DIGITAL
RIGHTS
WATCH

Submission to the United Nations, Special Rapporteur on freedom of peaceful assembly and of association

regarding the

Call for input for the HRC62 thematic report on "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects."

November 2025

Who we are

Digital Rights Watch is a charity founded in 2016 to promote and defend human rights as realised in the digital age. We stand for privacy, democracy, fairness, and freedom. Digital Rights Watch educates, campaigns, and advocates for a digital environment in which rights are respected, and connection and creativity can flourish. More information about our work is available on our website: www.digitalrightswatch.org.au

Acknowledgement of Country

Digital Rights Watch acknowledges the Traditional Owners of Country throughout Australia and their continuing connection to land and community. We acknowledge the Aboriginal and Torres Strait Islander peoples as the true custodians of this land that was never ceded and pay our respects to their cultures, and to elders past and present.

Contact

Tom Sulston | Head of Policy | tom@digitalrightswatch.org.au

Elizabeth O'Shea | Chair | lizzie@digitalrightswatch.org.au

Lucinda Thorpe | Privacy Campaigner | lucinda@digitalrightswatch.org.au

Introduction

Australians' right to protest is eroded daily. Behind the scenes, digital surveillance is assisting this erosion, and AI has the potential to accelerate the damage. This is made possible by Australia's weak privacy laws.

In 2024, the government committed to passing about 100 privacy reforms.[1] Thus far, only a handful have been enacted.[2] Passing these reforms would mitigate—and in some cases prevent—the harms outlined in this report.

This submission focuses on three instances in which AI-powered surveillance has impacted protest rights in Australia.

Case Study One: Home Affairs and 'Locate X'

A 2024 review of government tenders showed that the Australian Government held over $5 million AUD of contracts with Babel Street, a software company selling AI-powered surveillance products.[3] Government departments with these contracts included the Home Affairs Department, the Department of Defence and the Australian Signals Directorate.

None of these agencies engaged in community consultation or even notified the public that they had adopted surveillance technologies with the potential to be used against the general population. This evasion of public scrutiny allows government agencies to leverage commercial surveillance with little debate, while preventing the public from understanding how they are being surveilled.

A Freedom of Information (FOI) request filed by *The Guardian* revealed that the Department of Home Affairs' contract with Babel Street granted it access to Locate X, a smartphone tracking tool designed for indiscriminate use within

[1] Attorney-General's Department, *Government Response to the Privacy Act Review Report*, September 28,2023,https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF

[2] MinterEllison, "First Tranche of Privacy Reforms Passed," accessed November 6, 2025,https://www.minterellison.com/articles/first-tranche-of-privacy-reforms-passed

[3] "Babel St," Tenders Australia, accessed October 30, 2025, https://www.tenders.gov.au/Search/KeywordSearch?keyword=Babel+St

"digital fences".[4] Digital fencing enables the retrospective identification and tracking of every device within a defined area, such as within a protest. The FOI request also revealed that Home Affairs paid additional fees for the premium version of Locate X to ensure its utility in large crowds.[5] Locate X enables Home Affairs to retrospectively identify and track every device present at a protest, allowing authorities to map political participation without warrants or individual suspicion.

Mobile phones constantly generate precise location data through GPS signals, Wi-Fi networks, Bluetooth beacons and cell towers. Apps collect this data and share it with third-party data brokers as part of the advertising ecosystem. Users rarely read the fine print or understand that consent includes ongoing location collection, even when the app is not actively in use.[6] Data brokers combine these streams into large commercial datasets and sell access to analytics companies. Government agencies do not typically collect this information directly but instead purchase access to these datasets through commercial surveillance products such as those marketed by Babel Street.[7]

The information chain from user to government illustrates how commercial over-extraction of data facilitates state surveillance. The same pattern is evident in Australia's partnerships with companies such as Palantir, which has held government contracts since 2014 totalling AUD $37,315,489.60.[8] In most cases, the scope of these contracts remains unclear.

