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

GOVERNMENT SURVEILLANCE AND THE RIGHT TO PRIVACY

OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS CONSULTATION ON "THE RIGHT TO PRIVACY IN THE DIGITAL AGE"

April 1, 2014

About the Center for Democracy & Technology

The Center for Democracy & Technology (CDT) is a U.S.-based civil society organization that works globally to defend human rights and civil liberties online. We are dedicated to keeping the Internet open, innovative, and free, and we are committed to finding forward-looking and technically sound solutions to the medium's most pressing challenges. For over 20 years, since the Internet's infancy, CDT has played a leading role in shaping the policies, practices, and norms that have empowered individuals to more effectively use the Internet as speakers, entrepreneurs, and active citizens. CDT brings legal and technical expertise, thought leadership, and coalition-building skills to its work with domestic and global policy institutions, regulators, standards bodies, governance organizations, and courts.

I. Overview of Recommendations

CDT welcomes the opportunity to provide input for the United Nations High Commissioner for Human Rights' report following General Assembly Resolution 68/167, "The right to privacy in the digital age." This submission seeks to highlight specific technological and legal issues relevant to the right to privacy in the context of government surveillance. CDT emphasizes several key points to inform the High Commissioner's report:

- Human Rights Council member states have affirmed that "the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice."[1]

- The right to privacy is, without question, implicated by government communications surveillance. In addition, surveillance practices can restrict free expression and access to information, so it is necessary to consider rights to freedom of expression, freedom of association,

[1] *See* A/HRC/20/L.13, *available at* http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf.

and related rights.[2]

- Technological innovation in storage and analytical capabilities and the globalization of Internet services has enabled a new paradigm of government surveillance that relies heavily on bulk collection of communications data. National laws have failed to keep pace with this technical reality.
- Bulk collection of communications data is contrary to Article 17 of the ICCPR.
- Globalized communications technology gives governments unprecedented ability to access, analyze, and manipulate the digital communications of people who are located outside of the state's territory, therefore enabling governments to impinge on the human rights of people around the world.
- With this significant power comes extraordinary responsibility. States must embrace human rights obligations to people who are outside of the state's territory but within the state's jurisdiction, including potential targets of communications surveillance outside of the state's boundaries.
- Laws and regulations that govern surveillance lack transparency, and the interpretation of these laws is too often done in secret.
- Existing human rights treaties are adequate, but are in need of new interpretation. A dedicated special procedures mandate on the right to privacy in the digital age and a new General Comment on the right to privacy (to replace General Comment 16) may be a beneficial.

The following sections in this submission offer addition context and details to support these points. Section II gives an overview of the technological environment that enables the current surveillance paradigm. In Section III, we provide a case study of U.S. legal frameworks and surveillance capabilities, to the extent that this information is publicly available. Section IV offers a broader perspective, highlighting common themes in government "systematic access" to communications data, drawing on CDT's comparative study of regimes in 13 countries. Section V offers some final recommendations, focusing on the importance of government and corporate transparency as a starting point for meaningful discussion on the topic of surveillance and human rights and a first step towards reform. Concluding remarks are included in Section VI.

II. Introduction to the New Surveillance Paradigm

Recent revelations about the scope and scale of surveillance programs in the U.S. have highlighted what national security officials candidly admit: we have entered a "golden age" of

[2] *See* Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression, A/HRC/23/40, *available at* http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

surveillance.[3] There are at least three factors driving a paradigm shift away from particularized or targeted monitoring to systemic or bulk collection, in which government agencies seek larger and larger volumes of data, claiming that access to comprehensive data sets is necessary to find "the needle in the haystack."

First, the storage revolution and big data analytic capabilities, combined with fears about terrorism, are driving a steadily growing governmental appetite for access to data held by the private sector. Governments are demanding more data on the theory that big data analytic capabilities will allow them to extract small but crucial pieces of information from huge datasets.

Second, as Internet-based services have become globalized, trans-border surveillance has flourished, posing new challenges for human rights. As Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression Frank La Rue has stated, there is "serious concern with regard to the extraterritorial commission of human rights violations and the inability of individuals to know they might be subject to foreign surveillance, challenge decisions with respect to foreign surveillance or seek remedies."[4]

Gone are the days when intelligence agencies had to establish foreign listening posts or position satellites or antennas to capture communications that stayed largely within the country of origin. Now, in many instances, communications pass through or are stored in other countries on a routine basis. In that respect, the United States holds a unique position in terms of access to global communications data since a great deal of global communications travel over U.S. networks or are stored with U.S. cloud companies.

