KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMON GROUND BETWEEN COMPANY AND CIVIL SOCIETY SURVEILLANCE REFORM PRINCIPLES

January 15, 2014

On December 9, AOL, Apple, Facebook, Google, Linkedin, Microsoft, Twitter, and Yahoo! issued a call for governments around the world to reform their surveillance laws, as well as a released a set of principles to guide such reform. These principles align well in many ways with principles that civil society groups released this July applying human rights concepts to communications surveillance. While the respective principles differ in some important ways, there is enough commonality to suggest ample space for civil society and industry to move forward on a common set of norms and reforms that should inform the debate about surveillance law globally. This paper explores that commonality.

On December 9, AOL, Apple, Facebook, Google, Linkedin, Microsoft, Twitter, and Yahoo! issued a call for governments around the world to reform their surveillance laws, as well as a released a set of principles to guide such reform.[1] These principles align well in many ways with principles that civil society groups released this July applying human rights concepts to communications surveillance.[2]

The International Principles on the Application of Rights to Communications Surveillance, known as the "Necessary and Proportionate" principles, have the support of the Center for Democracy & Technology and over 300 other civil society organizations. Specifically, both the companies and civil society groups call for: (i) surveillance law to be clearly codified; (ii) particularized, as opposed to bulk surveillance; (iii) independent judicial oversight of surveillance; (iv) transparency of surveillance law; (v) transparency of surveillance activities; (vi) clear rules and efficient processes to resolve conflicts of law that may arise; and (vii) balancing government needs with privacy rights, particularity requirements.

While the respective principles differ in some important ways – the Necessary and Proportionate principles usually go further than do the company principles – there is enough commonality to suggest ample space for civil society and industry to move forward on a common set of norms and reforms that should inform the debate about surveillance law globally. This paper explores that commonality. It also shows that with respect to U.S. law – which has been the subject of much discussion as a result of the surveillance activities of the U.S. National Security Agency – the USA FREEDOM Act, the leading intelligence surveillance reform bill, would promote many, but not all, of the reforms called for in both sets of principles. The President should account for the growing consensus about these reforms as he prepares the reforms the Administration will embrace.

---

[1] Available at http://reformgovernmentsurveillance.com.

[2] Available at https://en.necessaryandproportionate.org/text.

I. Clarity and Codification

The company surveillance reform principles and Necessary and Proportionate principles both call for surveillance laws to codified and to be codified with clarity. The company principles call for governments to "codify sensible limitations on their ability to compel service providers to disclose user data..." and they call for any compelled disclosure or collection to be done under a "clear legal framework." The Necessary and Proportionate principles approach clarity and codification of surveillance law from the direction of a limitation on the right to privacy: "The State must not adopt or implement a measure that interferes with the right of privacy in the absence of an existing publicly available legislative act which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice and of and can foresee its application."

Certainly, a lack of clarity in U.S. law has invited a certain amount of mischief in application of the law. For example, the bulk collection of telephony metadata is premised on an interpretation of a phrase in Section 215 of the PATRIOT Act (50 U.S.C. § 1861), "relevant to an investigation," that was unheard of prior to the disclosure of the bulk collection program. The leading intelligence surveillance reform bill, the USA FREEDOM Act, would amend Section 215 to require more than mere relevance. Instead, the "tangible things" sought under the statute would have to pertain to an agent of a foreign power, the activities of a suspected agent of a foreign power, or an individual in contact with or known to a suspected agent of a foreign power. However, the USA FREEDOM Act does not address the fact that much intelligence surveillance conducted by the United States outside the U.S. is conducted under an Executive Order (No. 12333), which allows for broad surveillance of non-U.S. persons abroad, and not under any codification of the law. Nor does the USA FREEDOM Act sufficiently clarify Section 702 of FISA, which governs surveillance in the U.S. of people believed to be outside the U.S.

