Privacy International's oral statement to the Human Rights Council

37th ordinary session,

6 March 2018

Inter-active dialogue with the UN Special Rapporteur on the right to privacy

Mr. President,

Privacy International welcomes the opportunity to participate in this inter-active dialogue with the Special Rapporteur on the right to privacy.

With regards to the draft legal instrument, PI has not commented on the substance of such an instrument. We believe that existing international human rights law provides a clear and universal framework for the promotion and protection of the right to privacy in the digital age and we encourage you to continue working towards the interpretation of such standards, with the view to support their full implementation.

An example of the need for such human rights interpretation is in relation to government hacking for surveillance purposes.

A growing number of governments around the world are embracing hacking to facilitate their surveillance activities.

Reports have emerged that governments are using hacking to target journalists and human rights defenders in Bahrain, Mexico, Morocco and the United Arab Emirates. Other countries, such as France, Italy, the Netherlands and the United Kingdom have recently introduced legislation to authorize government hacking for surveillance.

Government hacking can easily cross borders and affect individuals across many jurisdictions, including those who may be unrelated to a government operation. The UK has explicitly included bulk hacking powers in its 2017 Investigatory Powers Act. In 2015, on the basis of a single warrant, the United States FBI ultimately hacked over 8,700 computers located in 120 countries and territories.

As a form of government surveillance, hacking presents unique and grave threats to our privacy and security.

It has the potential to be far more privacy intrusive than any other surveillance technique, permitting the government to remotely and secretly access our personal devices and the data stored on them as well as to turn on the microphone, camera, or GPS-based locator technology. Hacking allows also governments to manipulate data on our devices, including corrupting, planting or deleting data, or recovering data that has been deleted, all while erasing any trace of the intrusion.

At the same time, government hacking has the potential to undermine the security of our devices, networks and infrastructure. Government hacking often depends on exploiting vulnerabilities in systems to facilitate surveillance objectives. It may also involve manipulating people to undermine the security of their own systems. These techniques prey on user trust, the loss of which can further undermine the security of systems and the internet.

Given the privacy and security implications of hacking, Privacy International questions whether it can ever be a legitimate component of state surveillance. Governments may never be able to demonstrate its compatibility with international human rights law, notably its necessity and proportionality as a tool for surveillance.

We would like to ask the Rapporteur for his views on the topic and we would like to encourage him to develop a human rights analysis of government hacking for surveillance purposes, seeking information from states, oversight bodies and other stakeholders, with the view to develop specific recommendations based on international human rights law.

Thank you for your attention.