November 2025

Privacy International's Submission to the UN Special Rapporteur on freedom of peaceful assembly and of association regarding the thematic report "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects"

Introduction

Privacy International (PI) welcomes the opportunity to engage with the UN Special Rapporteur on freedom of peaceful assembly and of association regarding the call for input for the upcoming thematic report on "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects".[1]

PI is a non-governmental organisation that conducts research and advocates globally against government and corporate abuses of data and technology.[2] It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. In the following sections, PI seeks to answer some of the questions posed in the call for input.

I. Types of digital surveillance technologies being used, and their impact on the exercise of rights to freedom of peaceful assembly and association

Using digital surveillance technologies at protests interferes with the rights to freedom of assembly and association and other rights such as the rights to privacy and freedom of expression.[3] The UN High Commissioner for Human rights has confirmed this, concluding that "the use of [new] technologies to surveil or crack down on protesters [can lead to] … infringement of the right to peaceful assembly". Further still, unjustified interferences with these rights can lead to interference with other rights including freedom of movement,

[1] See: https://www.ohchr.org/en/calls-for-input/2025/call-input-hrc62-thematic-report-impact-digital-and-ai-assisted-surveillance
[2] See: https://www.privacyinternational.org/short-description/64/about-us
[3] UN Human Rights Council, Impact of New Technologies on the Promotion and Protection of Human Rights in the Context of Assemblies, including Peaceful Protests: Report of the United Nations High Commissioner for Human Rights, 24 June 2020, UN Doc A/HRC/44/24, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/35/PDF/G2015435.pdf?OpenElement

non-discrimination, as well as political participation, some examples of which we also provide below.[4]

PI and our partners[5] have been observing and documenting[6] the intrusive rise in digital surveillance technologies impacting the exercise of association and assembly rights (online and offline) through their deployment before, during and after protests or to target specific groups to stifle dissent, decrease civic space and undermine democratic values, which creates a chilling effect in society.[7]

Using digital surveillance technologies at protests today involves the acquisition, processing, generation, analysis, use, retention or storage of information about people engaging in protest just for participating in protests without any regard to whether they are suspected of wrongdoing.[8] The current deployment of these intrusive surveillance technologies is usually without a clear legal basis and without adequate safeguards and oversight mechanisms. Below we document some examples of technologies being deployed and their impact on the enjoyment of human rights.

Facial recognition technology (FRT)

We are observing governments and law enforcement deploying FRT at protests to identify, monitor and track protesters either openly or surreptitiously. In some cases, it is even used to aid the arrest, or detention of those participating in protests, or to build watch lists of protesters for intelligence purposes.[9]

Using FRT at protests has involved the deployment of FRT-enabled cameras by law enforcement to take pictures or videos of people attending the protest to identify them in real-time (live FRT) or at a later point (retrospective FRT).[10] However, even if a digital image of a protester is captured but a match is not found, these images could also potentially be used to create a new database or watch list of people who attend protests for future matching and identification purposes. Furthermore, police might use face-tracking technology[11] to follow an unidentified protester from a rally to their home or car, to identify

---

[4] UN Human Rights Council, "Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", (2019), UN Doc A/HRC/41/41, at para. 3, accessed online: https://undocs.org/A/HRC/41/41

[5] See: https://privacyinternational.org/where-we-work

[6] See: https://privacyinternational.org/examples/tracking-protest-surveillance; https://privacyinternational.org/long-read/5460/prosecuted-protesting. See also: UN Human Rights Council, "Protection of human rights in the context of peaceful protests during crisis situations", 16 May 2022, UN Doc A/HRC/50/42, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/343/05/PDF/G2234305.pdf?OpenElement

[7] Privacy International, 'Protest Surveillance', https://privacyinternational.org/learn/protest-surveillance.

[8] Ibid.

