Joint Civil Society Statement on Privacy in the Digital Age
Submitted to the 27th Session of the UN Human Rights Council

September 11, 2014

This week's discussion of the report on surveillance by the UN High Commissioner for Human Rights at the Human Rights Council is a critical moment in the global understanding of the human rights challenges raised by unlawful and arbitrary surveillance. The Office of the UN High Commissioner for Human Rights will present a report on the right to privacy in the digital age (A/HRC/27/37). As the report states, "the technological platforms upon which global political, economic and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it" on an unprecedented scale (para 2). It is imperative that the Council and Member States continue to promote and protect the right to privacy as technologies evolve and surveillance and data gathering capabilities become more powerful.

In this context, the Human Rights Council has the opportunity to demonstrate leadership, promote global understanding of the right to privacy, and ensure robust state implementation of that right. We ask the Council to create a new special procedures mandate on the right to privacy to ensure sustained attention to the issues raised by the High Commissioner's report within the UN's human rights institutions.

Key Report Findings and Recommendations

The report confirms that "international human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data" (para 47). This finding reaffirms the Council's recognition in A/HRC/RES/20/8 that "the same rights that people have offline must also be protected online."

The right to privacy is well-established in both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights (ICCPR). The report recognizes that the challenges posed by new digital surveillance capabilities do not confound human rights standards, but rather require re-examination of and renewed attention to state implementation of established standards.

Critically, the High Commissioner found that many governments have failed to meet their obligations under the right to privacy. Practices in many states have revealed "a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight." Combined with a "disturbing lack of governmental transparency," these failings have "contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy" (paras 47-48). The research of many of the undersigned organizations confirms this finding.

As an immediate measure, the High Commissioner called on all states to "review their own national laws, policies and practices to ensure full conformity with international human rights law" and address any shortcomings.

To facilitate national review, the report elaborated on several issues:

1. **Digital surveillance may engage a state's human rights obligations extraterritorially, regardless of the nationality or location of individuals whose communications are under surveillance.** A state's obligations can be engaged if that surveillance involves the exercise of power or effective control in relation to communications infrastructure. The same is true where regulatory jurisdiction over a third party that controls data is exercised, including where jurisdiction is asserted over the data of private companies as a result of the incorporation of those companies in the state in question (para 34). In a globalized world where data is routinely held in various jurisdictions and can travel across multiple borders in seconds, this point underlines the importance of the principle of non-discrimination in ensuring meaningful respect for privacy.

2. **States should adopt a clear, precise, accessible, comprehensive, and non-discriminatory legislative framework to regulate all surveillance conducted by law enforcement or intelligence agencies (para 50).** Surveillance should be undertaken under accessible law with foreseeable effects in accordance with the rule of law, including the right to an effective remedy. In many states, the legal frameworks governing surveillance fail to meet this standard, generating consequent accountability and transparency concerns.

3. **The overarching principles in determining whether an interference is permissible are legality, necessity, and proportionality (para 23).** In particular, it is essential to reiterate proportionality as a foundational principle. Mass surveillance is by nature disproportionate and large-scale collection practices often fall afoul of this principle. As the High Commissioner notes, "Mass or 'bulk' surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate" (para 25).

4. **Metadata merits stronger protection than it currently enjoys under national legal frameworks (paras 19-20).** The interception of data about a communication ("metadata") can be as sensitive as the interception of the content of a communication. There is growing recognition that metadata cannot reasonably be afforded weaker protections than communications content. Such data is storable, accessible, and searchable, and access to and analysis of the data can be revelatory and highly invasive.

5. **The interception, acquisition, and retention of data amounts to an interference with the right to privacy, regardless of whether data is subsequently consulted or used (para 20).** In the context of mass surveillance programs, "[e]ven the mere possibility of communications information being captured creates an interference with privacy, with the potential chilling effect on rights," including free expression and association (para 20). It also follows that mandatory third-party data retention requirements, where governments require Internet or mobile service providers to store data about *all* customers, "appears neither necessary nor proportionate" (para 26).

6. **A range of other rights may also be affected by communications surveillance and the collection of personal data, beyond the right to privacy**. The report cites freedom of opinion and expression; the right to peaceful assembly and association; to family life; and to health as illustrative examples. Although beyond the scope of the report, the High Commissioner stated that the linkages between mass surveillance and effects on other rights merit further consideration.

7. **States must ensure effective oversight and remedy for violations of privacy through digital surveillance (paras 37-41).** The report states that oversight by all branches of government and an independent civilian agency is essential to ensure effective protection of law. Effective remedies can come in a variety of forms, but must meet criteria that are well-established in human rights law.

8. **The private sector should respect human rights if asked to facilitate surveillance or data collection or when providing surveillance technology to states (paras 42-46).** Where Internet or telecommunications companies comply with government requests for user data or surveillance assistance without adequate safeguards, they risk complicity in resulting violations. The report calls on companies to "assess whether and how their terms of service, or their policies for gathering and sharing customer data, may result in an adverse impact on the human rights of their users," implicitly drawing a connection between company data collection practices and government access to data companies hold (para 44). When companies provide surveillance technology to states that do not have adequate legal safeguards, companies risk complicity in

violations of the right to privacy and other human rights (para 43).

A new Special Rapporteur on the right to privacy

The High Commissioner's report applies well established standards of international human rights law and provides a robust and universal foundation for examining state implementation of human rights obligations to surveillance and data collection activities. However, new surveillance capabilities and technologies raise complex and fast evolving issues.

As a result, the High Commissioner urged "ongoing, concerted multi-stakeholder engagement" to address challenges related to the right to privacy (para 49). The report also called for "further discussion and in-depth study of issues relating to the effective protection of the law, procedural safeguards, effective oversight, and remedies," as well as the responsibility of businesses (para 51).

We urge the Council to follow up on the High Commissioner's work, including by establishing a dedicated special procedure mandate on the right to privacy for the following reasons:

- A dedicated mandate holder would play a critical role in developing common understandings and furthering a considered and substantive interpretation of the right across a variety of settings, as recommended by the report. A dedicated mandate holder would also be an independent expert, allowing for a neutral articulation of the application of the right to privacy that draws on the input of all stakeholders.
- Establishing a separate mandate for privacy would allow for the development of a coherent and complementary approach to the interaction between privacy, freedom of expression, and other rights.
- A dedicated mandate holder would help assess the implementation by state and non-state actors of their applicable international responsibilities and obligations in a sustained and systematic way. Functions should include carrying out country visits; collecting best practices; receiving and seeking information from states, businesses, and other stakeholders; and issuing recommendations.

Submitted by Human Rights Watch

Endorsed by:
Access
American Civil Liberties Union (ACLU)
Amnesty International
ARTICLE 19
Association for Progressive Communications
Center for Democracy & Technology (CDT)
Electronic Frontier Foundation
International Commission of Jurists (ICJ)
Privacy International
World Wide Web Foundation