Home Affairs has offered no reassurances that guard-rails are in place to prevent this technology impacting our right to assembly, particularly where this affects minority groups. This is concerning given that the Australian government has a

[4] Ariel Bogle, "Revealed: Home Affairs paying to access controversial tool tracking mobile phone movements," *The Guardian (Australia)*, 6 Nov. 2023, https://www.theguardian.com/australia-news/2023/nov/06/home-affairs-locate-x-paying-mobile-phone-tracking-tool

[5] Ibid.

[6] Office of the Australian Information Commissioner. *Australian Community Attitudes to Privacy Survey 2020*. Canberra: OAIC, 2020. https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2020

[7] Bill Budington, "Creators of This Police Location Tracking Tool Aren't Vetting Buyers. Here's How To Protect Yourself," *Electronic Frontier Foundation Deeplinks Blog*, 8 Nov. 2024, https://www.eff.org/deeplinks/2024/11/creators-police-location-tracking-tool-arent-vetting-buyers-heres-how-protect

[8] "Tenders Australia," Search results for "PALANTIR Technologies Australia Pty Ltd," Tenders.gov.au, accessed 3 November 2025, https://www.tenders.gov.au/Search/KeywordSearch?Keyword=PALANTIR+TECHNOLOGIES+AUSTRALIA+PTY+LTD&submitSort=Go&OrderBy=Publish+Date&sort=.

long history of disproportionately surveilling minority groups,[9] such as Indigenous Australians.[10]

Home Affairs justified its use of surveillance technology saying it "collects commercially available and publicly available online information where it is necessary to support the department's and Australian Border Force's specific functions and activities, and where it is proportionate and in accordance with the law" — and "The department has acquired the minimal amount of Babel Street software that it considers necessary to facilitate the lawful investigation of priority matters."[11]

This surveillance exploits gaps in Australian privacy legislation. The *Telecommunications (Interception and Access) Act 1979*[12] governs how government bodies can intercept private communications between individuals and establishes strict warrant protocols to prevent abuse.[13][14] However, because Locate X relies on commercially available data, Home Affairs and other departments can use it without obtaining warrants. This means their use of Locate X is, at least technically, lawful under current legislation.

New technologies such as Locate X can provide detailed insights into a person's movements and associations comparable to what law enforcement would gain through a surveillance warrant, yet they are not subject to equivalent legal safeguards. Traditionally, mapping individuals' movements would require a telecommunications interception warrant or a named persons warrant,[15][16] approved by the Attorney-General and limited in scope and duration. By purchasing commercial location data instead, agencies can bypass these accountability mechanisms entirely. They can monitor broad populations without

[9] Freedom House, *Transnational Repression*, accessed November 3, 2025, https://freedomhouse.org/report/special-report/2025/more-action-needed-ensure-safety-combating-transnational-repression.

[10] Joy, R. (2023) 'Fear of the dark: The racialised surveillance of Indigenous peoples in Australia', in Brunon-Ernst, A. et al. (eds) *Law, Surveillance and the Humanities*. Edinburgh: Edinburgh University Press, pp. 216–234. doi:10.3366/edinburgh/9781399505086.003.0011. https://academic.oup.com/edinburgh-scholarship-online/book/55672/chapter-abstract/436057999?redirectedFrom=fulltext&login=true

[11] Ariel Bogle, "Revealed: Home Affairs paying to access controversial tool tracking mobile phone movements," *The Guardian (Australia)*, 6 Nov. 2023, https://www.theguardian.com/australia-news/2023/nov/06/home-affairs-locate-x-paying-mobile-phone-tracking-tool

[12] *Telecommunications (Interception and Access) Act 1979* (Cth)

[13] *Telecommunications (Interception and Access) Act 1979* (Cth) ch 2 pt 2-2.

[14] *Telecommunications (Interception and Access) Act 1979* (Cth) ch 2 pt 2-2, s 9.

[15] *Telecommunications (Interception and Access) Act 1979* (Cth) ch 2 pt 2-2 s 9.

[16] *Telecommunications (Interception and Access) Act 1979* (Cth) ch 2 pt 2-2 s 9A.

reasonable suspicion or statutory limits, enabling mass surveillance that would be unlawful under warrant-based systems.

