



UN experts: Safeguard human freedoms from systematic digital interference, surveillance and chilling effects on civic space

GENEVA – Ahead of the RightsCon summit on human rights in the digital age, hosted in Zambia from 5-8 May, UN experts* expressed deep concern over the growing global spread of intrusive surveillance technologies, their normalisation in everyday life, and called for the urgent strengthening of safeguards to protect human rights and fundamental freedoms.

“Digital surveillance tools and activities are often incompatible with international human rights obligations, foster an environment of fear, and exert profound chilling effects on the exercise of fundamental freedoms and civic space. Collectively, these developments limit the ability to express dissent and impede inclusive democratic public participation.

Globally, arbitrary and pervasive digital surveillance has become increasingly normalised. This results in unnecessary and disproportionate interferences with human rights. An ever-greater number of people are indiscriminately brought under surveillance without reasonable suspicion, affecting populations and groups far beyond any justified targets of surveillance.

Moreover, modern digital surveillance tools are expansive, highly intrusive, remote and opaque. It is increasingly hard to know when they are operating, under whose control and authorization, against whom and why. In such circumstances, the threat and/or *suggestion* of surveillance is as harmful as any actual surveillance in interfering with the right to privacy and chilling the exercise of fundamental rights. Further concerning is the normalisation of digital surveillance tools with dual civil/military capabilities for law enforcement purposes that undermine public freedoms.

The chilling effects generated and amplified by digital surveillance pose a critical threat to democratic governance and societal well-being. They interfere with legitimate civic and political activism and the peaceful expression and mediation of disagreement and undermine free democratic participation.

Across autocratic and democratic contexts, a combination of digital surveillance tools is overwhelmingly used against civil society, peaceful assemblies, political opposition, minorities, marginalised and dissenting voices. Remote biometric identification (such as facial recognition technologies) removes the ability to remain anonymous in public, while targeted seizure, compromise and monitoring of devices (such as through spyware or interceptions) expose some of the most intimate spaces of life. Often driven by AI systems, machine learning and other powerful computer processes, aerial surveillance and high-volume data analytics can gather and analyse unprecedented volumes of information (used in different contexts, including in social media patrolling.

AI systems intensify surveillance threats and activities through their ability to gather and analyse unprecedented volumes of data. Digital surveillance tools are designed to interoperate, with each amplifying the intrusive potential of another.

As systems and datasets are increasingly integrated, and AI allows highly intrusive and expansive data processing, people are exposed to heightened risks of identification, tracking, intrusive profiling, reprisals and persecution (including legal, retrospective or future) for political and civil dissent. Even when surveillance or other technologies are initially deployed in pursuit of legitimate objectives, they are highly susceptible to surveillance creep and repurposing to suppress dissent and human rights defenders. Too often surveillance measures bypass transparency, public oversight, and fundamental human rights safeguards.

These developments bring harmful impacts on the rights to freedom of peaceful assembly, association, political participation and expression (as well as other related rights). Intrusive and pervasive digital surveillance diminishes privacy and anonymity in online and offline spaces. It further erodes the trust essential for people to associate, mobilise and participate freely in public debates, without fear of stigmatisation or retribution.

Digital surveillance tools, methods and activities, amplify pre-existing socio-political vulnerabilities and historical discrimination. Women and marginalized activists are routinely targeted by gendered and racial stigmatization, including sexualized attacks, deepfakes, and doxxing intended to force their withdrawal from public life. Activists representing marginalised issues or groups face a magnified risk of harassment, attacks, reputational harm and criminalization resulting from harmful digital surveillance.

Digital surveillance tools and methods cannot be viewed in isolation, but as elements of a complex and interconnected surveillance ecosystem. The current digital landscape is characterised by a decisive shift from data minimization to one of data maximization. There is a failure to apply effective personal data protection principles generally and to protect and strengthen privacy-preserving technology like encryption. Complex surveillance tools rely on the collection, generation or structuring of vast quantities of data, which is often retained in perpetuity and remains available for future exploitation or targeting. These enhance and extend States surveillance powers and capabilities for conducting arbitrary, intrusive, and mass surveillance. Digital surveillance ecosystems are sustained by opaque alignments and collaborations between States, commercial developers, corporate actors, and data-intermediaries.