[9] Privacy International, How facial recognition technology can be used at a protest, May 2021, https://privacyinternational.org/explainer/4495/how-facial-recognition-technology-can-be-used-protest

[10] Privacy International, Facial recognition, https://privacyinternational.org/learn/facial-recognition

[11] Privacy International, How facial recognition technology can be used at a protest, May 2021, https://privacyinternational.org/explainer/4495/how-facial-recognition-technology-can-be-used-protest; see also Electronic Frontier Front, Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-time Tracking, and More, 7 October 2021, https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification

them with an address or license plate database. Police may also use face clustering technology[12] to create a multi-photo array of a particular unidentified protester and manually identify the protester by comparing that array to a database, where such manual identification would have been impossible based on a single photo of the protester.[13] To illustrate our concerns, we provide some examples of the use of FRT to restrict rights to assembly and association below.

In Hungary, in September 2025 the parliament passed amendments to the Assembly Act, the Infraction Act, and the Facial Recognition Technology Act to ban LGBTQI+ pride events and protests.[14] As well as directly threatening and enabling the deployment of FRT at such events to enforce the ban to identify and penalise those who attend. The Hungarian parliament took these measures despite it being a direct breach of Article 5 of the newly adopted EU AI Act which prohibits and restricts types and uses of FRT across Europe.[15] Not only does such use of FRT infringe on the rights to assembly, association and expression, it is also concerning that is being explicitly being used to target and penalise the LGBTQI+ community.

In Russia, FRT was reported to having been used to identify and track down a protester who held an individual demonstration in the Moscow underground, eventually leading to his arrest, which was taken to the European Court of Human Rights.[16] The police took screenshots of photos and a video of the protesters demonstration from social media, as well as collecting footage from CCTV installed in the stations of the Moscow underground, and several days later, used live FRT to locate and arrest him while he was traveling in the underground. The Court concluded that the processing of his personal data in the context of his peaceful demonstration, which had not caused any danger to public order or safety, had been particularly intrusive, and therefore incompatible with the ideals and values of a democratic society governed by the rule of law, in violation of both his privacy and protest rights.

In Austria, FRT was also used by police to later identify and prosecute someone who had attended a climate related protest in Vienna in March 2023.[17] Although it was later dropped due to police overreach at the protest.

---

[12] Ibid.
[13] Giulia Gabrielli, The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights', 15 May 2025, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/use-of-facial-recognition-technologies-in-the-context-of-peaceful-protest-the-risk-of-mass-surveillance-practices-and-the-implications-for-the-protection-of-human-rights/A4B2FABA8F32DDBC0217C86837CDBAC6#fn101
[14] The Guardian, Hungary bans Pride events and plans to use facial recognition to target attenders, 18 March 2025, https://www.theguardian.com/world/2025/mar/18/hungary-bans-pride-events-and-plans-to-use-facial-recognition-to-target-attenders
[15] European Centre for Not-for-Profit Law, Civil society urges the European Commission to uphold the AI Act in Hungary, https://ecnl.org/news/civil-society-urges-european-commission-uphold-ai-act-hungary
[16] *Glukhin v. Russia* (2023) ECtHR. See: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-225655%22]}
[17] Vol.at, 'Data Protection Advocates Criticize Use of Facial Recognition at Climate Demonstration in Vienna', 25 June 2025, https://www.vol.at/data-protection-advocates-criticize-use-of-facial-recognition-at-climate-demonstration-in-vienna/9504071

Another strategy increasingly pursued by governments to enable the use of FRT as a surveillance tool at protests, is to introduce bans around people wearing face coverings at protests which further curtails their rights and reasserts this chilling effect.

For example, FRT was reported to having been used during Hong Kong's pro-democracy demonstrations in 2019 to suppress and deter people from protesting around fears that participating could result in arrests or other consequences, like being barred from future work or school opportunities.[18] As a result, protesters used measures such as wearing masks, goggles and using face paint to omit detection. This led to Chinese authorities using legislation called the Emergency Regulations Ordinance to enact a ban on face coverings in October 2019.[19]

In the UK, the Crime and Policing Bill introduced to parliament in 2024 includes proposals to make it a criminal offense to wear a face covering that would conceal their or another person's identity when in an area that a protest is taking place.[20] The offense will carry a maximum penalty of one month imprisonment, a £1000 fine, or both. Although the Bill does not explicitly state that the purpose of this provision is to enable FRT, it is widely implied.

