GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

UNITED STATES

The Necessary and Proportionate Principles and the US government

Access
Amie Stepanovich, Drew Mitnick and Kayla Robinson
www.accessnow.org

Introduction

In June 2013, the scale and scope of US foreign intelligence surveillance began to be revealed to the world. Over a year later, the surveillance programmes described in the revelations facilitated by Edward Snowden continue to draw the ire of human rights advocates who argue the surveillance is, among other issues, unnecessary, disproportionate, and fundamentally lacking in transparency and oversight. The attention has galvanised policy makers in Washington, D.C., where the US Congress is moving closer to passing some version of communications surveillance reform. The Obama administration has released a number of reports and statements detailing its version of the operation of US surveillance work, and defending the constitutionality of these programmes. Simultaneously, the administration has quietly promoted principles which, if implemented, would bring US surveillance closer in alignment with international human rights law.

The Obama administration's principles provide a framework for US compliance with its own stated objectives (the US Framework).[1] The US Framework largely mirrors several of the International Principles on the Application of Human Rights to Communications Surveillance (Principles), an evaluative framework for assessing how human rights obligations and norms apply when conducting surveillance.[2] Below, we compare US surveillance practices to its own stated Framework and the Principles.

Policy and political background

Many US surveillance operations are authorised under either Section 215 of the Patriot Act (the "business records" provision), which has been interpreted to authorise bulk collection, or Section 702 of the FISA [Foreign Intelligence Surveillance Act] Amendments Act, which permits targeting of non-US persons "reasonably believed to be located outside the [US]" for foreign intelligence purposes.[3] Notably, the National Security Agency (NSA) presumes that a target is a non-US person when their location cannot be determined.[4]

The government also uses Executive Order (EO) 12333 to authorise surveillance programmes where the collection point is located outside of the US. It is widely believed that the government has interpreted EO 12333 to authorise any surveillance activities that are not otherwise unlawful or unconstitutional. Traditionally, there has been very little public information about EO 12333, including any oversight thereof. According to recent reports, EO 12333 authorises, inter alia, collecting all calls made in the Bahamas and another, undisclosed country.[5]

In March 2014, the US government adopted six privacy principles to govern surveillance. Scott Busby, Deputy Assistant Secretary of State for Democracy, Human Rights and Labor, articulated the US Framework at the 2014 RightsCon Silicon Valley conference, hosted by Access.[6] Secretary of State John Kerry reiterated the US Framework at a recent Freedom Online Coalition conference.[7]

A closer look at the US Framework for surveillance

Prior to the release of the US Framework, a number of government reports made recommendations encompassing several human rights principles. The President's Review Group on Intelligence and Communications Technologies (President's Review

1 Speech by Scott Busby at RightsCon, 4 March 2014. www.humanrights.gov/2014/03/04/state-department-on-internet-freedom-at-rightscon; Remarks to the Freedom Online Coalition Conference by US Secretary of State John Kerry, 28 April 2014. www.state.gov/secretary/remarks/2014/04/225290.htm

2 https://en.necessaryandproportionate.org/text

3 50 U.S.C. § 1881a (2008).

4 The Guardian. (2013, June 20). Procedures used by NSA to target non-US persons: Exhibit A – full document. *The Guardian*. www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document

5 Devereaux, D., Greenwald, G., & Poitras, L. (2014, May 19). The NSA is recording every cell phone call in the Bahamas. *The Intercept*. https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas

6 Speech by Scott Busby at RightsCon, 4 March 2014. www.humanrights.gov/2014/03/04/state-department-on-internet-freedom-at-rightscon

7 Remarks to the Freedom Online Coalition Conference by US Secretary of State John Kerry, 28 April 2014. www.state.gov/secretary/remarks/2014/04/225290.htm

Group) released a report that included a number of recommendations in line with the Principles: transparency in the operation of the US surveillance programmes; due process reforms for the Foreign Intelligence Surveillance Court (FISC); and more effective government oversight.[8] The Privacy and Civil Liberties Oversight Board (PCLOB) separately released a report arguing that bulk metadata collection is illegal under the terms of Section 215 and called for the creation of a special advocate to argue against the government before the FISC.[9] These recommendations could help guide the implementation of the US Framework and ensure compliance with its commitments.

