

United Nations report: US, UK surveillance programs violate international law

Thomas Gaist
18 July 2014

A report released Wednesday by United Nations High Commissioner for Human Rights (UNHCHR) Navi Pillay, “The Right to Privacy in the Digital Age”, finds that surveillance practices carried out by the major powers, the United States and the United Kingdom, in particular, violate basic principles of international law and are destructive of democratic rights.

The report singles out a number of government activities that conflict with international law, including bulk collection of communications metadata, unrestricted sharing of data between government agencies, reliance on secret rules and secret courts, dragnet surveillance of foreigners, and the use of surveillance to facilitate drone strikes. The report warns that new forms of data-sharing and surveillance-related interactions between governments and corporations pose immense dangers to people’s democratic rights.

“Examples of overt and covert digital surveillance in jurisdictions around the world have proliferated, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure,” the report states. “Governments reportedly have threatened to ban the services of telecommunication and wireless equipment companies unless given direct access to communication traffic, tapped fibre-optic cables for surveillance purposes, and required companies systematically to disclose bulk information on customers and employees. Furthermore, some have reportedly made use of surveillance of telecommunications networks to target political opposition members and/or political dissidents.”

Apologists for such police state practices have argued that the collection of communications metadata constitutes a benign, legal and privacy-compatible form of surveillance. The UN report rejects this line of reasoning, saying that metadata collection is as harmful

to privacy and democratic rights as the collection of actual content.

“From the perspective of the right to privacy,” the report states, “this distinction [between collection of content and metadata] is not persuasive. The aggregation of information commonly referred to as “metadata” may give an insight into an individual’s behavior, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.”

The surveillance programs have a “chilling effect on rights” simply by virtue of their existence, the report argues, declaring that wholesale state spying discourages individuals from fully expressing their thoughts in electronic communications.

Pointing to the framework of secret courts and secret law that has been developed alongside the US National Security Agency’s surveillance apparatus, the report notes that secret “law” is not actually a valid form of law. “Secret rules and secret interpretations—even secret judicial interpretations—of law do not have the necessary qualities of ‘law’,” the UNHCHR concludes.

Other illegal activities of the US and British governments highlighted by the report include: virtually universal recording and retention of telephone conversations, spying by host governments on communications at “global events,” and the passage of laws requiring that personal computers be equipped with surveillance-friendly software.

The threat to privacy posed by the surveillance is magnified by the increasing role of private corporations in acquiring and storing data on behalf of their respective governments, the report notes, pointing to the integration of corporations into the surveillance apparatus. This, the report argues, is producing a

“transnational network comprising strategic intelligence relationships between Governments, regulatory control of private companies and commercial contracts.” The report notes that corporations are increasingly complicit in human rights abuses by state intelligence agencies.

The report finds that mass surveillance threatens a long list of universal human rights, including “freedom of opinion and expression,” freedom to “seek, receive and impart information,” “freedom of peaceful assembly and association,” and the right to health. It notes the use of surveillance to facilitate American targeted assassination and rendition operations. Digital surveillance has been used to “gather information that has then led to torture and other ill-treatment,” as well as to death by drone strike, the report states.

The document describes privacy protections for foreign nationals as very weak, and “even non-existent.”

The complete disregard of the US, UK and other nations for the rights of foreign nationals is, according to the UN report, a clear breach of the fundamental principle set forth in the International Covenant on Civil and Political Rights (ICCPR) that “all persons are equal before the law and are entitled without any discrimination to the equal protection of the law.”

As the report notes, when uncertainty exists about the source of a communication, surveillance agencies assume that it is “foreign,” so they can collect and store it. With electronic communications constantly being routed through overseas servers, such practices insure that supposed protections for national citizens are worthless.

“There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata,” the report states.

The report notes that the threat to privacy rights is being magnified by statutory requirements that computer networks be designed so that they are “wire-tap ready.”

The picture the report draws of US and UK government lawlessness is stark. Article 12 of the Universal Declaration of Human Rights states, “No one shall be subjected to arbitrary interference with his

privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

Article 17 of the International Covenant on Civil and Political Rights, which has been ratified by 167 nations, includes an almost identical provision.

The UN report provides valuable documentation and analysis of violations of essential principles of international law. However, its overall orientation is based on the false premise that illegal state surveillance can be reined in within the framework of the existing social and economic order, i.e., capitalism.

As Edward Snowden’s revelations have shown, the governments of the US, the UK, France, Germany and other major capitalist countries acquire and store the private communications of foreigners, and of their own citizens, on a gargantuan scale. This is done to track and generate profiles of potential opponents of the state and the ruling elite.

The very fact that mass, illegal state surveillance is an international phenomenon points to its roots in the crisis of the world capitalist system. The sharpest expressions of this crisis are imperialist war and unprecedented levels of social inequality. The development of the framework of a police state and dictatorial rule is the inevitable response of the capitalist ruling class to the growth of social tensions and the threat of revolutionary mass struggles by the working class.



To contact the WSWs and the Socialist Equality Party visit:

wsws.org/contact