A similar approach has been taken in Kazakhstan. In 2025 an amendment to the country's prevention of offenses law bans face coverings in public spaces, which is reported to explicitly state "it is prohibited to wear clothing items in public places that impede facial recognition".[21]

Social media monitoring (SOCMINT)

People are increasingly using social media to organise protests, communicate with fellow protestors, and upload photos and videos of protests, which is why the use of social media monitoring in the context of protests by governments is raising concerns for the enjoyment of freedom of assembly and association.

Social media monitoring refers to the monitoring, gathering and analysis of information shared on social media platforms, such as Facebook, Twitter, Instagram and Reddit.[22] Law enforcement can 'data mine' these social media pages, gathering information to target specific groups to learn the identities and affiliations of the organisers, the

---

[18] UAB Institute for Human Rights Blog, The Abuse of Facial Recognition Technology in the Hong Kong Protests, 13 February 2025, https://sites.uab.edu/humanrights/2025/02/13/the-abuse-of-facial-recognition-technology-in-the-hong-kong-protests/

[19] BBC News, Hong Kong protests: Authorities to announce face mask ban, 3 October 2019, https://www.bbc.co.uk/news/world-asia-china-49918889

[20] UK Home Office, Policy paper: Crime and Policing Bill: public order offences factsheet, https://www.gov.uk/government/publications/crime-and-policing-bill-2025-factsheets/crime-and-policing-bill-public-order-factsheet

[21] Euro News, Kazakhstan bans face coverings in public places, 2 July 2025, https://www.euronews.com/2025/07/02/kazakhstan-bans-face-coverings-in-public-places

[22] Privacy International, Social media surveillance, https://privacyinternational.org/learn/social-media-surveillance

location and timing of a planned action, and other related information.[23] By systematically collecting and analysing this data, law enforcement can build a detailed and permanent record of protesters and activists lives - their views, their connections and locations. [24]

SOCMINT has the potential to be used as a mass surveillance tool to create digital dossiers on individuals before determining their relevance or role in a particular protest has even been determined. For example, in 2019 it was reported that police in London monitored around 9,000 activists using data scraped from social media platforms.[25] Secret dossiers were compiled on each activist, despite many of them having no criminal background.[26]

SOCMINT has also been reported as being used as a tactic by the US government, as they have been relying on AI to scrape people's social media to revoke visa applications of people who have been protesting Israel's ongoing genocide in Gaza.[27] It has been reported that as of early April 2025 at least 600 people have apparently had their visas revoked through the use of SOCMINT. This demonstrates the possible consequences that attending protests or associating with certain causes can have on wider rights, while also deterring people from attending future protests for fear of reprisals.[28]

SOCMINT can also be used as a form of digital surveillance to predict and deter protests before they happen. Research by Gabriel Grill from 2021 examined the research, products and discourses of civil unrest predictions based on social media data. The research found that most civil unrest predictions targeted "all kinds of protests", marking them as risky which could result in various detrimental treatments such as pre-emptive interventions, policing, increased surveillance, and targeting of individuals and groups.[29]

International Mobile Subscriber Identity (IMSI) Catchers

International Mobile Subscriber Identity or an 'IMSI catcher' is a device that locates and then tracks all mobile phones that are connected to a phone network in its vicinity, by 'catching' the unique IMSI number.[30] It does this by pretending to be a mobile phone tower, tricking mobile phones nearby to connect to it, enabling it to then intercept the data from that phone to the cell tower without the phone user's knowledge.[31] The police

---

[23] Privacy International, How social media monitoring can be used at a protest, May 2021, https://privacyinternational.org/explainer/4509/how-social-media-monitoring-can-be-used-protest
[24] Ibid.
[25] Freedom House, Social Media Surveillance, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance
[26] Ibid.
[27] Petra Molnar, Tech Policy Press, Trump's Social Media Surveillance: Social Scoring by Another Name, 21 April 2025, https://www.techpolicy.press/trumps-social-media-surveillance-social-scoring-by-another-name/
[28] The Guardian, US government has revoked more than 600 student visas, data shows, 10 April 2025, https://www.theguardian.com/us-news/2025/apr/10/how-many-student-visas-revoked
[29] Gabriel Grill, Future Protest Made Risky: Examining Social Media Based Civil Unrest Prediction Research and Products, 8 September 2021, https://pubmed.ncbi.nlm.nih.gov/34511729/
[30] Privacy International, IMSI Catchers, 6 August 2018, https://privacyinternational.org/explainer/2222/imsi-catchers
[31] Ibid.

