Comments of Human Rights Watch

For the Review Group on Intelligence and Communications Technologies

October 11, 2013

Human Rights Watch submits the following comments to the Review Group on Intelligence and Communications Technologies (Review Group) in response to its request regarding surveillance programs operated by the United States government. Human Rights Watch is an independent global organization with a presence in more than 90 countries, working to promote respect for and adherence to human rights obligations around the world.

I. Mandate and Capacity

President Obama has directed the Review Group to "assess whether, in light of advancements in communications technologies, the United States employs its technical collection capabilities in a manner that optimally protects our national security and advances our foreign policy while appropriately accounting for other policy considerations, such as the risk of unauthorized disclosure and our need to maintain the public trust."[1] Although the President's original memorandum does not mention privacy, a subsequent press statement asks the Review Group to assess the impact of current surveillance and data collection programs on the administration's "commitment to privacy and civil liberties."[2]

The United States has been a leader in promoting Internet freedom around the world and its Internet industry has become an engine of growth in today's globally connected economy. However, US credibility has been deeply undermined by recent revelations about the vast extent of its secret dragnet surveillance programs that have violated human rights, and that bear serious implications for global internet governance and economic competitiveness.

---

[1] White House Office of the Press Secretary, "Presidential Memorandum: Reviewing Our Global Signals Intelligence Collection and Communications Technologies," August 12, 2013, http://www.whitehouse.gov/the-press-office/2013/08/12/presidential-memorandum-reviewing-our-global-signals-intelligence-collec (accessed October 11, 2013).

[2] White House Office of the Press Secretary, "Statement by the Press Secretary on the Review Group on Intelligence and Communications Technology," August 27, 2013, http://www.whitehouse.gov/the-press-office/2013/08/27/statement-press-secretary-review-group-intelligence-and-communications-t (accessed October 11, 2913).

The summer of 2013 has been marked by a familiar pattern: a press disclosure suggests previously unknown government surveillance or data collection programs. This is followed by assurances from the Obama administration that the National Security Agency's surveillance programs are targeted, proportional, and subject to oversight. Documents then emerge that undermine this narrative. The pattern then repeats itself, undermining public trust in government's commitment to human rights.

We hope the Review Group can play a role in reversing this pattern. Its mandate requires it to examine whether existing safeguards and oversight mechanisms adequately protect rights. As a threshold matter, greater transparency about key aspects of the program is crucial to the examination. A meaningful public debate about whether current surveillance practices are justified is simply not possible without a fuller accounting of its elements. In addition, the Review Group's mandate includes an assessment of whether surveillance practices advance US foreign policy interests. Any pragmatic consideration of the impact of US surveillance programs on foreign policy must address their impact on US interests in promoting Internet freedom, human rights, and multi-stakeholder Internet governance. We address these issues in turn below.

II. Transparency, Oversight, and Public Accountability

HRW welcomes the opportunity to comment and make suggestions for reform. However, there are some obvious limitations in this approach. Only some information about these programs is public, or has become public through disclosures (willing, authorized, or otherwise). But many important aspects are still classified, such as how statutory authority is being interpreted and how supposed "minimization" and "targeting" procedures are being applied and enforced. Meaningful public debate about the lawfulness and proportionality of these programs will be difficult without greater public insight into these key aspects of current programs.

Excessive secrecy is one of the most problematic aspects of the US bulk surveillance programs. Some secrecy is necessary as it pertains to specific investigations. However, as the UN Special Rapporteur on freedom of expression Frank La Rue stated in his 2013 report, limitations on the right to privacy must be prescribed by law, "meeting a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee their application."[3]

The government so far has failed to plainly and fully describe what intrusions on privacy are imposed through these programs so that the public can understand and evaluate the limits on its

[3] Report of the UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, April 17, 2013 (hereinafter "April Report of the Special Rapporteur"), A/HRC/23/40, para. 83, http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed August 1, 2013).

rights. The fact that most US residents, as well as many members of Congress, did not understand the extent to which their own government had been collecting information, as revealed by the Verizon order, was the first evidence of this.[4]

When it became known how broadly the government had interpreted "relevance" under Section 215 of the Patriot Act, it was clear the level of secrecy had gone too far.[5] Even less is known about the breadth of orders currently being used to obtain communications content from Internet companies under Section 702. But given the vast sweep of the data capture and surveillance, there is little doubt that the programs lack the targeted and foreseeable nature that would ensure they are lawful and proportionate intrusions on individual privacy under international human rights law.

