AMNESTY INTERNATIONAL

The US NSA and the UK GCHQ want to listen in on all: Time for the Human Rights Council to discuss their activities: Amnesty International written statement to the 24th session of the UN Human Rights Council (9 to 27 September 2013)

AI index: IOR 41/018/2013
Date: 29 August 2013

Recent revelations about the nature and extent of surveillance activities by the United States, the United Kingdom, and other countries raise serious concerns regarding those states' respect for the right to privacy and other human rights, notably the rights to freedom of expression and association. The Human Rights Council should consider carefully the negative impacts of these activities on human rights of persons affected.

The right to privacy is reaffirmed in the Universal Declaration of Human Rights and guaranteed by the International Covenant on Civil and Political Rights and other universal and regional human rights instruments.[1]

Privacy is, in fact, essential to a person's identity. Simply put, people are different when they are under surveillance than when they have privacy. Privacy is critical to personal development and self-fulfilment. States should also keep in mind the overarching benefits that privacy has for society as a whole.

The state can take measures that interfere with privacy if doing so is necessary, for example to protect other rights, but its actions must be proportionate to a legitimate aim it seeks to achieve. The state must be able to justify those actions as passing this test of necessity and proportionality.

There is no question that the breathtaking extent of the United States Government's alleged surveillance of telephone and internet communication infringes on privacy.

Recent disclosures of surveillance by the United States' National Security Agency (NSA) related to a programme that collects records of every domestic phone call. Under a Foreign Intelligence Surveillance Court order dated 25

[1] UDHR, article 12 ; ICCPR, article 17 ; CRC, article 16; CRPD article 22.

April 2013 and made public by *The Guardian* on 5 June 2013,[2] the telecommunications provider Verizon has been required to provide "on an ongoing daily basis" information to the NSA on all telephone calls in its systems, including telephone calls between the United States and other countries. The information Verizon is required to hand over include the originating and terminating numbers, the duration of each call, telephone calling card numbers, trunk identifiers, International Mobile Subscriber Identity (IMSI) numbers, and comprehensive communication routing information.

These records do not include the content of the calls themselves, but for every person covered by this surveillance the "telephony metadata" that are gathered reveal much about their daily activities: who he or she calls, when, for how long and how often, and where he or she is when placing those calls if they go through mobile telephone systems. This is already much information about how a person goes about daily life.

The *New York Times* reported in August that the NSA is also examining all email messages that come into and go out of the United States.[3] The stated purpose is to locate information associated with terrorism or counterintelligence. While the aims may be legitimate, the methods the NSA employs apparently amount to it conducting a blanket search of every email message that enters or leaves a US-based server.

In fact, through whistleblower Edward Snowden's disclosures to *The Guardian* and the *Washington Post,*[4] we know that the NSA's surveillance programmes allow NSA analysts to search and read nearly everything the typical internet user does online. Emails, video, photos, video and voice calls, chats, file transfers, social networking details, and other information are open for scrutiny. One programme, Prism, reportedly gives the NSA a backdoor entry to major social networking, data storage and transfer, and email providers.

---

[2] See Glenn Greenwald, "NSA collecting records of millions of Verizon customers daily," *The Guardian,* 5 June 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (last viewed 29 August 2013).

[3] Charlie Savage, "NSA said to search contents of messages to and from US," *The New York Times,* 8 August 2013.

[4] See, for example, James Ball, "Edward Snowden NSA files: secret surveillance and our revelations so far," *The Guardian,* 21 August 2013, http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations (last viewed 29 August 2013); Barton Gellman, "NSA broke privacy rules thousands of times per year, audit finds," *The Washington Post,* 16 August 2013, http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html (last viewed 29 August 2013). See also Siobhan Gorman and Jennifer Valentino-Devries, "New details show broader NSA surveillance reach: programs cover 75% of nation's traffic, can snare emails," *The Wall Street Journal,* 20 August 2013, http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html (last viewed 29 August 2013).