Third, national security legal authorities have become increasingly powerful. It has long been the case that governments have claimed greater powers to collect data in the name of national security than in ordinary criminal law enforcement cases. Following the terrorist attacks of September 11, 2001, activities conducted in the U.S. under these separate rules for national security have vastly expanded even as privacy safeguards have eroded.[5] While there is growing evidence that the United States is not alone in its intrusive surveillance practices, the Snowden leaks have provided unique insights about the U.S. that are illustrative for the broader discussion.

---

[3] *See* Dana Priest, The Washington Post, *NSA growth fueled by need to target terrorists* (July 21, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html (NSA head told his staff that, by exploiting digital technologies, they could realize "the golden age" of electronic surveillance). CDT Fellow Peter Swire (now a member of President Obama's Review Group on Intelligence and Communications Technologies) predicted this two years ago. Peter Swire and Kenesa Ahmad, CDT Blog, *Going Dark or a Golden Age of Surveillance* (November 28, 2011), *available at* https://www.cdt.org/blogs/2811going-dark-versus-golden-age-surveillance ("[W]hile government agencies claim to be worried about 'going dark' in the face of technological change, today should be understood as a 'golden age of surveillance'").

[4] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, to the Human Rights Council, at 64 (April 17, 2013), *available at* http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[5] There have been reports of close cooperation in surveillance programs and intelligence sharing between the U.S. and a number of other countries, at least some of which also engage in mass surveillance activities: (Ewen MacAskill et al, The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications (June 21, 2013), available at http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; Spiegel Online, The German Prism: Berlin Wants to Spy Too (June 17, 2013), available at http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html; Angelique Chrisafis, The Guardian, France 'runs vast electronic spying operation using NSA-style methods' (July 4, 2013), available at http://www.guardian.co.uk/world/2013/jul/04/france-electronic-spying-operation-nsa.)

III. Case Study: United States

The U.S. is engaged in ongoing mass surveillance of the world's Internet users. In place of individualized suspicion and targeted collection required by the ICCPR and other human rights agreements, the U.S. Foreign Intelligence Surveillance Court ("FISC") approves, in secret opinions, bulk surveillance programs that permit the National Security Agency (NSA) to systematically collect communications data from the global data flows that traverse U.S. networks or are stored in U.S. based "cloud" service providers. The relevant publicly enacted laws do not provide the NSA adequate authority to conduct these programs. Further, these programs operate under enormous secrecy, depriving the public of critical public debate and the ability to know under what circumstances communications may be accessed. The Foreign Intelligence Surveillance Act ("FISA") programs are supported by secret legal interpretations, further weakening oversight. Safeguards implemented by the FISC to protect rights of people within the U.S. are inadequate under the U.S. Constitution. No safeguards are provided to non-Americans outside of the U.S. The result is a surveillance regime that violates the privacy rights of people around the world.[6]

A. NSA Surveillance Under Section 215 of the PATRIOT Act

Section 215 of the PATRIOT Act has been interpreted by the FISC to permit the government to compel the largest U.S. telephone carriers to provide the NSA with records of all calls made to, from, and within the U.S. on a daily, ongoing basis,[7,8] This "metadata" paints a clear, intimate picture of a person's daily life.[9] The law's chief Congressional sponsor has strongly objected to this interpretation of the law.[10] NSA analysts query records based on a "reasonable articulable suspicion" standard, with NSA determining whether the standard is met.[11] Recently released FISC opinions reveal that there have been repeated misrepresentations to the court and systematic violations of its rules.[12]

B. NSA Surveillance Under Section 702 of FISA

Under Section 702 of FISA, the government collects the content of communications of "non-U.S. persons" reasonably believed to be outside the U.S. Section 702 permits NSA targeting to collect "foreign intelligence information," a broad term permitting surveillance to support the "conduct of foreign affairs."[13] As UN Special Rapporteur on the promotion and protection

---

[6] For a full analysis of NSA's systemic surveillance programs, see, Testimony of Leslie Harris Before the European Parliament LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, available at https://www.cdt.org/files/pdfs/LIBEtestimony24September.pdf, hereafter, CDT EU LIBE Testimony.