If Home Affairs were to intercept private location data without a warrant, affected individuals could pursue civil remedies.[17] However, when the same information is acquired en masse through Locate X, no such remedy exists under the *Telecommunications (Interception and Access) Act 1979.*[18]

Case Study Two: Melbourne City Council expands CCTV Network

Melbourne City Council's proposed expansion of its CCTV network, and its potential use of artificial intelligence for facial identification, raises serious concerns about the right to peaceful assembly in Australia.

The majority of protests in Victoria occur within the City of Melbourne, meaning political activity is highly visible to these systems. When surveillance tools collect biometric data and track protesters without consent, they do more than monitor public spaces. These protests can expose political beliefs, facilitate disproportionate policing, and create a climate of fear that deters people from participating in democratic protest. This may act as a deterrent for people to attend protests, especially as the number of arrests and convictions resulting from protest is increasing in Australia.[19]

The plan came to light in a Melbourne council meeting on Tuesday 7th October 2025[20] and centers on placing 100 additional CCTV cameras into the Melbourne council area. 40 of these would be owned by the council and 60 are privately owned. Ownership of the private cameras has not yet been disclosed. The applicable privacy obligations of the private camera owners will depend on several factors: for instance, small businesses earning under $3 million annually

[17] *Telecommunications (Interception and Access) Act 1979* (Cth) ch 2 pt 2-10.
[18] *Telecommunications (Interception and Access) Act 1979* (Cth).
[19] Human Rights Law Centre, "New evidence shows right to protest in peril in Australia
," *Human Rights Law Centre*, accessed October 30, 2025,
https://www.hrlc.org.au/news/2024-07-03-protest-peril/
[20] Nate Woodall, "City of Melbourne Set to Vote on Security Camera Overhaul, Surveillance Powers for Staff," *ABC News*, October 8, 2025

are exempt from the Privacy Act 1988 (Cth), and companies contracting with the Victorian government may also be exempt but subject to other legislation.[21]

The council already operates a 300-camera-strong system, including about 18 privately owned cameras which feed into the council's monitoring operations.[22] The new privately owned cameras could include cameras installed by building owners as well as in "high-risk areas" such as government buildings and tobacconists.[23]

Currently, council-authorised officers cannot access CCTV footage for investigations into breaches of local laws; such footage may only be used by Victoria Police for criminal investigations.[24] However, the new plan allows authorised officers including security guards to be able to use the footage to investigate issues like illegal dumping, graffiti and public nuisance.[25]

At the meeting, Councillor Olivia Ball raised concerns about data ownership and accountability, asking whether private operators could retain copies of footage, how long recordings were kept, and whether the council's privacy policies would apply. Councillor Ball was told the council's policy of deleting the footage after 28 days would not apply to the private companies who own the cameras and that private companies would own the footage and could keep or duplicate the footage at will. [26]

Local councils such as Melbourne Council are subject to the Information Privacy Principles (IPP) Under the Privacy and Data Protection Act.[27] However there are exceptions for use and disclosure of data for law enforcement purposes, meaning the analysis and disclosure of the footage will be unregulated.[28] An impact assessment of the proposed expanded powers by law firm Maddocks found that the cameras would likely capture personal and potentially sensitive information.[29] Under IPP 10, local councils are prohibited from collecting sensitive information unless a specific exemption applies. None of the permitted exemptions include the use of CCTV for detecting misdemeanor crimes such as vandalism. Therefore,

[21] *Privacy Act 1988* (Cth) s 6D.

[22] Nate Woodall, "City of Melbourne Set to Vote on Security Camera Overhaul, Surveillance Powers for Staff," *ABC News*, October 8, 2025

[23] Ibid

[24] Ibid

[25] Ibid

[26] Ibid

[27] *Privacy and Data Protection Act 2014* (Vic) sch 1 IPP 2.1(d)–(g).

[28] *Privacy and Data Protection Act 2014* (Vic) sch 1 IPP 10.