Though the government claims the FISA court and the congressional intelligence committees act as checks on executive powers, these checks inadequately protect against excesses or ensure democratic accountability. Only a very small group of members of Congress are apprised of the most controversial aspects of the program, and even for those that are, the information is provided in secret. In such circumstances, no incentives exist for reform because any given legislator's constituency is left in the dark and therefore is unlikely to put pressure on their representative for change. Legislators, however, are generally sensitive to public anxiety about security. Between the administration's poorly documented claims that these sweeping programs are critical for national security, and the pervasive secrecy as to their scope and operation, legislators face considerable pressure but are unable themselves to exercise any independent judgment about whether they are indeed necessary or proportionate to protecting public safety.

The FISA court, as currently constituted, also appears incapable of exercising adequate oversight. Recent disclosures have exposed numerous problems related to the court's ability to rein in the inevitable attempts by executive agencies to maximize their authority. The chief judge of the FISA court admitted that the court "does not have the capacity to investigate issues of noncompliance" and is "forced to rely upon the accuracy of the information that is provided to the Court," putting

---

[4] See Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (accessed October 11, 2013). See also, e.g., Jim Sensenbrenner, "Op-Ed: How Obama has abused the Patriot Act," *Los Angeles Times*, August 19, 2013, http://www.latimes.com/opinion/commentary/la-oe-sensenbrenner-data-patriot-act-obama-20130819,0,1387481.story (accessed October 11, 2013).

[5] The Administration has argued that collection of all metadata of all customers of a given telecommunications company meets the relevancy standard because this "category of data," when searched and analyzed, will produce information "pertinent to terrorism investigations" and because the analytic tools used to analyze the data require the collection of large volumes of metadata. See "Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act," August 9, 2013, pp. 8-15, http://www.documentcloud.org/documents/750210-administration-white-paper-section-215.html, (accessed October 11, 2013).

in question the strength of judicial oversight.[6] A 2011 FISA court opinion released on August 21 suggests an ongoing pattern of misdirection by intelligence authorities: "The court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[7] (Notably, the administration only agreed to disclose this opinion after fighting a freedom of information request for over a year.) The Honorable James Robertson, former FISA court judge, has further urged the introduction of some form of institutional public advocate at the FISA court, citing lack of sufficient safeguards to protect the interests of those on the other side of the government's argument.[8] Had there been such an institutional advocate, for example, the very broad interpretation of "relevance" under Section 215 might have been challenged, and not approved.

The court has also issued orders greatly limiting the amount of information the public could obtain about how much information the US government was collecting. The orders left the public in the dark as to whether companies had ever objected to or challenged disclosure orders.

The following sections of this document outline questions raised by the disclosures to date that the Review Group should strive to answer in its public report to the fullest extent possible, or lay the groundwork for a public account of unanswered questions that remain beyond the Review Group's tenure.

A. Section 215 of the Patriot Act

Though there are limitations to what we know about programs run under Section 215 of the Patriot Act, what we have learned recently through disclosures is deeply troubling. On its face Section 215 authorizes the government to obtain certain "tangible things" or business records so long as they are "relevant" to an authorized investigation. However, the Foreign Intelligence Surveillance Court (FISC) has interpreted this relevance requirement extremely broadly.[9] This interpretation has

---

[6] Carol D. Leonnig, "Court: Ability to police U.S. spying program limited," *Washington Post*, August 15, 2013, http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html (accessed October 11, 2013).

[7] October 3, 2011 FISC Opinion Holding NSA Surveillance Unconstitutional, Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates), October 3, 2011, note 14, https://www.eff.org/document/october-3-2011-fisc-opinion-holding-nsa-surveillance-unconstitutional (accessed October 11, 2013).

[8] Hon. James Robertson, Ret., oral comments to the 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, http://www.pclob.gov/SiteAssets/9-july-2013/Public%20Workshop%20-%20Full.pdf (accessed October 11, 2013).