have the potential to use IMSI catchers to identify who was at a protest, by capturing the IMSI numbers of all the phones that were in its vicinity at that protest. They can be used to monitor or block calls and messages; edit your messages without your knowledge; or even write and send someone messages pretending to be from you.[32] IMSI catchers are usually deployed in secret, sometimes without a clear legal basis, and without appropriate safeguards and oversight mechanisms.

IMSI catchers have allegedly been used to target Black Lives Matter protesters[33], becoming another example of a surveillance tool used to over-police ethnic minorities participating in protests.[34] While it is not clear whether IMSI catchers were deployed during the protests following George Floyd's murder, Minnesota authorities had the ability to deploy IMSI catchers.[35] As do other states across the US.[36]

In the UK PI has been calling for transparency over the use of IMSI catchers for years to no avail.[37]

There are numerous reports about tech companies selling IMSI catchers not only legally but also, on the black market to oppressive regimes around the globe. In 2016, a Hong Kong-based tech company, HK Medsourcing, reportedly offered to sell an IMSI catcher for $15,000 to Vice Motherboard reporters posing as businessmen if they assured him they were using the device legally.[38]

PI conducted a legal analysis of the use of IMSI catchers in which we break down how the intrusive and unregulated use of IMSI catchers creates a chilling effect on civic society and infringes on our right to privacy, freedom of expression, and freedom of assembly and association.[39]

Mobile Phone Extraction (MPE)

---

[32] Privacy International, How IMSI catchers can be used at a protest, 5 May 2021, https://privacyinternational.org/explainer/4492/how-imsi-catchers-can-be-used-protest

[33] CBS News, Activists Say Chicago Police Used 'Stingray' Eavesdropping Technology During Protests, 6 December 2014, https://www.cbsnews.com/chicago/news/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/

[34] Privacy International, Ethnic minorities at greater risk of oversurveillance after protests, 15 June 2020, https://privacyinternational.org/news-analysis/3926/ethnic-minorities-greater-risk-oversurveillance-after-protests

[35] Buzzfeed, Here Are The Minneapolis Police's Tools To Identify Protesters, 29 May 2020, https://www.buzzfeednews.com/article/carolinehaskins1/george-floyd-protests-surveillance-technology

[36] See: https://privacyinternational.org/sites/default/files/2019-09/Nathan%20Wessler%20Witness%20Statement%20-%20redacted.pdf

[37] Privacy International, Remember those IMSI catchers? UK authorities play hide and seek with use of intrusive surveillance technology, 20 January 2023, https://www.privacyinternational.org/news-analysis/5206/remember-those-imsi-catchers-uk-authorities-play-hide-and-seek-use-intrusive

[38] Vice, The Black Market Dealers Selling Tactical Surveillance Equipment Online, 15 January 2016, www.vice.com/en_us/article/wnx57m/the-black-market-dealers-selling-state-surveillance-equipment-online

[39] Privacy International, IMSI catchers: PI's legal analysis, 25 June 2020, https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis

MPE tools enable police and other authorities to download content and associated data from people's phones including device information, phonebooks, call logs, texts, videos and photos, audio files, emails and other information.[40] The use of MPE is being used by governments against human rights defenders and activists as a more targeted measure to curtail the exercise of freedom of assembly and association. Increasingly, MPE has reportedly been used against activists to collect and uncover information and intelligence about them to charge them with a variety of crimes as part of wider efforts to crackdown on those speaking out against a government and to suppress dissent. For example, a MPE tool provided by Israeli-based Cellebrite was identified to have been used by Hong Kong police to search the device of Joshua Wong, a pro-democracy leader.[41]

In 2020, MPE was reported to also have been used in Venezuela with further evidence emerging in 2021 when the General Directorate of Military Counterintelligence (DGCIM) publicly said on national television that it has used Cellebrite's MPE tool[42,] Universal Forensic Extraction Device (UFED) for law enforcement purposes.[43] It has also been reported that Cellebrite's UFED was used against Mohammed al-Singace, a political activist in Bahrain, and the information collected was used as part of legal proceedings to prosecute him as evidence of criminal association.[44]

II. The Chilling Effect

Protest surveillance enables significant power imbalances and hinders people's autonomy and dignity and creates an atmosphere of fear around speaking out. It creates an environment of suspicion and threat, which can cause people who are not engaged in any wrongdoing to change their behaviour, including the way they act, speak and communicate.