The US Framework expands upon President Obama's Presidential Policy Directive 28 (PPD-28) which establishes principles to guide surveillance.[10] The six principles endorsed by the US are (1) rule of law, (2) legitimate purpose, (3) non-arbitrariness, (4) competent external authority, (5) meaningful oversight, and (6) increased transparency and democratic accountability. While the US Framework borrows heavily from the Principles, it omits several of them, and even in the case of those it adopts it often fails to meet the same standards. Principles not adopted by the US include due process, user notification, integrity of communications and systems, safeguards for international cooperation, and safeguards against illegitimate access.

Below, we examine the overlap between the US Framework and the Principles and examine where US policy fails to comply with the US Framework:

1. **Rule of law** – In his speech setting out the US Framework, Assistant Secretary Busby discussed how surveillance operates "pursuant to statutes and executive orders that were adopted as part of our democratic process." This principle further requires that laws, and their subsequent policies, provide clarity for individuals within the jurisdiction. US surveillance policy has proven to be anything but clear and accessible to the public. Instead, surveillance practices often depend on loose legal interpretations written in secret, approved by secret courts, and overseen by secret Congressional committees. By contrast, the Principles require that the law contains a "standard of clarity and precision" to provide users notice of the application of surveillance.

US surveillance policy does not conform with the rule of law principle. For example, Section 215 permits collection of records only when they are "relevant to an authorized investigation." However, authorities have interpreted the language to permit the acquisition of *all* phone records transiting the US. Similarly, Section 702 contains language that is overly vague, granting the Attorney General and Director of National Intelligence (DNI) the authority to "target persons reasonably believed to be located outside the United States to acquire foreign intelligence information." Programmes under this authority, namely PRISM and "Upstream" collection,[11] involve virtually limitless surveillance on any non-US person outside the US, and, by extension, "incidental" collection of vast amounts of data from US persons.

2. **Legitimate purpose** – The US Framework would permit surveillance only on the "basis of articulable and legitimate foreign intelligence and counter-intelligence purposes." This does not match the standard of the legitimate aim principle, which requires surveillance to be conducted only in the furtherance of a "predominantly important legal interest that is necessary in a democratic society." Further, PPD-28 permits bulk collection only for "detecting and countering" certain enumerated threats, and expressly prohibits the use of bulk collection for suppression of dissent, discrimination, or promoting US commercial interests. However, no similar restriction is placed on other non-bulk, yet highly intrusive forms of surveillance authorised under Section 702. The government should specify – and identify meaningful limits to – the purposes for which it acquires and collects foreign intelligence.

3. **Non-arbitrariness** – Non-arbitrariness, as articulated by the US Framework, requires surveillance to be tailored and intrusiveness minimised. This element matches up to the proportionality, necessity and adequacy principles.

8 Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies: Liberty and Security in a Changing World, 21 December 2013. www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

9 Privacy and Civil Liberties Oversight Board. (2014). Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court. www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf

10 Office of the Press Secretary. (2014). Presidential Policy Directive/PPD-28. www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf

11 Some slides used by the NSA revealed by Edward Snowden make a distinction between the "PRISM" and "Upstream" collection programmes. While we will use that shorthand in this submission, our understanding is that "Upstream" encompasses a wide range of surveillance programmes that have been revealed to date, including BLARNEY, FAIRVIEW, OAKSTAR, LITHIUM, and STORMBREW.

Proportionality requires considering government interests in light of the severity of intrusion and sensitivity of information. However, US indiscriminate bulk surveillance practices are not conducted in accordance with either the Principles or the US Framework.[12] The president has proposed a limit on the use of bulk collection of telephone metadata.[13] Obama's proposal, however, does not prohibit bulk collection generally, but only addresses telephone metadata bulk collection under the 215 authority.[14] The US should rather immediately end all mass surveillance practices.

In an example of the mismatch between the Framework and past practices, in 2012, the NSA queried its database of hundreds of millions telephone metadata records 288 times.[15] Of those 288 queries, only 16 produced a potential connection to suspected terrorist activity that warranted a referral to the FBI for investigation. It is difficult to see how this programme comports with the adequacy principle, or with the necessity principle's requirement that "[c]ommunications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights."

