Guiding Principles on Government Use of Surveillance Technologies

Purpose: These voluntary and non-legally binding Guiding Principles illustrate how governments can maintain their commitment to respect and protect democratic principles, human rights, and fundamental freedoms, consistent with their international obligations and commitments, in the responsible use of surveillance technology. These Guiding Principles are intended to prevent the misuse of surveillance technologies by governments and those acting on their behalf in three main areas of concern.

Context: The world has benefited from substantial technological progress in recent decades as the Internet has connected exponentially more people and devices. When used responsibly and in a manner consistent with applicable international law, surveillance technologies can be important tools for protecting national security, public safety, and critical infrastructure and for conducting criminal investigations, thereby ensuring that people can enjoy their rights and liberties.

At the same time, a growing number of governments misuse digital technologies to restrict access to information and the exercise of human rights and fundamental freedoms. These actions often target journalists, human rights defenders, activists, workers and union leaders, political opposition members, or others perceived as dissidents and critics. This can lead to the unequal enjoyment of human rights and fundamental freedoms, and disproportionately impacts women and girls in all their diversity as well as individuals or members of groups in marginalized or vulnerable situations that are already largely excluded from civic spaces, online and offline, such as Indigenous Peoples, LGBTI persons, persons belonging to national, racial, ethnic, religious, and linguistic minorities, and persons with disabilities. In some cases, governments use surveillance technologies in ways that violate or abuse the right to be free from arbitrary or unlawful interference with one's privacy, as set out in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). In the worst cases, governments employ such products or services as part of a broad State apparatus of oppression that violates or abuses a number of human rights and fundamental freedoms including freedoms of expression, religion or belief, association, and peaceful assembly, rights to equality before the law and equal protection of the law without discrimination, and procedural rights, causing online and offline civic space to shrink.

The responsible use of surveillance technologies aims to improve safety and security while respecting the rule of law, and to prevent and mitigate against any harmful consequences. Governments should therefore take steps to ensure that the use of surveillance technologies is lawful and responsible, and also that there are safeguards in place that apply to the collection, handling, and disclosure of material obtained using these technologies in order to protect individual privacy, personal data, and human rights and fundamental freedoms, and to foster transparency, accountability, and civic participation, while effectively and appropriately pursuing legitimate law enforcement, public safety, and national security objectives.

"Surveillance technologies" is a broad concept often defined and regulated in legislation. Technologies used for surveillance can refer to products or services that can be used to detect,

monitor, intercept, collect, exploit, preserve, process, analyze, invasively observe, and/or retain sensitive data, personally identifying information, including biomarkers, or communications concerning individuals or groups. These technologies can be used lawfully and legitimately with appropriate safeguards, though they can also be used in an unacceptable manner by governments. These principles apply to the use of surveillance technologies in three ways that are identified below as being of concern. These Guiding Principles are not intended to apply to activity that does not fall within an area of concern.

Scope: These Guiding Principles aim to prevent or mitigate three areas of concern:

1) The use of Internet controls to suppress human rights and fundamental freedoms and unjustly limit access to information;
2) Pairing advanced video surveillance with artificial intelligence (AI)-driven tools to persistently identify and monitor people without an appropriate legal basis; and
3) The use of big data analytic tools to support the discriminatory enforcement of laws and to target individuals or members of groups in marginalized or vulnerable situations, journalists, human rights defenders, workers and union leaders, dissidents, and other perceived government opponents as a means to enforce social and political control.

Governments should not use these surveillance technologies to unjustifiably interfere with freedom of expression; discourage the exercise of human rights and fundamental freedoms; perpetrate technology-facilitated gender-based violence or discrimination online and offline; perpetuate harmful or discriminatory norms and stereotypes; or limit bodily autonomy through any means, including but not limited to unlawful collection or misuse of personal health data, including reproductive and sexual data, or distribution of intimate images.

These Guiding Principles represent common practices and principles for which the implementation can vary across nations depending on legal frameworks and systems, with some nations providing even more robust safeguards. Similar non-legally binding instruments that articulate the responsible use of surveillance tools and data include the OECD Recommendation on Artificial Intelligence (AI), OECD Privacy Guidelines, OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, the Global Privacy Assembly resolution on Government Access to Data, Privacy and the Rule of Law, the UNESCO Recommendation on the Ethics of Artificial Intelligence, and the work of the Freedom Online Coalition.

Principles: The following principles are intended to guide the responsible use of surveillance technology to prevent the misuse in the three aforementioned areas of concern. Some states may choose to implement these principles in other areas as well.

- **Appropriate Legal Protections:** The use of surveillance technologies should be carried out in accordance with states' domestic law and international obligations and commitments, consistent with democratic values and the rule of law, and may incorporate principles such as lawfulness, necessity, proportionality, or reasonableness. Governments should not use surveillance technologies in a manner that violates human rights or undermines fundamental freedoms. Governments should implement mechanisms that prevent and address violations of applicable domestic and international

law, including international human rights law. Effective oversight, transparency, and redress processes should be clearly defined, reviewed for unintended consequences or misapplication, consistently practiced, and fairly enforced. Any person claiming such redress should have access to appropriate and effective judicial or non-judicial remedies. In such scenarios, it is especially important to ensure that systemic oversight and accountability mechanisms have sufficient authority and resources to identify and remedy possible abuses.