[7] See, Foreign Intelligence Surveillance Court Amended Memorandum Opinion (J. Eagan) of August 29, 2013, available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[8] For a full analysis of the government's interpretation of Section 215 and the details of the records and data obtained pursuant to this provision, see, CDT EU LIBE Testimony, 6-8.

[9] See, Aubra Anthony, The Center for Democracy & Technology, When Metadata Becomes Megadata: What the Government Can Learn (June 17, 2013), available at https://www.cdt.org/blogs/1706when-metadata-becomes-megadata-what-government-can-learn-metadata.

[10] See, Representative Jim Sensenbrenner, Politico, How secrecy erodes democracy (July 22, 2013), available at http://www.politico.com/story/2013/07/how-secrecy-erodes-democracy-94568.html.

[11] See, The Center for Democracy & Technology, NSA Spying Under Section 215 of the PATRIOT Act: Illegal, Overbroad, and Unnecessary (June 19, 2013), available at https://www.cdt.org/files/pdfs/Analysis-Section-215-Patriot-Act.pdf.

[12] Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates) of October 3, 2011, fn 14, available at http://tinyurl.com/Oct11FISC, hereafter, FISC October 2011 Opinion.

[13] See, definition of "foreign intelligence information," 50 U.S.C. 1801(e)(2)(B).

of the right to freedom of opinion and expression Frank LaRue has stated, "even a narrow, non-transparent, undocumented, executive use of surveillance may have a chilling effect without careful and public documentation of its use, and known checks and balances to prevent its misuse."[14]

Collection of occurs through both upstream and downstream collection techniques. PRISM governs downstream collection of information on targets through compelled disclosure by large U.S. companies. NSA's upstream program involves collection of communications on the Internet "backbone." The FISC does not review any particular acquisition or target, but rather approves Targeting and Minimization Guidelines, which offer no protection to the communications of non-citizens outside the U.S.[15]

C. Executive Order 12333

Executive Order 12333[16] offers the legal basis for additional surveillance programs outside the scope of FISA. EO 12333 specifically addresses surveillance abroad that targets non-U.S. persons. There is limited public information about how Executive Order 12333 has been interpreted by government officials, but the surveillance procedures issued under the Executive Order are designed to provide protections to U.S. citizens and residents, not to others who may be put under surveillance.[17] The Executive Order authorizes surveillance of people outside the U.S. on an incredibly broad scale: the "foreign intelligence information" that can be sought with surveillance under EO 12333 includes information about "the activities and intentions" of non-U.S. persons. This is not a meaningful limitation.

Surveillance activities likely conducted under this authority include:

- Bulk collection of location data from cell phones of people around the world.[18]
- Bulk collection of text messages of people around the world.[19]
- Collection of mass amounts of data flowing between data centers of major technology companies such as Google and Yahoo.[20]

---

[14] See A/HRC/23/40, available at http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[15] For a full analysis of the government's interpretation of Section 702, and description of its upstream and downstream collection techniques and the Targeting and Minimization Guidelines see, CDT EU LIBE Testimony, 8-12; see also, American Civil Liberties Union, Shadow Report to the Fourth Periodic Report of the United States 109th Session of the Human Rights Committee (September 13, 2013), 48-49 available at http://tinyurl.com/ACLUICCPR.

[16] The text of Executive Order 12333 is available at: http://www.archives.gov/federal-register/codification/executive-order/12333.html.

[17] See, for example, http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf and http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf.

[18] Barton Gellman and Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show*, The Washington Post (December 4, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

[19] James Ball, *NSA collects millions of text messages daily in 'untargeted' global sweep*, The Guardian (January 16, 2014), *available at* http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

- Mass collection of contact lists from personal email and instant message accounts around the world.[21]
- Data mining of massive databases containing emails, online chats, and browsing histories of millions of people.[22]
- Collection of user data available from mobile phone applications, including geographic data, address books, buddy lists, telephone logs.[23]

In addition, documents leaked by Edward Snowden also suggest that the NSA may also be engaged in:

- Cyberattacks, including a project to develop malware targeting users of Tor, a tool that enables people to communicate anonymously online.[24]
- Efforts to undermine international technical standards for encryption.[25]

Leaked documents give us a limited, fragmented view of the U.S. surveillance regime, making it difficult to assess the full scope and impact of these programs. Even as an incomplete picture, these documents offer a window into the immense capabilities that governments can develop in the current technical environment.

