PRIVACY INTERNATIONAL

Protecting civic spaces

Defending democracy and dissent

May 2019

Protecting Civic Spaces

Imagine that every time you want to attend a march, religious event, political meeting, protest, or public rally, you must share deeply personal information with police and intelligence agencies, even when they have no reason to suspect you of wrongdoing. First, you need to go to the police to register; have your photo taken for a biometric database; share the contacts of your family, friends, and colleagues; disclose your finances, health records, lifestyle choices, relationship status, and sexual preferences; turn over your emails and text messages; provide access to your Internet browsing history and third-party applications ("apps"); allow police to track your movements in real-time; and transmit all data stored on your cell phone, including patterns of behaviour you may not even be aware of and data you had previously deleted. Second, while at the event, you must let the police look over your shoulder at everything you do on your phone. Third, all that information will then be catalogued in a database that police and intelligence agencies can search and analyse at any time. Would you still feel comfortable exercising your rights to freedom of expression, religion, assembly and association?

Police and intelligence agencies are already capable of conducting generalised, invisible, real-time surveillance of civic spaces, from a distance, without people knowing or consenting. Civic spaces are the digital and real-life settings where people formulate ideas, discuss them with like-minded people and groups, raise dissenting views, consider possible reforms, expose bias and corruption, and organise to advocate for political, economic, social, environmental, and cultural change. Civic spaces include public streets, squares, and parks, as well as digital spheres including the Internet, messaging apps, and social media platforms. Police and intelligence agencies can extract information on a widespread scale from these civic spaces, and then create granular, searchable archives of the people who participate in them.

The current unregulated uses of surveillance technologies in civic spaces violate peoples' right to privacy and can hinder their ability to freely communicate, organise, and associate with others.[1] The right to privacy thus supports other fundamental rights and freedoms of democratic societies, including: the right to equal participation in political and public affairs, and the freedoms of opinion, expression, peaceful assembly, and association. Privacy creates spaces for people to develop and debate ideas and exercise these rights and freedoms. In private spaces, members of minority groups who may fear discrimination or harassment on the basis of their ethnicity, race, religion, sexual orientation, or gender identity can be empowered to express their opinions and cooperate to advance objectives that may be overlooked by majority groups.

Privacy also allows the press and possible whistle-blowers to hold those in power accountable without fear of retaliation. Privacy and the rights and freedoms it supports are critical restraints against unbridled government power and coercion. They require that the

[1] Privacy International, "What is privacy?", available at https://privacyinternational.org/explainer/56/what-privacy.

government remain answerable to its citizens and that the collective will of the people can evolve and be translated into law and policy. Without privacy, this democratic process cannot endure.

Privacy International (PI) is working to ensure new technologies are governed and used in ways that protect our privacy, preserve our civic spaces, and support democracy.

WHAT IS THE PROBLEM?

Police and intelligence agencies are expanding the depth and breadth of their surveillance of our civic spaces, often without sufficient legal basis or democratic input and oversight. While new technologies may be deployed under the guise of protecting democratic society, without adequate regulations and safeguards, those technologies can threaten democratic participation and dissent and thereby undermine democracy itself. This is not to say that new technologies should never be used: their use should be regulated, transparent, targeted based on reasonable suspicion, designed to minimise impact on our digital security, and subject to effective and independent control and supervision.

Surveillance technologies are capable of intruding on civic spaces on an unprecedented scale

New surveillance technologies are radically transforming the ability of police and intelligence agencies to monitor our civic spaces and collect, categorise, store, analyse, and share our personal data. PI is particularly concerned about technologies that police and intelligence agencies can, and sometimes do, already use to monitor people who have not committed nor are suspected of any crime and instead are exercising the rights essential to their participation in democracy. These technologies include: mass surveillance[2], IMSI catchers[3], remote hacking[4], mobile phone extraction[5], social media monitoring[6], facial recognition cameras[7], and predictive policing[8].

These technologies can chill and violate peoples' exercise of fundamental freedoms

When used together and improperly regulated, these surveillance technologies function as a panopticon, where no one can know whether, when, where, and how they are under surveillance. The omnipresence of these technologies disrupts our public spaces and could

[2] Privacy International, "Mass Surveillance", available at https://privacyinternational.org/topics/mass-surveillance.