4. **Competent authority** – While the US Framework seeks guidance from a "competent external authority", the Principles specify that the authority be judicial. In contrast to the Principles, the Framework expressly retains an exception for some operational decisions to be made within intelligence agencies. FISC, the judicial authority that reviews surveillance programmes and applications, has been repeatedly misled by US intelligence agencies in their applications, which makes its rulings inherently unreliable.[16]

The Principles further require that the competent judicial authority be "conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights." However, the secret nature of FISC makes it difficult for judges to consult with the independent technical and legal experts necessary to fairly decide complicated issues. One former FISC judge has gone on the record proposing the use of specially appointed advocates to help alleviate this problem, though this has not been adopted.[17]

5. **Oversight** – The US Framework calls for meaningful oversight. To underscore US adherence to this element, Assistant Secretary Busby highlighted extant internal oversight mechanisms. However, despite claims that the NSA's activities have been approved by all three branches of government, the NSA has reportedly lied to or misled all three branches.[18]

In accordance with the Principles, true oversight mechanisms should operate independently of the state entity conducting surveillance. Public oversight calls for independent oversight mechanisms that have the authority to access all potentially relevant information, an element lacking from current US policy.

6. **Increased transparency and democratic accountability** – The final element of the US Framework is transparency. Assistant Secretary Busby pointed to recent efforts to declassify FISC opinions and the government's intention to

12 Although some of these practices "only" collect communications metadata, a recent study has demonstrated exactly how revealing this information can be, even over a short period of time. See Mayer, J., & Multcher, P. (2014, March 12). MetaPhone: The Sensitivity of Telephone Metadata. *Web Policy*. webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata; Lohr, S. (2014, May 31). Quantifying Privacy: A Week of Location Data May Be an 'Unreasonable Search'. *New York Times*. bits.blogs.nytimes.com/2014/05/31/quantifying-privacy-a-week-of-location-data-may-be-unreasonable-search

13 Savage, C. (2014, March 24). Obama to Call for End to NSA's Bulk Data Collection. *New York Times.* www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html

14 This is problematic because the intelligence community engages in bulk collection of other information, including records of international money transfers. Savage, C., & Mazzetti, M. (2013, November 14). CIA Collects Global Data on Transfer of Money. *New York Times*. www.nytimes.com/2013/11/15/us/cia-collecting-data-on-international-money-transfers-officials-say.html. The U.S. government previously operated a programme to bulk collect internet metadata. Gellman, B. (2013, June 15). US Surveillance architecture includes collections of revealing internet, phone metadata. *Washington Post.* www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html

15 This is according to Professor Geoffrey Stone, a member of the President's Review Group. Speech by Geoffrey Stone at Public Citizen, 6 January 2014. www.citizen.org/pressroom/pressroomredirect.cfm?ID=4057

16 Cushing, T. (2013, August 21). Declassified FISA Court opinion shows NSA lied repeatedly to the Court as well. *techdirt.* https://www.techdirt.com/articles/20130821/16331524274/declassified-fisa-court-opinion-shows-nsa-lied-repeatedly-to-court-as-well.shtml

17 Carr, J. (2013, July 22). A Better Secret Court. *New York Times.* www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html

18 McCormick, R. (2013, October 28). Obama wasn't aware of the NSA's wiretap of world leaders, says White House Review. *The Verge*. www.theverge.com/2013/10/28/5037300/obama-unaware-of-wiretaps-on-world-leaders; Blake, A. (2013, June 11). Sen. Wyden: Clapper didn't give 'straight answer' on NSA programs. *Washington Post.* www.washingtonpost.com/blogs/post-politics/wp/2013/06/11/sen-wyden-clapper-didnt-give-straight-answer-on-nsa-programs; Ackerman, S. (2013, August 21). NSA illegally collected thousands of emails before FISA Court halted program. *The Guardian*. www.theguardian.com/world/2013/aug/21/nsa-illegally-collected-thousands-emails-court

release the statistics on the issuance of national security orders and requests.

In fact, the DNI has released a transparency report including the total number of orders issued under certain authorities in 2013, and the number of targets affected.[19] This report supplements the information already required as part of the intelligence community's annual FISA reporting.[20] While this is a step forward for transparency around government surveillance activities, the report falls short of what was called for by the We Need to Know Coalition,[21] which urged Congressional leaders and the Obama administration to require the government to publish information about the specific numbers of *requests*, the specific authorities making those requests, and the specific statutes under which those requests are made.[22]

Unlike Google's and Microsoft's transparency reports, which break down both the number of requests they receive and the number of accounts affected, the DNI's report only includes the number of requests and "targets", which makes the scope of the nation's surveillance machine appear far more limited than it actually is. To put this in context, in 2012, there were 212 requests for business records justified under Section 215, but that number also includes requests for the "ongoing, daily" disclosure of communications metadata of the millions of customers of AT&T, Verizon and Sprint. We know this because public disclosure of aggregate numbers of requests pursuant to most of the statutes to be included in the DNI's report is already required.