D. Recent Developments

There are some indications that the conversation about surveillance is evolving within the United States government. On January 17, 2014 the White House issued Presidential Policy Directive 28 (PPD 28), addressing Signals Intelligence Activities conducted by the United States government.[26] The directive places important limitations on use of non-publicly available intelligence surveillance data collected in bulk. However, while it purports to extend to people outside the U.S. the same restrictions on dissemination and retention of personal information collected through intelligence surveillance that people inside the U.S. enjoy, the PPD falls short. Civil society groups in the U.S. have offered ideas to the Intelligence Community on how PPD-28 could be implemented to extend more significant protections.

---

[20] Barton Gellman and Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, The Washington Post (October 30, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[21] Barton Gellman and Ashkan Soltani, *NSA collects millions of e-mail address books globally*, The Washington Post (October 14, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

[22] Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet,'* The Guardian (July 31, 2013), *available at* http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[23] James Glanz, Jeff Larson, and Andrew Lehren, *Spy agencies tap data streaming from phone apps*, The New York Times (January 27, 2014), *available at* http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?_r=0.

[24] Glenn Greenwald, *NSA and GCHQ target Tor network that protects anonymity of web users*, The Guardian (October 4, 2013), *available at* http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

[25] Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security*, The Guardian (September 5, 2013), *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[26] Presidential Policy Directive – Signals Intelligence Activities (PPD 28) is available at http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

On March 27, 2014, the White House released a proposal to end the Section 215 bulk telephony data collection program as it currently exists.[27] While it is promising to see the administration acknowledge the need for reform, it is still far from clear whether, and how, these reforms will be implemented and whether the implementation will significantly improve the enjoyment of privacy rights by people inside the United States and around the world. It is worth noting, though, that none of the surveillance reforms announced so far would limit the bulk collection of communications of non-U.S. persons outside the U.S.; rather, the reforms go to use of the information collected in bulk and retention and dissemination of such information.

One area where there has been no change is the way the U.S. interprets the scope of its obligations under the International Covenant on Civil and Political Rights (ICCPR). In March 2014, The United Nations Human Rights Committee reviewed US compliance with obligations under the ICCPR.[28] During the review, the U.S. government held the position that it owes no human rights obligations to people outside of U.S. territory. The issue of extraterritoriality is particularly significant in the context of communications surveillance, because contemporary technology gives the U.S. government unprecedented ability to access and manipulate the digital communications of people outside of its territory, enabling the U.S. to impinge on the human rights of people around the world. While leaked documents[29] reveal long-running debate on the topic within the government, the U.S. delegation held firm to a strictly territorial interpretation during the review. In its Concluding Observations, the Committee countered that U.S. interpretation was contrary to "the Committee's established jurisprudence, the jurisprudence of the International Court of Justice and state practice."[30] Human rights institutions must continue to press the U.S. and all other states to acknowledge and act according to their extraterritorial human rights obligations.

IV. Global Themes

United States surveillance programs have dominated the news over the last year, but governments around the world are grappling with issues of government access and the right to privacy. To better understand how governments approach this issue, CDT conducted a comparative study on "systematic access", which includes both direct access by the government to private-sector databases or networks, and government access, whether or not mediated by a company, to large volumes of data.[31] CDT commissioned reports on the laws, court decisions, and publicly available information about actual practices in thirteen countries (Australia, Brazil, Canada, China, France, Germany, India, Israel, Italy, Japan, South Korea, the United Kingdom, and the United States). A number of themes emerged, including several that are relevant to discussions about the right to privacy.

---

[27] Additional information about the proposal is available at http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m.

[28] CDT's Shadow Report for this review is available at https://www.cdt.org/report/report-nsa-surveillance-un-human-rights-committee.

[29] Charlie Savage, *US seems unlikely to accept that rights treaty applies to its actions abroad*, The New York Times (March 6, 2014), *available at* http://www.nytimes.com/2014/03/07/world/us-seems-unlikely-to-accept-that-rights-treaty-applies-to-its-actions-abroad.html.