[3] Privacy International, "IMSI catcher explainer", available at https://privacyinternational.org/explainer-graphic/2728/imsi-catcher-explainer.

[4] Privacy International, "Police hacking explainer", available at https://privacyinternational.org/explainer-graphic/2714/police-hacking-explainer.

[5] Privacy International, "Police mobile phone extraction explainer", available at https://privacyinternational.org/explainer-graphic/2717/police-mobile-phone-extraction-explainer.

[6] Privacy International, "Social media intelligence (SOCMINT) explainer", available at https://privacyinternational.org/explainer-graphic/2721/social-media-intelligence-socmint-explainer.

[7] Privacy International, "Facial recognition cameras explainer", available at https://privacyinternational.org/explainer-graphic/2725/facial-recognition-cameras-explainer.

[8] Privacy International, "Predictive policing explainer", available at https://privacyinternational.org/explainer-graphic/2719/predictive-policing-explainer.

have a chilling effect as it dissuades people from using civic spaces to exercise their rights. These privacy intrusions are problematic regardless of whether or not you believe you have nothing to hide: they violate your rights and the rights of others.

The use of these technologies can interfere with peoples' rights to express themselves anonymously, formulate and share their thoughts, engage in controversial dialogue, attend public gatherings, and seek redress of grievances against the government. People may self-censor their thoughts, words, and actions: people may avoid visiting certain social media profiles; liking, sharing, re-tweeting controversial posts; joining certain discussion groups; or even using certain words. Ultimately, this self-censorship can change how people seek out new information, develop and discuss ideas, and organise around them. Important issues may not be adequately reported on. We all benefit from the exchange of ideas and peoples' ability to organise and petition for change, and we all suffer when people are less free to do so.

Surveillance technologies are being used in a legal and regulatory vacuum

Laws and regulations are not keeping pace with technological developments to provide effective safeguards or oversight. While people are rightly increasingly concerned with the ways data analytics can be employed to profile voters, micro-target advertisements, exert undue influence on voting decisions, and potentially swing elections, we also need to address other ways in which our democracies are vulnerable.[9] In addition to ensuring that voters' choices are their own, to protect the integrity of democratic institutions, we also need to ensure that individuals can exercise their fundamental rights to develop and share ideas, organise, and protest without unlawful interference by the state authorities.

Most of these surveillance technologies have been deployed in the absence of laws and regulations which provide precise, clear and public parameters for the use of such technologies, including independent authorisation and oversight. In some cases, police are being left to self-regulate their behaviour, which does not ensure consistency between jurisdictions, guarantee legality or best practices, or inspire public confidence.[10] These concerns about legality and the dearth of regulation have formed the basis of many of PI's legal interventions challenging the use of these technologies.[11] Without strong legal safeguards, governments can, at any time, change how they use surveillance technologies and the data they generate.

There is risk of abuse by government

Surveillance technologies are ripe for abuse because of the lack of transparency surrounding their use and the highly sensitive nature of the data they collect. These technologies give the government a wealth of information it could use to selectively prosecute activists and dissenters, and thereby chill protests and other expressions of criticism against the

[9] Privacy International, "Data Exploitation and Democratic Societies", 1 May 2019, available at https://privacyinternational.org/feature/2850/data-exploitation-and-democratic-societies; Privacy International, "Data and Elections", available at https://privacyinternational.org/topics/data-and-elections.

[10] Privacy International, "Digital stop and search: how the UK police can secretly download everything from your mobile phone", available at 27 March 2018, available at https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile.