A leaked NSA presentation of another programme, XKeyscore, states that it allows NSA analysts to search and read the content of emails, Facebook chats, private messages, and other social media activities as well as browser history and "every email address seen in a session by both username and domain," "every phone number seen in a session (e.g. address book entries or signature block)," and other user activity – including "username[s], buddylist[s], machine specific cookies."

The United Kingdom's Secret Intelligence Service and Government Communication Headquarters' Tempora programme is said to involve some 200 probes on transatlantic cables, enabling the agency to process 600 million "telephone events" and 39 million gigabytes of internet traffic each day. The programme reportedly enables the agency to store and analyse voice recordings, the content of emails, entries on Facebook, the use of websites, and the "metadata" that record who has contacted whom.

States that engage in these forms of massive surveillance must acknowledge that they are operating in a way that is qualitatively very different from traditional methods of investigation that rely on surveillance techniques that focus on individuals.

Even when individual communications are not monitored, the capacity to store and analyse data that have been collected in bulk and over time and then aggregated, potentially from different sources, can allow the production of a very accurate picture of who associates with whom (and at what level of intimacy), how they spend their free time, what health conditions they may have, what their political views are likely to be, and other details of their private lives.[5]

Moreover, once collected and stored, these data may potentially be used in the future for reasons that would not have justified the initial collection of information. The potential for misuse thus extends indefinitely into the future.

And, as noted above, several of the US and UK programmes are reported to have the capacity to monitor and record the content of communications. These programmes lack the transparent independent judicial oversight that is normally required to monitor and intercept private communications.

Instead, the states that engage in these forms of surveillance hide behind technicalities that do not adequately take account of the real and potential

---

[5] See, for example, Daniel J. Solove, "Five myths about privacy," *The Washington Post,* 13 June 2013, http://articles.washingtonpost.com/2013-06-13/opinions/39948998_1_government-surveillance-privacy-internet-surveillance (last viewed 29 August 2013); Daniel J. Solove, "Why privacy matters even if you have 'nothing to hide,'" *The Chronicle of Higher Education,* 15 May 2011, http://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/ (last viewed 29 August 2013); Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (New Haven and London: Yale University Press, 2011).

impact of these programmes on persons' lives. Their justifications must be subject to robust judicial and parliamentary scrutiny.

The United States defends the bulk collection of telephony metadata by asserting that the content of the calls is not monitored or recorded. In fact, U.S. government lawyers argue – and as far as is known the secretive Foreign Intelligence Surveillance Court has so far agreed – that warrants are not required for this activity because persons do not have a privacy interest in the phone numbers and the other details of the calls they make.

That is a convenient conclusion for those who want to conduct surveillance without basic legal safeguards, but it is not a reasonable one. Human rights principles do not allow the state to collect information that enables it to assemble a detailed picture of a person's daily activities and network of contacts without a specific and individualized reason subject to scrutiny by an independent judiciary.

As for the other US programmes, which give NSA analysts broad access to the content of private communications, the state's rationale appear even flimsier. Some of the programmes only target communications that the agency "reasonably believes" to involve a "non-US person." That allows for a very wide margin of error, and it offers no protection to persons who are not US citizens and do not live in the United States.

Ultimately, instead of attempting to make a showing – in advance and in public – that their surveillance measures are necessary and proportionate, the US, UK and other governments are asking their populations, and the rest of the world, to trust them – blindly.

In debate in the UN Security Council on 6 August 2013, a representative of the United States told the Security Council that he welcomed a fair discussion about the appropriate balance between privacy and security.[6] Amnesty International urges this Council to undertake such a discussion, It can start that discussion with an in-depth examination of the issues identified by the Special Rapporteur on the promotion and protection of the right to freedom of opinion in his report to the twenty-third session of this Council on the implications of states' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression.[7]

[6] UN DPI Press Release, SC/11807, 6 August 2013.
[7] A/HRC/23/40 of 17 April 2013.