[30] The Human Rights Committee's Concluding Observations are available at: http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fUSA%2fCO%2f4&Lang=en.

[31] CDT's paper "Systematic Government Access to Personal Data: A Comparative Analysis" is available at https://cdt.org/systematic-access.

Lack of Transparency: Government practices are difficult to assess for several reasons. First, the relevant laws are at best vague and ambiguous, and government interpretations of them are often hidden or even classified. Second, practices are often opaque; it is sometimes in the interests of both governments and companies to proceed quietly, and the companies are often prohibited from public comment. Finally, oversight and reporting mechanisms are either absent or limited in scope when they exist, and generally do not reach voluntary data sharing by companies.

Inconsistency Between Published Law and Practice: In many countries, the published law appears to say something different from what governments are reportedly doing. Even after the Snowden leaks, we lack an accurate or comprehensive understanding of systematic access because both its legal basis and actual practice are hidden from public view.

New Capabilities Strain Existing Legal Frameworks: Though governments have long required corporate entities to systematically report certain data, that information used to remain "stovepiped." Governments now have the capability to collect, store, aggregate, and analyze enormous quantities of data at low cost. The trend toward systematic collection poses challenges to the existing legal frameworks because many of the statutes regulating government access and data usage were premised on particularized or targeted collection, minimization, and prohibitions on information sharing and secondary use.[32]

These three points are interconnected. Existing laws are interpreted for contexts never imagined by the original authors. These interpretations often occur in secret and result in surveillance programs that are hidden from scrutiny. Secret programs are difficult, if not impossible, to effectively assess in the context of human rights obligations. Therefore, transparency is a necessary prerequisite for evaluating whether a state complies with its obligations under international human rights agreements.

V. Recommendations on Transparency

CDT believes that transparency is an important first step to fostering government surveillance laws, programs, and practices that respect human rights. Accordingly, we urge governments to make the following surveillance transparency reforms by adopting appropriate legislation, regulation, and practices:

- Ensure that laws authorizing surveillance are public, clear, specific, that their application is foreseeable, and that official legal interpretations of the law are published, with deletions as necessary.
- Establish independent oversight mechanisms to ensure that government reports on surveillance activities are accurate and complete.

[32] A cornerstone of the privacy framework that has guided privacy laws globally for the past 30 years is the principle that data collected for one purpose should not be used for another purpose, yet big data analytics explicitly promises to find unanticipated meanings in data. Big data equally challenges other core privacy principles. Ira Rubinstein, *Big Data: The End of Privacy or a New Beginning?* International Data Privacy Law (2013) vol. 3, no. 2 pp.74-87 ("when this advancing wave arrives, it will … overwhelm the core privacy principles of informed choice and data minimization"). See generally Christopher Kuner, Fred H. Cate, Christopher Millard, and Dan Jerker B. Svantesson, *The challenge of "big data" for data protection*, International Data Privacy Law (2012) vol. 2, no. 2 pp. 47-49.

- Compel the competent authorities to disclose the information about:
    - Which intelligence agencies/bodies are legally permitted to conduct surveillance;
    - The scope of the powers of each of those entities;
    - The process by which an intelligence agency/body is assigned these powers;
    - The judicial, ministerial, independent, or other oversight mechanisms through which redress for unlawful surveillance may be pursued;
- Compel the competent authorities to disclose information about the surveillance demands they make, collectively, on companies, including:
    - The number and nature of surveillance demands;
    - The number of user accounts affected by those demands;
    - The specific legal authority for each of those demands; and
    - Whether the demand sought communications content or non-content.
- Permit companies to disclose, with the level of detail set out above, information on surveillance demands that they receive on at least an annual basis.
- Permit companies to disclose technical requirements for surveillance that they are legally bound to install, implement, and comply with.

VI. Conclusion

In light of current global surveillance capabilities and practices, existing treaties must be interpreted to guide states in adopting rights-respecting practices. It would be beneficial for the OHCHR report to highlight the importance of increased transparency, adoption of targeted surveillance in place of bulk collection, and acceptance of extraterritorial human rights obligations by all states.

For further information, please contact CDT Policy Analyst Emily Barabas, ebarabas@cdt.org.