[11] Privacy International, "Legal Work", available at https://privacyinternational.org/how-we-fight/legal-work.

government. In the US, there is a history of the Federal Bureau of Investigation conducting surveillance against civil rights leaders, such as Martin Luther King Jr.[12], to undermine them, and these tactics have extended to recent surveillance of Black Lives Matter and Standing Rock activists.[13] In the UK, police also have a history of infiltrating and spying on advocacy groups.[14] In Mexico, it was reported that Mexican authorities used NSO Group's Pegasus spyware to target journalists and human rights defenders working to expose government corruption and human rights abuses.[15] Before that, a massive scandal in North Macedonia revealed that the phone calls of some 20,000 activists, lawyers, opposition members, journalists, civil servants, business people, and even members of the government had been unlawfully monitored.[16] In addition, police or intelligence agents could be tempted to use these technologies illegally, such as by spying on former romantic partners or whistleblowing officers alleging racial discrimination.[17] We need to prevent the government using surveillance technologies against activists and people exercising their rights to bring concerns to the government's attention.

These technologies allow discrimination and can disproportionately exclude some groups from civic spaces

Surveillance technologies can be used to disproportionately target and impact vulnerable groups and racial, ethnic, and religious minorities. For example, police and intelligence agencies could subject minorities and immigrants to a higher level of scrutiny without any reason to suspect members of such groups of wrongdoing. This has happened in the past. In the United States, the now defunct National Security Entry-Exit Registration System (NSEERS) required people from 25 Muslim-majority countries, plus North Korea, to register with the government when they entered and existed the country; however, the structure of this

[12] Federal Bureau of Investigation (FBI), The King Encyclopedia, The Martin Luther King, Jr. Research and Education Institute, available at https://kinginstitute.stanford.edu/encyclopedia/federal-bureau-investigation-fbi.

[13] George Joseph, "Exclusive: Feds regularly monitored black lives matter since Ferguson", The Intercept, 24 July 2015, available at https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/; Alleen Brown, Will Parrish and Alice Speri, Standing rock documents expose inner workings of 'surveillance-industrial complex', The Intercept, 3 June 2017, available at https://theintercept.com/2017/06/03/standing-rock-documents-expose-inner-workings-of-surveillance-industrial-complex/.

[14] Rob Evans, "UK political groups spied on by undercover police – search the list", The Guardian, 13 February 2019, available at https://www.theguardian.com/uk-news/ng-interactive/2018/oct/15/uk-political-groups-spied-on-undercover-police-list.

[15] Privacy International, "International Human Rights Implications of Reported Mexican Government Hacking Targeting Journalists and Human Rights Defenders", Briefing, 28 June 2017, available at https://privacyinternational.org/sites/default/files/2017-12/Briefing%20on%20the%20International%20Human%20Rights%20Implications%20of%20Reported%20Mexican%20Government%20Hacking%20Targeting%20Journalists%20and%20Human%20Rights%20Defenders.pdf.

[16] Privacy International, "Macedonia: Society On Tap", 23 March 2016, available at https://privacyinternational.org/feature/1120/macedonia-society-tap.

[17] Jason Lewis, "Hundreds of police officers caught illegally accessing criminal records computer", The Telegraph, 20 August 2011, available at https://www.telegraph.co.uk/news/uknews/crime/8713194/Hundreds-of-police-officers-caught-illegally-accessing-criminal-records-computer.html; "High-ranking police officers censured for data breaches", BBC News, 11 February 2014, available at https://www.bbc.co.uk/news/uk-england-26136754; Paul Peachey, "Police 'used terror powers to spy on officers blowing whistle on racism'", Independent, 3 January 2016, available at https://www.independent.co.uk/news/uk/crime/police-accused-of-using-terror-powers-to-spy-on-officers-blowing-whistle-on-racism-a6795036.html.

program still exists and it could be reinstated.[18] The Trump administration recently asked technology companies to help employ artificial intelligence to engage in a process of "extreme vetting" of prospective immigrants to assess whether they posed terrorist threats, but then dropped such plans in response to widespread public criticism.[19] Minority groups, often marginalised and lacking the means to defend themselves, are in most need of civic spaces to express themselves and help each other.

There is not enough transparency or public input into how surveillance technologies can, should, or are being used

Police and intelligence agencies have been using these technologies without adequate public consultation, and sometimes without even consulting the public at all. You have had insufficient input into whether the government should be buying these intrusive technologies or how these technologies can be used. At the same time, you do not have the ability to refuse being monitored.