It is also worth noting that the government has only released the number of targets, not the exponentially larger number of people whose privacy is violated when their data are caught in the NSA's dragnet. Moreover, by grouping statutes together in the categories, the DNI is further obfuscating the nature and scope of the government's surveillance activities, and limiting an informed, public debate about the extent of the intelligence community's intrusions into the private lives of users all over the world.

Public disclosure by both the government and the communications providers who hold user data is crucial in keeping both accountable. At this time, the US government has not demonstrated an intention to publicly disclose details of the scope and scale of its surveillance activity at the level of clarity and granularity envisioned by the Principles, nor has it allowed corporations it requests data from to do so either.

Conclusions

The revelations provide evidence of widespread violations of the fundamental right to privacy, with implications for the rights to freedom of expression and association, among other rights. Bulk surveillance is inherently arbitrary, and therefore in violation of international law. Legitimate surveillance activities should always be based on probable cause and targeted toward a specific individual or organisation.

Unfortunately, currently proposed legislative reforms would fail to move the US towards the Framework or the Principles. The House of Representatives recently passed the USA Freedom Act, a bill that many advocates viewed as the best hope for human rights reforms. The bill passed the House after being weakened during secret deliberations between the Obama administration and members of the House. The changes were so significant that most rights groups withdrew support.[23]

As originally written, the USA Freedom Act would have achieved a number of significant human rights reforms, including preventing bulk collection by requiring a nexus to an investigation, bringing clarity to Section 215, increasing FISC oversight and introducing a special advocate, increasing the ability of companies to disclose government national security data requests, and increasing the power of internal oversight bodies, as well as adding external checks. The House watered down many of the reforms.

Congress' failure to enact reforms is a great disappointment. The US must change its laws if it is to bring its surveillance programmes closer in

19 The report contained figures for Section 702 and Section 215 orders, as well as other authorities including the FISA "Trap and Trace" provision and National Security Letters. Office of the Director of National Intelligence. (2014, June 26). Statistical Transparency Report Regarding Use of National Security Authorities Annual Statistics for Calendar Year 2013. www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf

20 U.S. Department of Justice. (2014, April 30). 2013 Report pursuant to the Foreign Intelligence Surveillance Act of 1978. www.justice.gov/nsd/foia/foia_library/2013fisa-ltr.pdf

21 We Need to Know is a multi-stakeholder group including companies like Google and Microsoft, NGOs including Access, CDT and the ACLU, and various trade associations. We Need to Know. (2013, July 18). Letter to Congressional leaders and Obama administration on transparency. https://www.accessnow.org/page/-/weneedtoknow-transparency-letter.pdf

22 Furthermore, the Coalition called for the ability to differentiate requests based on content versus non-content data, and enumerate the number of persons, accounts or devices affected. The DNI report only includes the numbers of orders issued, and the number of "targets" affected.

23 Masnick, M. (2014, May 21). As feared: House guts USA Freedom Act, every civil liberties organization pulls their support. *techdirt*. www.techdirt.com/articles/20140520/17404727297/as-feared-house-guts-usa-freedom-act-every-civil-liberties-organization-pulls-their-support.shtml; Stepanovich, A. (2014, May 20). Access withdraws conditional support for USA FREEDOM Act. *Access Now*. https://www.accessnow.org/blog/2014/05/20/access-withdraws-conditional-support-for-usa-freedom-act

alignment with the Principles and other international human rights standards. While the president's policy statement is an admirable show of commitment to surveillance reform, only greater legal restrictions and increased external oversight of these programmes can assure the protection of fundamental freedoms, and reassure the public that the US conducts its surveillance activities in a rights-respecting manner.

Action steps

The following advocacy steps are recommended in the US:

- Call or write to Congress urging them to support rights-respecting surveillance reform.
- Provide comments to the PCLOB showing support for efforts to ensure that rights are protected during the development of laws to protect the nation against terrorism.
- Endorse the International Principles on the Application of Human Rights to Communications Surveillance:

  https://en.necessaryandproportionate.org/take-action/access
- Encourage companies to protect your personal information by supporting the Data Security Action Plan: https://www.encryptallthethings.net
- Take steps to protect your own information by using secure communications platforms, like those suggested by Reset the Net: https://pack.resetthenet.org