[29] Ibid

the council's current CCTV practices result in the unlawful collection of sensitive personal information, in breach of IPP 10. The council has not addressed this issue.

Lord Mayor Nicholas Reece has floated using AI to analyse CCTV for facial identification to "tracking offenders' gait…or distinctive clothing items like a backpack."[30] It is unclear whether this technology would be applied to all security camera footage, including that of private camera footage, under the current proposed policy.

Lord Mayor Nicholas Reece justified his decision by pointing to other locations which are implementing similar AI technology.[31]

AI facial identification tech is faulty and racially biased.[32] Across facial recognition technology, people of colour, particularly from West Africa are consistently more likely to be misidentified as a match in facial surveillance systems, making them more likely to be inaccurately blamed for the offences caught on council CCTV cameras. In one commercially available system, people of West African descent were 25 times more likely to be misidentified.[33] The best system tested still misidentified individuals of west African descent 2.3 times more than other populations.

These AI fuelled accusations against West Africans in Melbourne could contribute to the villainisation of a minority group. Australia has already experienced 'moral panic' around African Gangs, with the media falsely labelling crimes as related to African gangs.[34] Unreliable AI facial identification will continue Australia's legacy of pointing the finger at Africans for crime[35]. Being falsely accused of crimes can result in serious stress and often incurs a financial cost as individuals navigate the legal system to prove their innocence. West African individuals are also more likely to experience language barriers as

[30] Nate Woodall, "City of Melbourne Set to Vote on Security Camera Overhaul, Surveillance Powers for Staff," *ABC News*, October 8, 2025

[31] Ibid

[32] National Institute of Standards and Technology, "Face Recognition Technology Evaluation: Demographic Effects in Face Recognition," accessed 3 November 2025,https://pages.nist.gov/frvt/html/frvt_demographics.html

[33] National Institute of Standards and Technology, "Face Recognition Technology Evaluation: Demographic Effects in Face Recognition," Irex_000, accessed 3 November 2025,https://pages.nist.gov/frvt/html/frvt_demographics.html

[34] Tebeje Molla, "Racial Moral Panic and African Youth in Australia," *International Journal of Intercultural Relations* 84 (2021): 95–106, https://www.sciencedirect.com/science/article/abs/pii/S0147176721001061

[35] Baak, Melanie. 2011. "Murder, Community Talk and Belonging: An Exploration of Sudanese Community Responses to Murder in Australia." *African Identities* 9 (4): 417–34. doi:10.1080/14725843.2011.614415.

approximately half of the population living in the greater Melbourne area were born overseas, compounding the stress of being falsely accused of a crime.[36][37][38]

Individuals from countries with authoritarian regimes or civilian oriented surveillance may be uncomfortable with having their political beliefs evidenced by CCTV footage and used in facial recognition technology. Already Chinese students in Melbourne report experiencing intense anxiety around expressing political beliefs, fearing surveillance.[39] This may deter certain diasporas from attending or organizing protests, reducing visibility of their causes.

The planned expansion of surveillance infrastructure by Melbourne City Council, particularly when combined with AI facial identification, will directly and disproportionately limit people's willingness to exercise their right to assemble. The knowledge that attendance at a protest may result in biometric capture, misidentification, and police attention shifts the protest environment from a democratic public square to a monitored and potentially punitive space. For people of colour, who are more likely to be wrongly identified and subjected to police intervention, the risks are even greater. As a result, AI-enhanced CCTV does not merely record protest activity. It actively shapes who feels safe to participate in democratic life.

Without strong accountability, human-rights safeguards, and limitations on the use of biometrics, Melbourne risks chilling lawful political expression and closing down the civic space on which a healthy democracy depends.

Case Study Three: Operation of Clearview AI in Australia

[36] Australian Bureau of Statistics, "People in Greater Melbourne who were born in Congo, Democratic Republic of – 2021 Census QuickStats," *ABS QuickStats*, accessed November 3, 2025,https://www.abs.gov.au/census/find-census-data/quickstats/2021/9108_2GMEL.

