

**Privacy International's oral statement
to the Human Rights Council 51st ordinary session,
16 September 2022**

**Inter-active dialogue with the UN High Commissioner for Human Rights - Report on right to
privacy in the digital age**

Mr. President,

Privacy International welcomes the opportunity to participate in this inter-active dialogue with the High Commissioner for Human Rights.

We share the concerns expressed in the new report on the right to privacy in the digital age and support the recommendations therein.

We would like to expand on two interlinked issues addressed in the report: government hacking powers and the attempts to limit the use of encryption.

Governments have resorted to hacking to target human rights defenders, journalists, and political opponents, as most prominently revealed in the Pegasus-NSO Group cases. Government hacking can be more privacy intrusive than any other surveillance technique, permitting remote and secret access to personal devices and their data, also in real-time, and even manipulation of data on those devices (including altering or deleting it) without being detected.

It not only poses unique threats to privacy, but it also undermines the security of our devices, networks and entire infrastructure. Hacking is about causing technologies to act in a manner the manufacturer, owner or user did not intend or did not foresee.

In a similar fashion, governments are seeking to undermine confidentiality of encrypted communications by imposing among others general monitoring obligations on encrypted communications. Proposals among others require companies to introduce back doors, implant silent listeners, or scan all communicated content in ways that cannot be targeted to specific users, and would indiscriminately affect any (potentially millions or billions of) users.

Governments seek to justify these surveillance measures in the name of preventing and investigating terrorism or child sexual abuse online, despite security experts raising serious concerns about the effects of such measures.

Given the privacy and security implications of government hacking and of general monitoring obligations imposed on companies that undermine encryption, Privacy International questions whether their use can ever be compatible with international human rights law.

We would like to ask the High Commissioner what concrete steps governments should take to prevent the use of government hacking and to promote the use of encrypted communications.

Thank you for your attention.