II. Particularized, as Opposed To Bulk, Surveillance

Both the company surveillance principles and the civil society groups' principles call for government surveillance to be particularized. The company principles state, "... governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications." Particularity appears in the civil society groups' Necessity principle. It states, "... when there are multiple means" of engaging in communications surveillance, governments should engage in "the means least likely to infringe upon human rights." Particularized surveillance based on individualized suspicion is by nature less likely to infringe upon the human right to privacy than is unparticularized, bulk surveillance. Further, the Necessity principle requires that any communications surveillance be limited to that which is strictly and demonstrably necessary to achieve a legitimate aim. Unparticularized surveillance fails that test. Bulk collection of communications metadata – a form of unparticularized surveillance -- is not necessary, as demonstrated by the U.S. government's inability to identify a single instance in which its telephony metadata bulk collection program was necessary to thwart

a terrorist attack,[3] and by its own decision to shut down its Internet metadata bulk collection program due to ineffectiveness.[4]

The USA FREEDOM Act promotes the particularity for which both sets of principles call. As indicated above, it would amend Section 215 of the PATRIOT Act to require that the "tangible things" sought under the statute pertain to an agent of a foreign power, the activities of a suspected agent of a foreign power, or an individual in contact with or known to a suspected agent of a foreign power. Mere relevance to an investigation – the standard in current law that the government interprets to permit unparticularized bulk collection of telephony metadata – would not be enough. The Act is intended to end bulk collection of telephony metadata and to clearly outlaw bulk collection of metadata associated with Internet communications.

III. Independent Judicial Oversight That is Adequately Informed

The company surveillance principles and Necessary and Proportionate principles each call for independent judicial oversight of government surveillance. The company principles declare that surveillance activities should be "subject to strong checks and balances," including independent judicial review. The Necessary and Proportionate principle of "Competent Judicial Authority" similarly states that surveillance should be authorized by "a competent judicial authority that is impartial and independent."

Both the company principles and Necessary and Proportionate principles advocate these judicial oversight bodies be adequately informed. The company surveillance principles directly call for an adversarial process at the courts that review surveillance applications. The Necessary and Proportionate principles call for adequate information for judicial oversight without recommending specific policy mechanisms such as an adversarial process. Instead, the "Competent Judicial Authority" principle states that courts making surveillance determinations should be "conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights," and possess "adequate resources in exercising the functions assigned to them." While not the exclusive means of achieving them, an adversarial process promotes these objectives. According to former Foreign Intelligence Surveillance Court (FISC) judge James Robertson, the absence of an adversarial process at the FISC leaves judges dependent upon the government for critical

[3] *Klayman v. Obama*, CV 13-0851 (RJL), 2013 WL 6571596 (D.D.C. Dec. 16, 2013) ("[T]he Government does not cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time sensitive in nature"). *See also, Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies* (December 12, 2013), ("Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."). P. 104. *Available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.*

[4] [4] *See*, CBS News, *NSA was the one "acting nobly," agency head says* (June 27, 2013), *available at* http://www.cbsnews.com/videos/nsa-was-the-one-acting-nobly-agency-head-says/.

information and deprives them of hearing both sides of the matter before them.[5] Additionally, FISC opinions released this year discuss instances of "substantial misrepresentation" that led to significant misperceptions by the court for several years.[6] An adversarial process can help head off judicial reliance on one party's misrepresentation and skewed characterization of the facts.

The USA FREEDOM Act would promote informed decision making about surveillance by creating a Special Advocate to argue "in support of legal interpretations that protect individual privacy and civil liberties" at the FISC. The Special Advocate would have the ability to request participation of amici curiae and could hire expert technologists to help ensure that the FISC is fully conversant in relevant issues and technologies.

IV. Transparency of Surveillance Law

The company surveillance principles and Necessary and Proportionate principles both call for transparency in surveillance laws and for transparency of significant decisions interpreting them. According to the company principles, "governments should allow important rulings of law [regarding surveillance] to be made public in a timely manner so that the courts are accountable to an informed citizenry." The Necessary and Proportionate "Legality" principle would prohibit states from adopting or implementing, "... a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act" that is clear and precise. The Necessary and Proportionate principle of "Due Process" likewise requires "lawful procedures that govern any interference with human rights [be] properly enumerated in law, consistently practiced, and available to the general public." In addition, the Necessary and Proportionate "Transparency" principle says that, "States should provide individuals with sufficient information to enable them to fully comprehend the scope, nature and application of the laws permitting communications surveillance." This would necessitate the public release of judicial rulings that determine the bounds and nature of surveillance law.

The USA FREEDOM Act would require the Attorney General to publicly disclose all FISC decisions, and appeals of such decisions, that contain a significant interpretation of law, and establishes a process for such disclosure. The Special Advocate would be permitted petition to the FISA Court of Review if he or she believes a ruling containing a significant interpretation of law has not been disclosed or if a summary of the ruling was disclosed but was inadequate.