[37] Australian Bureau of Statistics, "People in Greater Melbourne who were born in Nigeria 2021 Census QuickStats," *ABS QuickStats*, accessed November 3, 2025,

[38] Australian Bureau of Statistics, "People in Greater Melbourne who were born in Ghana 2021 Census QuickStats," *ABS QuickStats*, accessed November 3, 2025,

[39] Human Rights Watch, *"They Don't Understand the Fear We Have": How China's Long Reach of Repression Undermines Academic Freedom at Australia's Universities*, June 30 2021. Available at:https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines

Clearview AI offers a facial recognition tool drawing from a database of over three billion images scraped without consent from the internet and social media.[40] Such indiscriminate scraping will inevitably include images from protests. The tool enables users to input a person's face and search for matches in the photo database. If a match is found Clearview informs the user where the photo appeared.[41] There have been two known contracts between Clearview and Australian Police forces.

In 2021 the Office of the Australia Information Commissioner (OAIC) found that Clearview had violated Australian privacy by 'scraping their biometric information from the web and disclosing it through a facial recognition tool'.[42] The OAIC found no legal basis for Clearview's argument that it did not deal with personal information and that being a US company it was beyond the Jurisdiction of the Privacy Act.

The OAIC determination made several declarations, including that Clearview must cease collecting images from Australia and destroy all Australian images currently in their database.[43] It is unclear whether Clearview has abided by these declarations. The OAIC has acknowledged this uncertainty but considers the evidence insufficient to reopen the investigation.[44]

Such uncertainty means activists cannot rely on legal protections being enforced and that their biometric data may remain in circulation indefinitely.

Clearview AI's scraping of biometric data from online images including those taken at protests poses a threat to the right to freedom of assembly and political expression in Australia. When individuals know that attending a protest could result in their face being captured, identified, and logged into a searchable database, they may choose not to participate. This creates a chilling effect, where people self-censor their movements and avoid political activity due to fear of being monitored or targeted.

[40] Clearview AI, "The Power of Facial Recognition in U.S. Federal Government," accessed November 6, 2025,https://www.clearview.ai/federal

[41] Australian Information Commissioner and Privacy Commissioner Angelene Falk, "Clearview AI breached Australians' privacy," Office of the Australian Information Commissioner, 3 November 2021, https://www.oaic.gov.au/news/media-centre/clearview-ai-breached-australians-privacy

[42] Australian Information Commissioner and Privacy Commissioner Angelene Falk, "Clearview AI breached Australians' privacy," Office of the Australian Information Commissioner, 3 November 2021, https://www.oaic.gov.au/news/media-centre/clearview-ai-breached-australians-privacy

[43] Office of the Australian Information Commissioner, *Commissioner-initiated investigation into Clearview AI, Inc (Privacy) [2021] AICmr 54*, Commonwealth of Australia. Available at: https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html

[44] Office of the Australian Information Commissioner (OAIC), *Statement on Clearview AI*, 24 August 2023. Available at: https://www.oaic.gov.au/news/media-centre/statement-on-clearview-ai

The use of Clearview AI poses heightened risks for refugees, migrants, and visa-dependent workers who cannot safely be associated with political dissent. For example, Chinese migrants in Australia have faced serious repercussions for expressing anti-CCP views or supporting Hong Kong's pro-democracy movement. Human Rights Watch has documented multiple cases in which Chinese police contacted the families of students in Australia after they criticised the Chinese government abroad.[45] If migrants are photographed at protests and their images are scraped into an international biometric database, facial recognition technologies could expose their identities, political views, and personal networks to foreign authorities. This risk extends not only to the individuals themselves but also to family members remaining in the country of origin.

A further example is the large number of photographs of individuals celebrating at Pride. These images often provide clear views of faces in a context that can disclose sensitive information such as sexual orientation. When combined with biometric matching, this places LGBTQ+ protesters at increased risk of harassment, discrimination, or violence.

If Australians had a right to delete, citizens could request that Clearview delete all the data held on them. This would prevent their political affiliations being exposed. This would remove some of the risks experienced by international activists in regards to their home government becoming aware of their political affiliations.