- **Nondiscrimination:** In accordance with the prohibition on discrimination, surveillance technology should not be used to target individuals or members of a group solely based on race, color, gender, ethnicity, indigeneity, language, religion, age, national origin, disability, genetic information, social origin, sexual orientation, political opinion, or any other classification protected by law or on other grounds inconsistent with applicable domestic law or international obligations and commitments. Governments should also strive to mitigate disparate impact from surveillance technologies on the basis of the aforementioned attributes. Where a surveillance process incorporates an automated technology system, such as an AI system, the development of the technological system should employ appropriate, justifiable, equitable, transparent, and understandable design practices. Efforts to prevent and mitigate unintended bias and disparate impact should begin in the design and development stages. Deployed systems should be routinely evaluated for discriminatory effect, unintended bias, and disparate impact, noting that these cause and perpetuate disproportionate harm to persons or groups in marginalized or vulnerable situations, especially those facing multiple and intersecting forms of discrimination, and to ensure that outcomes are consistent with applicable law and policy.

- **Oversight and Accountability:** Governments should ensure the operation of surveillance technologies is governed in a manner that proactively mitigates the risks of misuse and enables appropriate access to judicial or administrative review. Governments should adopt appropriate domestic oversight mechanisms, including human oversight, that help ensure compliance with applicable international human rights obligations as well as applicable domestic laws, procedures, and policies. In developing and applying oversight mechanisms, governments are encouraged to seek and consider feedback from relevant stakeholders, consistent with law enforcement and national security needs, including civil society, technologists, academics, the private sector, and victims or survivors of unjustified state surveillance, to ensure lawful and responsible use of surveillance technology. Governments are encouraged to document the uses of surveillance technologies through logs and records in order to facilitate meaningful oversight and monitoring of outcomes and to foster procedural fairness where appropriate.

- **Transparency:** Governments should ensure transparency on the applicable general legal framework supporting the use of surveillance technologies. Governments should clearly define the legal basis for using surveillance technology with transparency on the safeguards in place to prevent abuse or discriminatory uses. This may include how such technology works, the nature and duration of potential impacts, how negative impacts are mitigated, the frequency of use, and how data processing is consistent with applicable

legal obligations. Procurement policies should be transparent and require, consistent with the UN Guiding Principles on Business and Human Rights, that vendors providing surveillance technologies to governments develop internal policies and processes consistent with the procuring government's domestic and international legal obligations. Transparency mechanisms should exist and take into account the need to balance the interest of individuals and the public to be informed with the need to prevent the disclosure of information that would harm law enforcement, national security, or public safety objectives. Governments should consider how they can provide meaningful transparency, including effective notice to possible subjects of surveillance, while balancing these legitimate imperatives.

- **Limitations on Data Scope and Collection:** The quantity and nature of information collected through surveillance technology and the timeframe for which that data is retained should be limited to what is relevant or necessary and appropriate to achieve specified and legitimate objectives of public interest and be consistent with applicable domestic and international law, including rules on safeguarding personal information and the confidentiality of communications. Within this context, biometric tools such as fingerprint scans, DNA analytics, facial recognition, speech recognition, gait recognition, and iris scans should be used only when lawful and appropriate in the circumstances balancing the interests at stake, giving due regard to the context of collection and use.

- **Secure Post-Acquisition Data Handling:** Data acquired by governments through the use of surveillance technology should be subject to procedures appropriately ensuring its use, processing, retention, aggregation, and dissemination are consistent with the purpose for which it was acquired. Personal data acquired or generated through the use of surveillance technology, including disparate personal data elements that are not sensitive separately but become sensitive once combined, should only be shared in compliance with applicable laws, policies, and regulations. Private sector entities participating in the acquisition, generation, or processing of surveillance data through a government contract should be subject to appropriate safeguards, including requirements for disclosure of breaches, reporting misuse, penalties for misuse of data by public or private actors, whistleblower protections, and reasonable data deletion schedules.

- **Respect for Human Rights, Including Privacy:** Governments should work to ensure that the surveillance technologies they utilize are designed, developed, and deployed with appropriate mechanisms in place to safeguard human rights and fundamental freedoms, including the right to be free from unlawful or arbitrary interference with one's privacy, and respect for bodily autonomy, including of women and girls in all their diversity, and LGBTI persons. Such designs, development, and deployments should, where appropriate and consistent with applicable international human rights obligations and commitments, incorporate data retention and minimization procedures, which might include timed deletion, based on what is necessary and appropriate to achieve legitimate objectives, and appropriate privacy enhancing technologies.

- **Integrity:** Governments should ensure that their surveillance technologies use secure equipment and undergo testing and evaluation to demonstrate that they are effective, safe,

compliant with applicable law, and mitigate adverse outcomes. Governments should strive for testing conditions in a modelled environment to mirror as closely as possible the conditions in which the system is anticipated to be deployed or has been deployed. This might not always be possible given the unknown characteristics of the system where these technologies may be deployed. Such testing should take into account both the specific technology used and the roles of any human operators or reviewers. They should be regularly assessed to ensure their continued integrity for the purpose.

- **Training:** Government officials involved in the policy development, procurement, operation, oversight, and accountability of surveillance systems should be well informed on the appropriate and lawful use and technical limitations of the technology and data protection best practices, including on matters related to privacy and other human rights. They should also have ongoing access to legal advice. Governments should aim for detailed and recurring training on lawful and responsible use of surveillance technology for end users, including users of associated data, and access to appropriate advice on ethics. Governments could consider peer-to-peer learning mechanisms to prevent a continuation of any problematic practices as appropriate.

These Guiding Principles have been developed through consensus by the Freedom Online Coalition's 36 Member States, which are dedicated to the support of Internet freedom and the worldwide protection of human rights and fundamental freedoms online.