Countries Should Protect Privacy in Digital Age

Unchecked Mass Surveillance Threatens Rights

(Geneva) – Governments around the world should aggressively protect online privacy through stronger laws and policies as pervasive electronic surveillance increases.

There is an urgent need to overhaul national surveillance practices to protect everyone's privacy, or risk severely limiting the potential of the Internet , Global growth in digital communications, coupled with increased government computing powers, have fueled expansive, new surveillance practices. Justifying the use of these tactics under outdated legal frameworks has permitted overbroad and highly invasive intrusions on the right to privacy.

To guide countries in modernizing privacy protections, Human Rights Watch has endorsed a set of International Principles on the Application of Human Rights to Communications Surveillance, released on September 20, 2013, by a broad group of civil society organizations in Geneva. "The shocking revelations of mass monitoring by the US and UK [show how privacy protections have not kept pace with technology," said Cynthia Wong, senior Internet researcher at Human Rights Watch. "As our lives become more digitized, unchecked surveillance can corrode everyone's rights and the rule of law."

The International Principles provide immediate guidance to governments and make recommendations to ensure communications surveillance practices are lawful, necessary, proportionate, and subject to adequate safeguards against abuse. The principles, endorsed by over 250 nongovernmental groups, emerged from a year-long consultative process among experts in communications surveillance law, policy, and

technology. Governments should commit to reviewing their national surveillance practices and ensure that they are consistent with these principles, as well as recommendations made by the special rapporteur on the right to freedom of expression, Human Rights Watch said.

In her opening statement at the current session of the Human Rights Council on September 9, UN High Commissioner for Human Rights Navi Pillay expressed concern over the broad scope of surveillance programs, including in the US and UK. The high commissioner urged all countries to ensure that they have adequate safeguards to protect the right to privacy and other human rights, even "while national security concerns may justify the exceptional and narrowly tailored use of surveillance."

Pillay's remarks echoed prescient recommendations by Frank La Rue, special rapporteur on the right to freedom of expression, in his annual report to the UN Human Rights Council in April. He warned that inadequate legal frameworks "create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression."

Both the high commissioner and the special rapporteur recognize that national laws have not kept pace with technological change, Human Rights Watch said. Many surveillance regimes were enacted before social media existed and when cross-border communication was relatively rare.

In a pre-Internet age, conventional surveillance techniques were labor intensive and time consuming, which helped to constrain arbitrary and abusive practices. Today, authorities can construct a detailed portrait of a person's life with a request to a mobile phone company. The costs of data storage and computer

processing continue to fall, making mass interception of fiber-optic cables feasible.

As many aspects of people's lives become digitized, governments will be able to track people's location, associations, and communications even more effectively. The details of US and UK surveillance programs revealed by the former NSA contractor Edward Snowden are emblematic of this trend, Human Rights Watch said. Information revealed by the *Guardian* on June 21 suggests that since 2011, the British Government Communications Headquarters (GCHQ) has been intercepting fiber-optic cables carrying Internet data in and out of the UK. The *Guardian's* reporting alleges that this data includes recordings of phone calls, email content, and data on the use of websites and social media and that the UK may be sharing data with the US.

In the US, secret documents and court opinions have revealed that US surveillance programs are neither targeted nor proportional, Human Rights Watch said. Media reports indicate that the US is accessing vast amounts of data via cable intercept and by requesting user communications stored by major Internet and telecommunication companies that operate globally.

Although the exact scope of data collection and use is still unclear, disclosed documents suggest that current privacy safeguards have been breached thousands of times in recent years, calling into question the adequacy of oversight mechanisms. Both the UK and US governments appear to be intruding into the private digital lives of people around the world, the vast majority of whom are not suspected of any wrongdoing. Even more troubling, neither government seems willing to publicly recognize the privacy interests of people outside its borders, in law or rhetoric.

However, problems with the UK and US surveillance programs are representative of a broader, global issue. Given how intrusive digital surveillance can be, all governments should review their practices and update laws to ensure protection of all users' data, regardless of their citizenship or location, Human Rights Watch said.

The US and UK's actions also call attention to the ways governments are increasingly pressing Internet and telecommunications companies to help monitor online activity. Internet users trust companies to store and transmit the most intimate details of their daily lives. These companies have a responsibility to safeguard user privacy and avoid contributing to governments' misuse of surveillance powers.

Consistent with the UN Guiding Principles on Business and Human Rights endorsed by the Human Rights Council in 2011 and the Global Network Initiative's (GNI) guidelines], technology companies should credibly demonstrate they are standing up for their users, and seek to operate more transparently. The GNI is a global coalition of companies, human rights organizations, investors, and academics that formed to address issues of corporate responsibility in the technology sector. Governments should enable companies to disclose aggregate data on surveillance requests.

Just as national laws have become outdated, international standards have also not kept pace with technological change. The Human Rights Committee's General Comment 16 on the right to privacy has not been updated since 1988, which predates the commercial Internet. Recognizing this reality, La Rue has asked the Human Rights Committee to consider issuing a new general comment on the right to privacy. Human Rights Watch supports the rapporteur's recommendation to advance international understanding of how new surveillance capabilities may

undermine privacy and other rights. "Without updates to national privacy regimes, we are quickly headed toward a world where privacy disappears the second we go online or make a phone call," Wong said. "As mobile and Internet adoption expands globally, every country should ensure people can use these technologies without fear of invasive and disproportionate intrusions into their private lives."