The use of these technologies prioritises corporate profits over peoples' privacy

Corporations are selling these costly technologies to police and intelligence agencies. It is unclear to what extent companies have access to the data these technologies extract, but what is clear is that this is a highly profitable industry that can create perverse incentives for collecting and examining more and more data.[20] For example, IBM, Microsoft, Cisco, Oracle, and Palantir offer to help police sort and make use of the oceans of data these technologies extract.[21] There are risks inherent to making these types of databases available to corporations.

The data collected through these technologies could fall into the wrong hands

No data can be completely secure: once we store data, it becomes vulnerable to a breach due to accident, carelessness, an insider threat, or a hostile opponent. Poor practices on handling the data can undermine the prosecution of serious crimes, as well as result in the loss of files containing intimate details of people who were never charged.[22] The more data the government collects and stores, the more valuable such databases become. Malicious actors

---

[18] Kaveh Waddell, "America Already Had a Muslim Registry", The Atlantic, 20 December 2016, available at https://www.theatlantic.com/technology/archive/2016/12/america-already-had-a-muslim-registry/511214/.

[19] Drew Harwell and Nick Miroff, "ICE just abandoned its dream of 'extreme vetting' software that could predict whether a foreign visitor would become a terrorist", The Washington Post, 17 May 2018, available at https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/?noredirect=on&utm_term=.c5c030ee3b2e.

[20] Privacy International, "The Global Surveillance Industry", available at https://privacyinternational.org/explainer/1632/global-surveillance-industry.

[21] Privacy International, "101: Integrated Policing", available at https://privacyinternational.org/explainer/29/101-integrated-policing.

[22] "Report on Police Scotland's proposal to introduce the use of digital device triage systems (cyber kiosks)", Justice Sub-Committee on Policing, The Scottish Parliament, 8 April 2019, SP Paper 512, available at https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2019/4/8/Report-on-Police-Scotland-s-proposal-to-introduce-the-use-of-digital-device-triage-systems--cyber-kiosks-/JSPS052019R01.pdf.

could exploit such data to interfere in, among other things, the democratic election cycle, the justice system, or with freedom of the press.

WHAT IS THE SOLUTION?

The purchase, use, and scope of these surveillance technologies should be explicitly **prescribed by clear and precise law and limited to the means necessary and proportionate to achieving legitimate aims**. Mass surveillance, including bulk collection of peoples' data from civic spaces, cannot satisfy the requirements of necessity and proportionality. Any targeted surveillance measures, including in public spaces, must be necessary and proportionate to achieve a legitimate aim, such as preventing or investigating serious crimes. People should be able to understand how laws might be applied, what kinds of data might be collected about them, and how that data will be stored.

For the public to be assured there is no risk of government abuse, there must be **adequate safeguards and effective oversight around the trial, purchase, and use of surveillance technologies**.

Prior to each time these technologies are used, the government should be required to get a **search warrant based on reasonable suspicion from an independent judicial authority**. Search warrants should ensure that the people and places searched are limited to those where the government has sufficient legal justification to do so (based on probable cause or reasonable suspicion, as appropriate) and do not constitute bulk collection of peoples' data. To prevent overly intrusive searches, warrants can also exclude certain places from being searched or certain data from being collected. After each search, a reviewing court should be able to examine whether it was lawful.

The government needs to **protect the security of the data** it collects. Any information that is beyond the scope of a warrant, irrelevant, or immaterial should not be stored, categorised, or analysed; instead, it should be immediately destroyed. All actions the government takes with respect to such data should be recorded.

People who are subject to unlawful uses of surveillance technologies or collection of data should have access to an **effective remedy**.

There must be **greater transparency and accountability** around the government's use of surveillance technologies. The government should justify the acquisition and use of these technologies and prove to the public that these technologies are not used in a way that is discriminatory, disproportionate or otherwise unlawful.

To **curb corporate interests in maximising profits at the expense of peoples' privacy and other rights**, the government should make publically available any solicitation letters, purchase orders, invoices, contracts, loan agreements, and correspondence with companies regarding acquisition of these technologies.

