Civic Space Brief

UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER

Pervasive Surveillance & Civic Space

What is pervasive surveillance?
Surveillance is increasingly embedded in our digital and physical lives. States and non-State actors can use cameras, biometric tools, communication platforms, and even commercial data to monitor everyone. Targeted and mass monitoring can reveal defenders', journalists' and trade unionists' movements, personal data, networks and work connections and other contacts without their knowledge and expose them to significant risks.

How does digital surveillance work?
Weak data protection safeguards and mass data collection, and rapid development of privacy-intrusive technologies reinforce each other to exacerbate risks for critical actors, such as HRDs and journalists and their sources.

Tools can:

- **Hack devices.** Spyware and forensic tools can expose messages, contacts and files.
- **Track every move.** Phones, telecom networks and location data can reveal movements, routines and meetings.
- **Identify who is a defender.** Facial, iris, voice and gait recognition and other biometric systems can identify people in public spaces, at airports, train stations, borders or during protests.
- **Analyse people's thinking and behaviour.** AI can connect large datasets and infer relationships, activities and opinions, seeking to predict behaviour.

> *I felt very lonely and scared. I didn't know what to do, whether to throw the phone away […]. Thinking that they had had access to photos, conversations.*
>
> *Testimony of a Human Rights Defender who was subjected to Pegasus software*

How does surveillance impact HRDs?
Defenders were **among the earliest known targets of commercial spyware** in 2012, and hundreds of attacks against defenders, journalists and others have since been documented. In response, some States have committed to imposing limitations on their use of spyware. Meanwhile, civil society, technical experts and companies have developed advanced security tools, strengthened specialised threat reporting and undertaken legal action. Yet these measures are insufficient: spyware tools continue to be developed, sold and used with inadequate transparency and accountability.

How does AI transform surveillance?
AI makes surveillance cheaper, faster and easier to scale. By enabling data to be processed, inferred and combined from communications, biometrics, location data and online activity, it **accelerates identification, tracking, deanonymization and profiling,** making it harder for defenders to protect their identities, networks and movements. AI tools can also reinforce hacking and interception tools and facilitate more widespread collection and reuse of personal data, expanding continuous surveillance.

New and emerging forms of human rights defence

As digitalization expands**, those working in tech develop responses to new risks.** Engineers, coders, security researchers, whistle-blowers and others have been crucial for exposing abuses and arguing for embedding privacy, security and human rights protection within digital technologies. When they promote, protect or strive for the protection and realization of human rights and fundamental freedoms through peaceful means, **they can be considered human rights defenders**.

Their expertise should help shape regulation, corporate practices and support technologies that put people and rights at the centre.

Global Alliance for Human Rights

Civic Space Brief

UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER

RESISTING PERVASIVE SURVEILLANCE

Privacy, online and offline, is at the core of a human rights respecting online world. As technology reshapes society, we must redouble efforts to prevent digital tools from being used to track, monitor – and ultimately silence – human rights defenders.

1

DEFEND THE RIGHT TO PRIVACY

Privacy is fundamental for people being able to think freely, independently form opinions, express themselves and associate with others and meaningfully participate in society. Mass surveillance cannot be justified by broad security and safety arguments. Without privacy, there is no real democracy and no real security.

2

LIMIT THE AVAILABILITY OF INTRUSIVE TOOLS

States should introduce moratoriums on the sale, transfer and use of intrusive surveillance technologies until adequate human rights safeguards are in place. Without stronger domestic and export controls, and effective measures to hold vendors, developers, manufacturers, middlemen actors and users to account, serious risks will not only remain but worsen with proliferation.

> *Measures of surveillance that are incompatible with international human rights law are already widespread […] Without an active public discussion, societies risk sleepwalking into surveillance systems allowing those in power to exert unprecedented levels of control over day-to-day life.*
>
> High Commissioner for Human Rights

3

EFFECTIVELY PROTECT DATA

Laws and regulatory frameworks must do both, effectively protect personal data and protect against arbitrary and intrusive surveillance powers. States must enforce robust data protection laws, uphold encryption, prevent arbitrary surveillance powers, and guarantee independent oversight and effective remedies. Independent data protection authorities should be resourced to be able to investigate violations and provide remedies.

4

HOLD STATES AND COMPANIES ACCOUNTABLE

States must conduct human rights due diligence that involves people at risk when developing, buying or deploying technologies with surveillance capacities, including proactively identify risks. Companies must identify, prevent and remedy harms linked to their products, services and business relationships, and report meaningfully on their impacts.

5

EXPOSE SURVEILLANCE ABUSE

Surveillance abuses thrive in secrecy. Journalists, civil society, researchers and technical experts were instrumental in detecting, investigating and documenting spyware abuses, identifying those responsible and bringing them to light. Their vital work requires highly specialised technical, investigative and legal expertise – and resources. The work exposing surveillance must be financially supported and actively encouraged in law and practice.

6

EQUIP DEFENDERS FOR SELF-PROTECTION

Defenders must understand how their data can be used for surveillance and have access to effective and accessible privacy-protecting tools. Even as funding for defenders shrinks, they require sustained and practical support and tools tailored to the contexts in which they operate to protect themselves and their networks, sources and communities from surveillance. Protection from surveillance is crucial to enable their core work to defend and advance human rights.