Clearview was used by the Australian Federal Police, until the OAIC began their investigation into Clearview. [46][47] Originally the AFP denied having any relationship with the company and rejected several FOI Requests on this basis. Internal documents later revealed that the AFP was utilizing Clearview technology.[48] The OAIC found that the AFP had "handl[ed] personal information in a way that could have serious consequences for individuals whose information was collected", consequently the AFP were found to have violated the Privacy Act.

[45] Human Rights Watch, "They Don't Understand the Fear We Have: How China's Long Reach of Repression Undermines Academic Freedom at Australia's Universities," June 30, 2021,https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines

[46] Bogle, A., 2020. *Australian Federal Police officers trialled controversial facial recognition tool Clearview AI*, ABC News, 14 April. Available at: https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894

[47] Australian Information Commissioner and Privacy Commissioner Angelene Falk, "Clearview AI breached Australians' privacy," Office of the Australian Information Commissioner, 3 November 2021, https://www.oaic.gov.au/news/media-centre/clearview-ai-breached-australians-privacy

[48] Bogle, A., 2020. *Australian Federal Police officers trialled controversial facial recognition tool Clearview AI*, ABC News, 14 April. Available at: https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894

Victoria Police Officers were also found to be using Clearview technology. This came to light after a freedom of information request found that Clearview was marketing directly to Victorian police officers, informing them that “Clearview is like Google Search for faces. Just upload a photo to the app and instantly get results from mug shots, social media, and other publicly available sources”.[49] Once the officers had made accounts they were instructed to “Search a lot. Your Clearview account has unlimited searches”.[50] Victoria Police have dedicated evidence gathering teams which often record at protests. Statements made by Victoria Police indicate this footage may be kept for up to 50 years.[51] Clearview AI would enable them to identify who is in the footage.

Police biometric identification enables long-term tracking of political involvement, allowing authorities to profile activists, map networks, and link a person’s image to their ideological stance. Over time, this shifts protests from democratic spaces of expression to sites of systemic monitoring and potential retaliation.

Clearview AI’s use is not confined to Australian law enforcement. Authorities in the United States,[52] New Zealand[53] and Ukraine[54], among others, have already integrated the technology into policing and immigration operations. Governments can use facial recognition to identify individuals at protests, including Australian protests, and infer their political beliefs, information that can then be used for intelligence screening, ongoing monitoring, or punitive action at borders. This risk is not hypothetical: U.S. Immigration and Customs Enforcement has already used Clearview AI to target undocumented immigrants, demonstrating how easily such technology can become a tool of coercion.[55] When Australians attend protests

[49] Stilgherrian, “Victoria Police Emails Reveal Clearview AI’s ‘Dodgy’ Direct Marketing,” *ZDNet*, February 14, 2020, https://www.zdnet.com/article/victoria-police-emails-reveal-clearview-ais-dodgy-direct-marketing/

[50] Ibid

[51] Jake Goldenfein, “Police Photography and Privacy: Identity, Stigma and Reasonable Expectation,” *UNSW Law Journal* 36, no. 1 (2013): 256–292, https://www.austlii.edu.au/cgi-bin/viewdoc/au/journals/UNSWLJ/2013/12.html

[52] Kashmir Hill, “The Facial-Recognition App Clearview Sees a Spike in Use after Capitol Attack,” *The New York Times*, January 9, 2021, https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html

[53] Mackenzie Smith, “Police Searched for Suspects in Unapproved Trial of Facial Recognition Tech, Clearview AI,” *RNZ*, May 15 2020,https://www.rnz.co.nz/news/national/416697/police-searched-for-suspects-in-unapproved-trial-of-facial-recognition-tech-clearview-ai

[54] Paresh Dave and Jeffrey Dastin, “Exclusive: Ukraine Has Started Using Clearview AI’s Facial Recognition During War,” *Reuters*, March 13 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/

[55] Peter Cohan, “How ICE Reportedly Uses Clearview AI to Target Immigrants,” *Inc.*, April 25, 2025, https://www.inc.com/peter-cohan/how-ice-reportedly-uses-clearview-ai-to-target-immigrants/91179292

overseas, or when foreign authorities gain access to images taken at local demonstrations, there is no clear limit on how that information may be used, shared or stored. The result is a climate of uncertainty in which attending a protest may expose individuals — and in some cases their family members — to surveillance consequences that cannot be foreseen or controlled. This uncertainty alone is enough to deter people from publicly exercising their democratic rights.