The above use of digital surveillance technologies to target and monitor protesters and specific groups is evidentially having a chilling effect on the exercise of freedom of assembly and association and other rights. When people are aware that their conversations, likes and associations are being monitored, and may form part of a record, they may self-censor out of fear that the information may be misinterpreted or

---

[40] Privacy International, How the police can gain access to your phone's content at a protest, 15 June 2021, https://privacyinternational.org/explainer/4504/f2p42-how-police-can-gain-access-your-phones-content-protest

[41] Quartz, Hong Kong's mass arrests are giving police crucial intelligence: people's phones, 21 July 2022, https://qz.com/1844937/hong-kongs-mass-arrests-give-police-access-to-phones

[42] See: https://privacyinternational.org/taxonomy/term/584

[43] Haaretz, Israeli Phone-hacking Firm Cellebrite Vowed Not to Sell to Sanctioned Countries. So What's It Doing in Belarus?, 18 August 2020, https://www.haaretz.com/israel-news/2020-08-18/ty-article/.premium/whats-israeli-phone-hacking-firm-cellebrite-doing-in-sanctioned-belarus/0000017f-e198-d75c-a7ff-fd9dff0b0000 & Proyecto ITEMP, Behind the Resale of Cellebrite Technology That Can Hack Your Phone, 20 February 2022, https://www.itempnews.org/2022/02/20/cellebrite-hacking/

[44] The Intercept, Phone cracking Cellebrite software used to prosecute tortured dissident, https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/

used against them.[45] Consequently, individuals may refrain from criticising authorities, engaging in controversial debate or accessing certain information.

This fear and self-censorship directly interfere with an individual's ability to exercise their freedom of association and assembly rights as people may become hesitant to join an online group, sign a petition or express interest in a protest. Activists, journalists and human rights defenders who aim to hold government to account may be more inclined to self-censor, undermining their role in holding the state and other actors accountable, a vital role that they play in a democratic society.[46] Such conformity and self-censorship discourages participation in political discourse, shrinks the space for dissent and ultimately creates a chilling effect in society.

Members of certain communities are disproportionately harmed by these digital surveillance practices in violation not only of their exercising of freedom assembly and association but leading to discrimination and exacerbating existing inequalities of already marginalised communities including people from ethnic minorities, women and people with disabilities.[47] Digital surveillance technologies can be trained on under representative data sets, biased training data, and/or include implicit bias of coders and designers. There is also a lack of transparency and accountability around these. Overall, these can embed issues such as inherent racism within these technologies,[48] even if not intentional, structural racism can be embedded in the design and implementation of the technology.[49]

Furthermore, some of these communities are often already subject to greater scrutiny from law enforcement, and the use of digital technologies contributes to a surveillance cycle where they are monitored more intensely, their data is interpreted more negatively, and they are flagged for suspicion at a much higher rate.[50]

III. Recommendations and safeguards

As a general remark, PI believes that the use of digital and AI-surveillance to restrict peaceful assembly and association, poses significant risks to human rights, risks that in certain cases cannot be adequately mitigated. As a result, governments should not design or deploy digital and AI-assisted surveillance that would interfere with assembly