---

[5] *See*, Statement of former Judge Robertson, Privacy and Civil Liberties Oversight Board, Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act (July 9, 2013), available at http://www.pclob.gov/SiteAssets/9-july-2013/Public%20Workshop%20-%20Full.pdf ("anybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding. It's quite common, in fact it's the norm to read one side's brief or hear one side's argument and think, hmm, that sounds right, until we read the other side"); *see also*, Lauren Henry, The Center for Democracy and Technology, *Former Judge Slams Foreign Intelligence Surveillance Court Procedures* (July 10, 2013), *available at* https://www.cdt.org/blogs/1007former-judge-slams-foreign-intelligence-surveillance-court-procedures.

[6] See, *Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) of October 3, 2011*, fn 14, *available at* https://www.eff.org/sites/default/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf.

V. Transparency of Surveillance Demands

The company surveillance principles and Necessary and Proportionate principles both call for permitting companies to disclose the number and nature of government surveillance demands made of them, and for governments to disclose the number and nature of the surveillance demands they make. According to the company principles, companies should be allowed to "publish the number and nature of government demands for user information" that they receive. The Necessary and Proportionate principle of "Transparency" says that, "States should enable service providers to publish ... records of State communications surveillance."

Both sets of principles also support transparency by requiring government reporting on surveillance activities. The company principles state that governments should be required to publicly disclose the number and nature of government demands for user information. The Necessary and Proportionate "Transparency" principle says that governments should publically provide, "aggregate information on the number of requests approved and rejected...."

The Necessary and Proportionate transparency principles go further than do than the company principles. First, they call for government reporting to include "a disaggregation of the requests by service provider and by investigation type and purpose." The company principles do not. Second, they call for independent oversight to ensure that the government has been transparent and accurate in publishing information about its surveillance activities.

The USA FREEDOM Act would promote the transparency for which both sets of principles call. The legislation would permit companies to report quarterly an estimate of the number of government surveillance orders received and complied with, and the number of users whose information was requested. These company reports could categorize information based upon the different legal authorities used. It would also require the government to publicly report the number orders issued, and the number of U.S. persons and non-U.S. persons who are monitored, under the various FISA authorities.

VI. Addressing Conflicting Legal Demands

The flow of data across borders can cause the same piece of data to be the subject of conflicting legal demands by two countries. Country X might demand that a communications service provider disclose the data under the laws of Country X, and Country Y might require that the same piece of data be protected against disclosure under the laws of Country Y. The company surveillance principles and the Necessary and Proportionate principles call for resolving these conflicts through improved mutual legal assistance treaty (MLAT) processes. The company principles state, "In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved mutual legal assistance treaty — or 'MLAT' — processes." The Necessary and Proportionate principle of "Safeguarding for International Cooperation" likewise contemplates a reformed MLAT process to address these conflicts, but goes further, declaring that "the mutual legal assistance treaties (MLATs) and other agreements entered into by States should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied." Note, however, that MLATs address trans-border government requests for data for criminal purposes only. Thus, while improved MLAT processes will provide some aid, they will not

resolve conflict of law issues that arise when data is sought for national security/intelligence purposes. The USA Freedom Act does not address conflicting legal demands.

VII. Balancing Government Needs With Individual Privacy Rights

The company surveillance principles and the Necessary and Proportionate principles both call for balancing government needs with individual privacy rights with regard to surveillance activities. According to the first company principle, governments should "balance their need for [user] data in limited circumstances" with "users' reasonable privacy interests and the impact on trust in the Internet." The civil society groups' principle of "Proportionality" indicates that, "Decisions about communications surveillance must be made by weighing the benefit sought to be achieved against the harm that would be caused to the individual's rights and to other competing interests...." Thus, both sets of principles call for a balance between government needs for surveillance on the one hand and privacy and other interests on the other. Among those other interests, according to the companies, is trust in the Internet and according to the civil society groups' principles, free expression and other rights. The overall purpose of the USA Freedom Act is to re-balance government needs and individual privacy rights.

VIII. Conclusion

Common goals and features of the company surveillance principles and the Necessary and Proportionate principles suggest ample ground for moving forward with a meaningful surveillance reform that both companies and civil society would support.