Unless holistic surveillance ecosystems and compounding human rights harms are addressed, the "necessary in a democratic society" test to evaluate the acquisition, deployment and use of digital technologies will remain biased in favor of harmful surveillance tools and methods. This risks further exacerbating chilling effects that silence dissent and shrink civic space.

Powerful and intrusive technologies, including AI, are being implemented for law enforcement and other security purposes, in the absence of adequate legal

frameworks. States are increasingly adopting laws that expand surveillance powers and provide broad security exceptions which nullify existing safeguards.

The proliferation of overbroad laws to counter terrorism, “extremism”, “foreign agents” and cybercrime, as well as those for protecting national security and sovereignty, have profoundly impeded and chilled the legitimate work of civil society actors, including humanitarians, human rights defenders, journalists, dissidents, activists, and minority groups.

There is an increasing digital surveillance, cyber threats, and deliberate disruption of civilian internet in armed conflicts, gravely endangering civilians and hindering fundamental freedoms including when exercised for humanitarian, peace-building and conflict prevention purposes. Civilian digital systems in armed conflict must be protected in line with international human rights and international humanitarian law.

International, regional, and national laws and regulations must be urgently strengthened on the design, use, and transfer of digital surveillance tools to prevent arbitrary and indiscriminate surveillance. This includes adopting a binding international instrument on digital surveillance technology, and clear and robust national laws and regulations that restrict the use of digital surveillance in line with international human rights standards and with the independent judicial approval and oversight. These laws must adequately address technologies’ capabilities, and ensure their uses comply with the human rights law requirements of legality, legitimate aim, necessity, proportionality and non-discrimination requirements. Judicial safeguards, accessible and effective remedies, and reparation for violations, including compensation, must also be made available.

States must effectively regulate AI and surveillance technologies as they pose serious risks for human rights in law enforcement, counter-terrorism and national security contexts, border management, and military operations. Misuse of AI can intensify unjustified surveillance, predictively profile populations, censor online expression, and propagate disinformation. It can enable authorities to target dissent, human rights defenders, and civil society, and stifle rights to privacy and liberty, and civil and political freedoms at a much larger scale and faster pace – all undermining democracy and the rule of law.

Therefore, it is necessary for States and businesses to conduct rigorous human rights due diligence and impact assessments of AI and other technologies throughout their lifecycle, including development, transfer and use. States must prohibit the use or transfer of AI systems, surveillance and other technologies that cannot satisfy human rights law or that pose unacceptable risks to human rights. Other uses must be subject to rigorous risk-based regulation.

AI algorithms must be transparent and explainable. AI systems must be always subjected to meaningful human control. There must also be stringent safeguards on data quality, testing and validation, and personal data protection and security. Digital surveillance and AI systems must be subject to independent oversight, and there must be effective and accessible mechanisms for accountability and remedies, taking into account intersectional harms and chilling effects.

It is not too late to halt the serious harms being done by the ever-expanding misuse of new and runaway surveillance technologies. States must urgently recommit to safeguarding fundamental rights, including the rights to freedom of peaceful assembly and association and privacy, by ensuring effective limits on digital surveillance technologies.”

ENDS

***The experts:**

- Gina Romero, the Special Rapporteur on the rights to freedom of peaceful assembly and of association (www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association)
- Ben Saul, the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (www.ohchr.org/en/special-procedures/sr-terrorism)
- Mary Lawlor, the Special Rapporteur on the situation of human rights defenders (www.ohchr.org/en/special-procedures/sr-human-rights-defenders)
- Ana Brian Nougères, the Special Rapporteur on the right to privacy (www.ohchr.org/en/special-procedures/sr-privacy)

Special Rapporteurs/Independent Experts/Working Groups are independent human rights experts appointed by the United Nations Human Rights Council. Together, these experts are referred to as the [Special Procedures](#) of the Human Rights Council. Special Procedures experts work on a voluntary basis; they are not UN staff and do not receive a salary for their work. While the UN Human Rights office acts as the secretariat for Special Procedures, the experts serve in their individual capacity and are independent from any government or organization, including OHCHR and the UN. Any views or opinions presented are solely those of the author and do not necessarily represent those of the UN or OHCHR.

Country-specific observations and recommendations by the UN human rights mechanisms, including the special procedures, the treaty bodies and the Universal Periodic Review, can be found on the Universal Human Rights Index <https://uhri.ohchr.org/en/>.

For inquiries and media requests, please contact: hrc-sr-freeassembly@un.org.