Check against delivery

Human Rights Council 27th Session

Panel Discussion on the Right to privacy in the digital age

United Nations Human Rights

OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS

Opening Statement

Ms. Flavia Pansieri

Deputy High Commissioner for Human Rights

12 September 2014

Salle XX, Palais des Nations

Excellencies,

Ladies and gentlemen,

I am delighted to introduce this discussion on the right to privacy in the digital age, with the participation of such a distinguished panel.

In a very short space of time, digital communications technologies have revolutionized the way human beings interact. For millions of people, the digital age is one of emancipation - perhaps the greatest liberation movement the world has ever known. Just as an example, over 1 million people participated electronically in the open dialogue and consultation that was conducted to develop a framework for the Post-2015 sustainable development goals – and called for full inclusion of human rights therein. Human rights defenders, activists, democratic voices, minorities and others can communicate via digital platforms, and can participate in global debate in ways that were previously inconceivable.

But these digital platforms are vulnerable to surveillance, interception and data collection. Deep concerns have been expressed as policies and practices that exploit this vulnerability have been exposed across the globe.

Surveillance practices can have a very real impact on peoples' human rights, including their right to privacy, and their rights to freedom of expression and opinion, to freedom of assembly, to family life and to health. Information collected through digital surveillance has been used to target

dissidents. There are also credible reports suggesting that digital technologies have been used to gather information that has then led to torture and other forms of ill-treatment.

In resolution 68/167, the General Assembly requested the High Commissioner to submit a report on "the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale". This report is being presented to the Council at its present session. It builds on expert consultations and in-depth research that examined existing national and international legislation and jurisprudence, together with a compilation of information from a broad range of sources, including a questionnaire to stakeholders.

As the report makes clear, international human rights law provides a robust and universal framework for 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.

However, practices in many States reveal a sometimes deliberate lack of adequate national legislation and enforcement; weak procedural safeguards; and ineffective oversight. All of this contributes to widespread impunity for arbitrary or unlawful interference in the right to privacy.

The High Commissioner's report examines the protection afforded by international human rights law regarding privacy, including the meaning of

"interference with privacy" in online communications; the definition of "arbitrary and unlawful" interference in this context; and the question of whose rights are protected, and where.

For instance, on the question of what constitutes privacy interference, it is clear that the aggregation of communications data may give comprehensive insight into an individual's behaviour, social relationships, private preferences and identity – extending even beyond the information obtained by reading someone's mail. The collection and retention of communications data may therefore constitute an interference with privacy whether or not those data are subsequently consulted or used. The very existence of a mass surveillance programme regarding email communication and other forms of digital expression creates an interference with privacy, and the onus is on the State to demonstrate that its interference is neither unlawful nor arbitrary.

Turning to "arbitrary or 'unlawful" interference with privacy, the report notes that State surveillance of electronic communications data may be a legitimate law enforcement measure –if it is conducted in compliance with the law. But States must demonstrate that the surveillance is both necessary and proportionate to the specific risk being addressed. Mandatory third-party data retention – where telephone companies and Internet service providers are required to store metadata about communications by their customers, for subsequent access by law enforcement and intelligence agencies – appears neither necessary nor proportionate.

States have an obligation to ensure that individuals' privacy is protected

by law against unlawful or arbitrary interference. This means that all forms of communications surveillance must be conducted on the basis of publicly accessible law; and this law must in turn comply with the State's own constitutional regime and international human rights law. Secret rules and secret interpretations of the law – even if issued by judges – are not compatible with the principle that laws should be clear and accessible. Neither are laws or rules that give excessive discretion to executive authorities such as security and intelligence services.

Additional concerns have been raised regarding extra-territorial surveillance and interception of digital communications. Drawing on the work of the Human Rights Committee and the International Court of Justice regarding the determination of when a State exercises jurisdiction, the report notes that a State's human rights obligations are engaged whenever it exercises power or effective control. If surveillance involves a State's exercise of power, or effective control, in relation to digital communications infrastructure, then *wherever it may be taking place,* that surveillance may engage a State's human rights obligations. This would include, for example, direct tapping or penetration of a communications infrastructure, as well as exercise by the State of regulatory jurisdiction over a third party which physically controls the data.

International human rights law is also explicit on the principle of non-discrimination. States must take measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity -- regardless of the ethnicity, nationality, location or other status of the people whose communications it is

monitoring.

Procedural safeguards and effective oversight are crucial for safeguarding the right to privacy in law and in practice. A lack of effective oversight has contributed to impunity for arbitrary or unlawful intrusions on the right to privacy in the digital environment. Internal safeguards devoid of independent oversight have been demonstrably ineffective against unlawful or arbitrary surveillance methods. Appropriate safeguards may take a variety of forms, but it is vital that they include independent civilian oversight and participation from the executive, the judiciary and parliament in order to ensure the effective protection of the law.

Moreover, States have a legal obligation to provide effective remedies for violations of privacy through digital surveillance, in judicial, legislative or administrative forms, with procedures that are known and accessible.

Excellencies,

Another vital issue is the role of the private sector. Governments increasingly rely on corporations to conduct and facilitate digital surveillance. And in some cases there may be legitimate reasons for a company to provide user data. But when the request is in violation of human rights law, or where the information is used in violation of human rights law, that company risks being complicit in human rights abuses.

The Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, provide a global standard for preventing and addressing adverse human rights effects of business activity. They make

clear that the responsibility to protect human rights applies throughout a company's global operations, regardless of where its users are located, and independently of whether a State meets its own human rights obligations. Many corporations appear to be insufficiently aware of these issues.

In addressing these and other gaps regarding the implementation of the right to privacy, a disturbing lack of government transparency often renders examination of this issue extremely arduous – as well as any exercise in accountability. Yet there is a clear need for further discussion and in-depth analysis. The High Commissioner's report is one important step in that direction; and I trust that today's meeting will be another. I look forward to your discussions.

Thank you.