Where the company and civil society principles differ, there is room for further discourse and effort to come to a common understanding. For example, the company principles call for governments to refrain from making demands that companies locate data within national borders and call for protecting the free flow of data across national borders. The Necessary and Proportionate principles do not reject data localization per se, but they call for states to refrain from compelling software and hardware producers to build surveillance or monitoring capabilities into their products. Both are technology mandates designed to facilitate surveillance. On the other hand, the Necessary and Proportionate principles call for restrictions against discrimination, requiring notification of surveillance to users, and safeguards against illegal surveillance such as criminal penalties, whistleblower protections, and rules to exclude from legal proceedings the product of surveillance conducted illegally. The company principles do not call for these reforms.

Where the principles are in agreement – clarity of the law and codification, particularity of surveillance demands, independent judicial oversight, transparency about surveillance, MLAT reform, and balancing government needs with privacy – there can be a concerted, joint effort. It ought to include support for the USA FREEDOM Act, which would promote many of these reforms. Additional legislation in the U.S. and abroad, and additional administrative actions, will be needed to fully implement the surveillance principles. Enacting such measures will protect rights, support business growth, and preserve the development of a free and open Internet.

For additional information, please contact CDT's Greg Nojeim, Director of the Project on Freedom, Security & Technology (gnojeim@cdt.org, 202/637-9800), or Jake Laperruque, Privacy, Security and Surveillance Fellow (jake@cdt.org, 202/637-9800).

CHART COMPARING NECESSARY & PROPORTIONATE PRINCIPLES, TECH COMPANY PRINCIPLES, AND THE USA FREEDOM ACT

	Necessary and Proportionate Principles	Tech Company Principles	USA FREEDOM Act
Clarity and Codification of Surveillance Law	Any interference with privacy must be pursuant to clear legislative acts sufficiently precise to give users notice of how they will be applied	Compelled disclosure or collection of user data should be done under a clear legal framework; codify limits on compelled disclosure	Clarifies surveillance law in several ways, including the standard under Section 215 of the PATRIOT Act
Particularized as Opposed To Bulk Surveillance	"When there are multiple means" of engaging in communications surveillance, governments should engage in "the means least likely to infringe upon human rights."	"Governments should limit surveillance to specific, known users for lawful purposes, and should not undertake bulk data collection of Internet communications."	Records sought under intelligence statutes must pertain to a suspected agent of a foreign power, his activities, or someone in contact with or known to such person. Relevance to an investigation is not enough.
Independent Judicial Oversight That is Adequately Informed	Surveillance should require authorization by "a competent judicial authority that is impartial and independent," with review courts being "conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights...."	Surveillance activities should be "subject to strong checks and balances," courts that review surveillance should be "independent and include an adversarial process."	The USA FREEDOM Act would better ensure that reviewing courts are adequately informed by creating an adversarial process at the FISC and by creating a Special Advocate tasked with vigorously advocating "in support of legal interpretations that protect individual privacy and civil liberties."
Transparency of Surveillance Law	"Lawful procedures that govern any interference with human rights [be] properly enumerated in law, consistently practiced, and available to the general public."	"Governments should allow important rulings of law [regarding surveillance] to be made public in a timely manner so that the courts are accountable to an informed citizenry."	The USA FREEDOM Act would establish a procedure for the public release of key judicial rulings regarding surveillance law in a timely manner, with necessary redactions for security purposes and oversight by the Special Advocate.
Transparency of Surveillance Activities	"States should be transparent about the use and scope of communications surveillance techniques and powers," through mandatory government reporting and permitted company reporting.	"Transparency is essential to a debate over governments' surveillance powers," and should be achieved through mandatory government reporting and permitted company reporting.	The USA FREEDOM Act would enhance transparency through mandatory government reporting and permitted company reporting, including details on the degree to each surveillance authority is employed and the number of individuals affected.
Addressing State Legal Demands that Conflict	"The mutual legal assistance treaties (MLATs) and other agreements entered into by States" should be used to resolve conflicts of law regarding surveillance in a manner that best protects privacy.	"In order to avoid conflicting laws, there should be a robust, principled, and transparent framework to govern lawful requests for data across jurisdictions, such as improved [MLAT] processes."	No provision.
Balancing Government Needs With Individual Privacy Rights	"Decisions about communications surveillance must be made by weighing the benefit sough to be achieved against the harm that would be caused to the individual's rights."	It is essential to "balance [governments'] need for the data in limited circumstances" with "users' reasonable privacy interests."	The central goal of the legislation is to balance government needs with individual privacy, providing government with strong investigative authority, but establishing a variety of checks to ensure that surveillance is limited to necessary situations.