---

[45] Freedom House, Social Media Surveillance, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance
[46] Ibid.
[47] Privacy International, Ethnic minorities at greater risk of oversurveillance after protests, 15 June 2020, 15th June 2020, https://privacyinternational.org/news-analysis/3926/ethnic-minorities-greater-risk-oversurveillance-after-protests &
Electronic Privacy Information Centre, Privacy & Racial Justice, https://epic.org/issues/democracy-free-speech/privacy-and-racial-justice/
[48] Eduwik, How AI Bias Affects Marginalized Communities, 5 August 2025, https://eduwik.com/how-ai-bias-affects-marginalized-communities/
[49] ACLU Minne, Biased Technology: The Automated Discrimination of Facial Recognition, 29 February 2024, https://www.aclu-mn.org/en/news/biased-technology-automated-discrimination-facial-recognition
[50] Report of the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, UN Doc. A/HRC/56/68, paras 9-19, https://docs.un.org/en/A/HRC/56/68

and association rights without having first demonstrated their capacity to comply with existing human rights law.

It is difficult to see how the use of some of these digital technologies that enable mass surveillance could ever comply with international human rights standards, due to their indiscriminate nature. For example, PI maintains that live FRT should never be deployed at protests as it amounts to a mass surveillance tool and therefore will always be indiscriminate and disproportionately interfere on individual's rights.[51] This position is shared by the UN High Commissioner for Human Rights who has recommended that States "[n]ever use facial recognition technology to identify those peacefully participating in an assembly".[52]

These recommendations align with the position previously taken by this mandate holder that *"surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision*" and hence recommended that "*indiscriminate and untargeted surveillance" both online and offline should be outlawed*.[53] Furthermore, the UN High Commissioner for Human rights has also stated that the use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited.[54]

If any use of digital surveillance during protests for targeted purposes is to be considered, this should only be in extremely limited circumstances and should only be used in a manner that complies with international and national human rights law, as well as other relevant legislation and standards. This includes being subject to the overarching principles of legality, necessity and proportionality. Restrictions and safeguards on its use must be clearly defined in primary legislation, before any technology is deployed to prevent abuse. They should also ensure this considers the entire lifecycle of the technology from its procurement to deployment.

PI previously responded to a call for input on the development of practical tools to assist law enforcement bodies in promoting and protecting human rights

---

[51] PROTECTING HUMAN RIGHTS AT PEACEFUL PROTESTS: PI's submission to Special Rapporteur on freedom of assembly, January 2024, https://privacyinternational.org/sites/default/files/2024-01/2023.04.05%20Privacy%20Internationals%20Response%20to%20SR%20on%20FoA.pdf

[52] An important legal case which highlights the significance of the legal safeguards outlined above, at paras. 2.3 – 2.5 is *Bridges* v *South Wales Police*. The UK Court of Appeal held that a police force's deployment of automated facial recognition technology (AFRT) was not "in accordance with the law", particularly because the police powers to deploy the technology (who was it going to be deployed against and where it would be deployed) was left to the discretion of individual police officers. As a result, the polices' use of AFRT was found to be a violation of the applicant's right to privacy under Article 8 of the European Convention on Human Rights. *R (on the application of Edward Bridges)* v *South Wales Police* [2020] EWCA Civ 1058, paras 81–94, https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

[53] A/HRC/41/41, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, 17 May 2019, para 57.

[54] See: https://www.ohchr.org/en/press-releases/2020/06/new-technologies-must-serve-not-hinder-right-peaceful-protest-bachelet-tells

in the context of peaceful protests, in which PI outlined recommendations that should apply to surveillance undertaken by law enforcement at every stage of a protest.[55] We invite the Special Rapporteur to consider the measures we had put forward in our submission in order to facilitate the exercise of the right to freedom of peaceful assembly and protect the rights of groups particularly at risk in the context of protests including prohibiting discriminatory surveillance practices, banning predictive policing technologies, and ensuring public consultations before acquiring new technologies, amongst others.

PI calls on the Special Rapporteur to provide explicit guidance regarding safeguards and restrictions on the use of how targeted digital surveillance technologies, if permitted, can be used in a way that does not interfere with freedom of assembly and association and other rights including the right to privacy.

[55] PROTECTING HUMAN RIGHTS AT PEACEFUL PROTESTS: PI's submission to Special Rapporteur on freedom of assembly, January 2024, https://privacyinternational.org/sites/default/files/2024-01/2023.04.05%20Privacy%20Internationals%20Response%20to%20SR%20on%20FoA.pdf