Tools like Clearview shift the protest environment from a public square to a surveillance space where consequences may follow long after the event. This undermines the democratic right to assemble without fear, and threatens the vibrancy of civil society.

Recommendations

Recommendation one: Facial Recognition Surveillance technology should not be used.

Facial recognition surveillance is unethical and should not be used. It invades the public's privacy, preventing anonymity. Facial recognition surveillance systems indiscriminately track and record the public's movements, providing no option to withdraw consent. A right to privacy and anonymity as people move through their towns and cities is crucial to protecting the right to assembly.

Recommendation two: Establish a Global Framework for AI Surveillance Safeguards

In a globalised information environment, weak privacy protections in any country create vulnerabilities for people everywhere. Companies can exploit these gaps by processing and storing biometric data in jurisdictions with little or no oversight, increasing the risk of data breaches, misuse, and cross-border surveillance. At present, most countries have no dedicated laws governing facial recognition or other AI powered surveillance technologies, allowing governments and corporations to deploy these systems without clear limits or accountability. To prevent a race to the bottom in privacy standards, the United Nations should establish strong, human-rights-based guidance for the lawful use of AI powered surveillance worldwide. Harmonised international rules would ensure that biometric data remains protected regardless of where it is handled, prevent exploitation of weak regulatory environments, and safeguard fundamental rights — including privacy, equality, and freedom of assembly — in every member state.

Recommendation three: Regulation of commercially available AI surveillance products.

The use of commercial surveillance products by government agencies must be strictly regulated. At present, departments and officers can adopt tools such as Clearview AI without independent oversight or robust privacy assessment. Before entering any contract with a biometric surveillance provider, the government should be required to conduct a formal evaluation addressing key questions:

1. Does the technology exhibit unacceptable levels of algorithmic bias? If bias is present to a degree where one demographic would be disadvantaged by the technology the technology should not be adopted.

2. Does the company have strong, verifiable data security and human-rights protections?

3. Do the anticipated public benefits outweigh the privacy and civil liberties risks?

If a company enables human rights abuses overseas, it has already demonstrated a willingness to prioritise commercial interests over human dignity and safety. Such an organisation cannot be trusted with Australian data, and any existing government contracts with them should be subject to immediate review and potential termination.

If any of these criteria cannot be satisfied, the technology should not be used under any circumstances. In addition, agencies must undergo regular, independent reviews of these tools to ensure ongoing compliance, provide transparency, and allow emerging concerns about human rights or security to be swiftly addressed.

Recommendation four: Transparency regarding the government use of surveillance tools

The public has a right to know when, where, and how surveillance technologies are being deployed upon them by government agencies. Currently, tools such as facial recognition, geolocation analytics, and commercial data-broker platforms can be procured and used without meaningful public disclosure. To safeguard the right to peaceful assembly, governments should be subject to mandatory transparency requirements covering:

- **Which surveillance tools are in use**, including vendor details and underlying capabilities
- **The legal basis for their use**, including warrant requirements, retention rules, and applicable exemptions
- **The specific contexts in which they are deployed**, such as crowd monitoring, border processing, or criminal investigations
- **Whether these tools are used on protest activity**, and if so, under what constraints
- **Arrangements for contracting and data sharing**, including with private companies or foreign authorities

Transparency enables civil society, journalists, and affected communities to scrutinise surveillance powers, identify emerging risks, and challenge unlawful or disproportionate use. It also allows activists to make informed decisions about protest participation and implement protective measures where necessary. Without clear visibility into state surveillance practices, the right to assembly becomes conditional on state secrecy rather than public accountability.