13 Principles for a Human Rights Respecting State Surveillance Framework

Reporters Without Borders (RWB) joins the Association for Progressive Communications and more than 215 other organizations in calling for the adoption of the "International Principles on the Application of Human Rights to Communications Surveillance," which were developed by Access, Electronic Frontier Foundation and Privacy International in consultation with a group of international experts.

Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity, reinforces other rights, such as freedom of expression, information and association, and is recognised under national, regional and international human rights instruments. This Council recognized with A/HRC/RES/20/8 "the same rights that people have offline must also be protected online." However, in recent years, many States have developed national legal frameworks and practices that exploit the capacities of new technologies to engage in mass surveillance. Those frameworks reflect a shift from surveillance of communications based on the rule of law (in particular legally authorised targeted surveillance based on clear criteria) to mass surveillance through untargeted collection of communications data of ordinary citizens where no lawful grounds for surveillance exists. These national legal frameworks often contain outmoded definitions of communications that purport to distinguish between the content of communication, versus data about the communication. Typically, the content of communications is strongly protected whereas non-content transactional data, traffic data, or "meta-data" is typically given much less protection, even though it can be just as revealing and have serious privacy implications.

Activities that restrict the right to privacy, including communications surveillance, can only be justified when prescribed by law, are necessary to achieve a legitimate aim, and are proportionate to the aim pursued. During the present session of the Council, Member States will consider a report on challenges facing States in their efforts to secure democracy and the rule of law. Arbitrary, secretive and non-targeted mass surveillance is indicative of a broader breakdown in democratic principles and the rule of law. We urge these Member states to adopt surveillance frameworks consistent with the Principles, summarized below.

As more technologies facilitate State surveillance of communications, States are failing to ensure that laws and regulations related to communications surveillance adequately protect international human rights, in particular the rights to privacy and freedom of expression and association. These Principles attempt to explain how existing international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques.

The Principles concentrate on the core issue: how do existing human rights laws, jurisprudence and norms protect the information of individuals in light of technological developments?

They provide civil society groups, industry, States and others with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights.

This initiative is the outcome of a global consultation with international experts in communications surveillance law, policy and technology from civil society, industry and elsewhere. It is fully consistent with the views taken by UN Special Rapporteur on the right to freedom of opinion and expression Frank La Rue in his report on State surveillance of the Internet (A/HRC/23/40).

The determination of whether a State may conduct communications surveillance must be consistent with the following summarized principles:[1]

LEGALITY
Any limitation to the right to privacy must be prescribed by law. Given the rate of technological changes, laws that limit the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process.

LEGITIMATE AIM
Laws should only permit communications surveillance by specified State authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.

[1] The full text can be accessed at https://necessaryandproportionate.org/, and http://en.rsf.org/rwb-signs-international-principles-31-07-2013,45001.html

NECESSITY
Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim. The onus of establishing this justification, in judicial as well as in legislative processes, is on the State.

ADEQUACY
Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified.

PROPORTIONALITY
Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society. Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights.

COMPETENT JUDICIAL AUTHORITY
Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent.

DUE PROCESS
Due process requires that States respect and guarantee individuals' human rights by ensuring that lawful procedures that govern any interference with human rights are properly enumerated in law, consistently practiced, and available to the general public.

USER NOTIFICATION
Individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support of the application for authorisation.

TRANSPARENCY
States should be transparent about the use and scope of communications surveillance techniques and powers. States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance. States should enable service providers to publish the procedures they apply when dealing with State communications surveillance.

PUBLIC OVERSIGHT
States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance. Oversight mechanisms should have the authority to access all potentially relevant information about State actions, including, where appropriate, access to secret or classified information.

INTEGRITY OF COMMUNICATIONS AND SYSTEMS
In order to ensure the integrity, security and privacy of communications systems, and in recognition of the fact that compromising security for State purposes almost always compromises security more generally, States should not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their systems, or to collect or retain particular information purely for State surveillance purposes.

SAFEGUARDS FOR INTERNATIONAL COOPERATION
In response to changes in the flows of information, and in communications technologies and services, States may need to seek assistance from a foreign service provider. Accordingly, the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied. States may not use MLAT processes and foreign requests for protected information to circumvent domestic legal restrictions on communications surveillance.

SAFEGUARDS AGAINST ILLEGITIMATE ACCESS
States should enact legislation criminalising illegal communications surveillance by public or private actors. The law should provide sufficient and significant civil and criminal penalties, protections for whistle blowers, and avenues for redress by affected individuals. States should also enact laws providing that, after material obtained

through communications surveillance has been used for the purpose for which information was given, the material must be destroyed or returned to the individual.

During HRC23, civil society groups made a statement to the Council expressing:

> "strong concern over recent revelations of surveillance of internet and telephone communications of US and non-US nationals by the government of the United States of America and the fact that US authorities makes the results of that surveillance available to other governments such as the United Kingdom. Of equal concern is the indication of apparent complicity of some US-based Internet companies with global reach."[2]

In that statement, groups requested that the High Commissioner prepare a compilation of national States surveillance policies and practices in place to assess their impact on human rights standards.

TODAY WE CALL ON STATES TO:

(a) recognise that surveillance threatens the human rights to privacy and freedom of expression and association, and to put these Principles at the heart of their communications surveillance frameworks.

(b) commit to ensuring that advances in technology do not lead to disproportionate increases in the State's capacity to interfere with the private lives of individuals.

We also support requests made by civil society groups in their statement during HRC23

WE CALL UPON THE HUMAN RIGHTS COUNCIL TO:

1) reaffirm its commitment to promoting the right to privacy in light of evolving technological challenges;

2) establish a framework for national guidelines similar to the Council-endorsed United Nations Guiding Principles on Business and Human Rights (A/HRC/RES/17/4) by which surveillance activities of each State can be reviewed and assessed during the UPR process and by the relevant Treaty Bodies in ways that are consistent with these Principles, the Special Rapporteur's report (A/HRC/23/40, and resolutions A/HRC/RES/17/4 and A/HRC/RES/20/8, as well as with all relevant international human rights instruments.

Finally we support the recommendation of Special Rapporteur La Rue that the Human Rights Committee consider developing a new General Comment on Article 17 of the ICCPR protecting the right to privacy in a manner consistent with these Principles.

[2] Civil Society Statement to the Human Rights Council on the impact of State Surveillance on Human Rights addressing the PRISM/NSA case: http://bestbits.net/prism-nsa/