Finally, to allow for greater protection of peoples' data, the government should support the development and use of **encryption**. The government should be prohibited from requiring

corporations to engineer vulnerabilities in products or services that would undermine peoples' privacy and security.

WHAT PI IS DOING

PI is engaged in advocacy, research, campaigns, strategic litigation, technical analysis, and work with partners in our International Network to:

- **Challenge surveillance practices that violate peoples' rights and freedoms**. We are contesting the UK intelligence agencies' unlawful bulk collection of data and other mass surveillance and UK-US intelligence sharing practices.[23]
- **Increase transparency around the use of these surveillance technologies**. We promote mechanisms for people to understand how their data is collected, processed, and shared by government institutions, and for people to seek redress or delete their data. In the UK, we are challenging police forces' refusals to disclose information on their purchase and use of IMSI catchers.[24] Internationally, we shine light on spending by countries such as the UK, US, Germany, and France to transfer these technologies to authoritarian countries, which can entrench despotic regimes and enable human rights abuses.[25]
- **Keep the public informed and engaged with how these technologies can impact our rights, freedoms, lives, civic spaces, societies, and democratic institutions**. We publish explainers to illustrate potential risks.[26] In the UK, we are campaigning to encourage you to contact your locally elected Police and Crime Commissioner to share your views about how police can and should be using surveillance technologies in your area.[27]
- **Promote strong cyber security policies and encryption and anonymity tools that support human rights.** We highlight key examples of cyber security[28], encryption, and anonymity services[29] that create private spaces for people to express themselves, and how governments and corporations can ensure people better access these tools.

---

[23] Privacy International, "Bulk Personal Datasets & Bulk Communications Data challenge", available at https://privacyinternational.org/legal-action/bulk-personal-datasets-bulk-communications-data-challenge; Privacy International, "10 Human Rights Organisations v. United Kingdom", available at https://privacyinternational.org/legal-action/10-human-rights-organisations-v-united-kingdom.

[24] Privacy International, "Press release: Privacy International fights to unearth police use of intrusive mobile phone monitoring technology", 7 August 2018, available at https://privacyinternational.org/press-release/2221/press-release-privacy-international-fights-unearth-police-use-intrusive-mobile.

[25] Privacy International, "Teach 'em to Phish: State Sponsors of Surveillance", 17 July 2018, available at https://privacyinternational.org/report/2159/teach-em-phish-state-sponsors-surveillance.

[26] Privacy International, "Contesting Surveillance", available at https://privacyinternational.org/programmes/contesting-surveillance/all.

[27] Find your PCC, Association of Police and Crime Commissioners, available at http://www.apccs.police.uk/find-your-pcc/.

[28] Privacy International, "After the Gold Rush: Developing Cyber Security Frameworks and Cyber Crime Legislation to Safeguard Privacy and Security", 1 October 2018, available at https://privacyinternational.org/advocacy-briefing/2272/after-gold-rush-developing-cyber-security-frameworks-and-cyber-crime.

[29] Privacy International, "Securing Safe Spaces Online Encryption, online anonymity, and human rights", February 2018, available at https://privacyinternational.org/sites/default/files/2018-02/Securing%20Safe%20Spaces%20Online_2_0.pdf.

- **Strengthen democratic oversight and safeguards**. We develop principles and policy positions so that governments and industry can better protect privacy and other rights. For example, we have proposed model safeguards around the use of government hacking.[30]
- **Equip civil society organisations across the world to better promote strong protections for people**. We work with partners in countries such as Argentina, Chile, Colombia, Mexico, and South Africa to examine how governments' data collection practices impact fundamental rights and freedoms and what we can do to challenge unlawful practices. We support our international partners' efforts to embed privacy safeguards and enforcement mechanisms in law and policy.[31]

[30] Privacy International, "Government Hacking and Surveillance: 10 Necessary Safeguards", available at https://privacyinternational.org/feature/957/government-hacking-and-surveillance-10-necessary-safeguards#8c.

[31] Privacy International, "Watching The Watchers: Accessing and Challenging Control Over Our Data", 29 January 2018, available at https://www.privacyinternational.org/feature/1095/watching-watchers-accessing-and-challenging-control-over-our-data.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471