadata. However, the idea of doing so seems to appeal to many Australian politicians. Last year, Scott Morrison, the current Australian Prime Minister, vowed to penalize those who boycotted businesses for environmental reasons in response to climate change protests in Australia. In late 2019, Peter Dutton, the Minister for Home Affairs, advocated for punishment for climate protesters, including depriving them of welfare payments, charging them for the cost of police responses to protests, and even public shaming, calling for their "names" and "photos" to be "distribute[d] […] as far and wide as we can". In a political climate riddled with such anti-protest rhetoric, metadata tracking tools and COVID-19 tracing apps are convenient tools to identify protesters, undermine the anonymity, foundational to social movements and political protests in public spaces in Australia.

Facial Recognition Technology on Public Space and Political Protests

Another convenient tool, at the increasing disposal of governments and law enforcement in public spaces in Australia, has been facial recognition technology (FRT). The Australian states of Queensland and Western Australia have built-in real-time FRT in their security cameras. Likewise, Australian police forces, including the Australian Federal Police and Queensland, Victoria and South Australia's state police, reportedly use the private company Clearview AI's FRT service (despite previously denying this). New South Wales police is using photographs collected by the Australian Federal Government to trial facial recognition in criminal investigations. And just two years ago, in 2019, the Australian Federal Government attempted to establish a centralized facial recognition database, but this initiative

was thwarted by a parliamentary commission over human rights and privacy concerns.

Despite the increasing deployment of FRT in Australian cities, streets and airports, such use is currently not regulated under any legislation. There is no Bill in development either. However, as I have argued in a recent paper, 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 social movements and protests. This chilling effect is even stronger in Australia, as compared to many other jurisdictions, because Australia has no human rights protection enshrined in its Constitution and no national human rights legislation. Only three out of eight of Australia's 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.

The dangers of FRT have been recognized both by courts and politicians in many other countries. For example, law enforcement's use of automated FRT was successfully challenged in 2020 in the *Bridges* case, where the Court of Appeal of England and Wales held that police use of automated FRT was unlawful because it was not "in accordance with law" under Article 8 ECHR. Some jurisdictions have already regulated and limited its use by law enforcement. For example, in the USA, California, New Hampshire, and Oregon have prohibited the use of FRT in conjunction with police body cameras. The State of New York has adopted a *Public Oversight of Surveillance Technology Act*, which aims to increase transparency for how surveillance technologies are used by the New York Police Department. San Francisco has prohibited the use of FRT by local agencies, including transport authorities and law enforcement. Some municipalities in Massachusetts have banned government use of facial recognition data in their communities. Other countries are also taking action; for example, the UK has an *Automated Facial Recognition Technology (Moratorium and Review) Bill*, proposing to ban the use of FRT technologies in the UK.

Given the danger that FRT surveillance in public spaces poses to political protests, the rights to peaceful assembly and association, and wider democratic participation, the Australian government should entirely ban the use of FRT in policing, law enforcement, and other areas with "a high risk to human rights". Such a moratorium on FRT is a necessary step for protecting Australians from the technology's "chilling effect" on political expression.

Holding Companies Accountable for Public Space Surveillance

Private actors also play role in the increasing surveillance of public spaces, stifling protest movements and political participation in Australia, and we need to insist on holding them accountable. For the past twenty years since 9/11, private companies, such as telecommunications service providers and tech giants, have

been cooperating with law enforcement agencies and developing the technical infrastructure needed for public space surveillance. Data retention and access regimes depend on private companies' collection and retention of data, and police purchase and use privately-developed FRT technology or image databases, both of which often happen in secret.

For this reason, we need to think of new ways to hold the companies providing the infrastructure accountable – and 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 are the primary exceptions of horizontal application). The same is true of international human rights law. This leaves private companies in the human rights gap. However, as I have detailed in my recent article, many voluntary "social and corporate responsibility" efforts by private tech companies have merely been "transparency washing" – performatively promoting transparency and respect for human rights while acting in ways that undermines both.

The problem of the human rights gap is even greater in Australia, which lacks a federal level human rights framework, and where even governments often remain unaccountable for public space surveillance. Australians thus 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 privacy and freedom of association. We need to demand hard legal obligations for private actors because of the significant role they play in increasing public space surveillance and infrastructure after 9/11. We need data protection and human rights laws that bind companies, to ensure that political movements and protests can flourish, that communities whose rights to peaceful assembly and association have been curtailed via data tracking and FRT technologies can access an effective remedy.

Conclusion

The High Court of Australia, Australia's apex court, has emphasized 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. If the government and law enforcement can resort to surveillance tools, such as metadata tracking and FRT, without any restrictions or safeguards in place, the right of Australians to protest anonymously will be curtailed, and Australia's political discourse will be stifled.

Before these technologies develop further and become more invasive, now is a good time to limit public surveillance infrastructure in Australia. We need laws limiting the use of such technologies 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 limiting police access to federal metadata regimes for the purposes of suppressing political protests or intervening with protestors. The reforms could continue with an explicit ban on the police use of FRT in public spaces in Australia. 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 in Australia.

My work and research for this submission 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). I would like to thank Emily Hunyor for research assistance.