[9] See Office of the Director of National Intelligence, "Primary Order for Business Records Collection Under Section 215 of the USA PATRIOT Act," July 31, 2012, http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf (accessed

apparently led the court to authorize the National Security Agency (NSA) to collect all call detail record or "telephony metadata" created by the US telecommunications company, Verizon, and others.[10] Metadata, while not including the substantive content of communications, can be highly revealing, demonstrating patterns of behavior, associations, and beliefs, especially when collected at large scale.

Congressman Jim Sensenbrenner (R-WI), author of the PATRIOT Act, has argued that "seizing phone records of millions of innocent people is excessive and un-American."[11] Congressman Sensenbrenner has filed an amicus brief in a lawsuit against administration officials to argue that such bulk collection of phone records violates the Patriot Act and Congress's clear intent in enacting Section 215.[12]

The government claims that the metadata being collected cannot be "queried"—that is, searched or processed in some way—unless there is a reasonable suspicion that a particular telephone number is associated with a specified foreign terrorist organization.[13] Even then, the government claims that it can only be queried to identify contacts of the telephone number associated with the specified foreign terrorist organization. Follow-up investigations resulting from analysis of metadata, such as surveillance of particular US telephone numbers, the government claims, requires a traditional FISA court order based on probable cause that the person under investigation is an agent of a foreign power.[14]

However, many of the details of these alleged limits are not in the statute. They may be in the purported "minimization procedures," but the full content of these procedures have not been made public. The government claims that only a small portion of the data that is collected under Section 215 is actually ever reviewed because the vast majority of data is never going to be responsive to terrorism-related queries. For example, in 2012 the Office of the Director of National

---

October 11, 2013); Jennifer Valentino-Devries and Siobhan Gorman, "Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering," *The Wall Street Journal*, July 8, 2013, http://online.wsj.com/article/SB10001424127887323873904578571893758853344.html (accessed July 25, 2013); Eric Lichtblau, "In Secret, Court Vastly Broadens Powers of N.S.A.," *The New York Times*, July 6, 2013, http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all& (accessed July 31, 2013).

[10] Ibid.

[11] Congressman Jim Sensenbrenner, "Press Letter: Author of Patriot Act: FBI's FISA Order is Abuse of Patriot Act," June 6, 2013, http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=337001 (accessed October 11, 2013).

[12] Congressman Jim Sensenbrenner, "Press Release: Sensenbrenner and NRA Support ACLU Lawsuit," September 6, 2013, http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=347782 (October 11, 2013).

[13] Robert Litt, General Counsel for Office of Director of National Intelligence, Prepared Remarks for an address on "Privacy, Technology and National Security: An Overview of Intelligence Collection," at the Brookings Institution, July 19, 2013, http://www.lawfareblog.com/wp-content/uploads/2013/07/Bob-Litt-Brookings-Speech1.pdf (October 11, 2013).

[14] Ibid.

Intelligence has said fewer than 300 "identifiers" were approved searching this data. What is actually meant by the term "identifiers," and how many individuals an identifier may implicate, is not yet fully clear. However, millions of people may be subject to scrutiny through their metadata, which can expose their network of contacts and connections, because analysts are entitled to extend their collection and analysis three "hops" from the original target.[15] The FISA court itself has questioned the efficacy of safeguards in the past, finding in 2009 that the "NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been 'so frequently and systematically violated that it can fairly be said that this critical element of the overall … regime has never functioned effectively.'"[16]

The claim that *all* metadata may be lawfully collected as "relevant" to an authorized investigation strains any common or reasonable interpretation of "relevant." Similarly, the notion that data is not "collected" until it is searched strains any common or reasonable interpretation of the word "collect." The injury to personal privacy, and consequently to freedom to associate, speak, get information, or act according to one's conscience, begins at the moment the government seizes a communication, regardless of when, whether or how the government decides to analyze it.

Furthermore, if collection of all telephony metadata, even with limitations on further use, is deemed acceptable, where does the line between permissible and impermissible collection end? Senator Ron Wyden (D-Ore.), who sits on the Senate Intelligence Committee and therefore has far more knowledge about the capacities of the program than the general public, has warned, for example, that medical records, financial records, school records, and records of credit card purchases, could be subject to bulk collection under current interpretations of Section 215 of the Patriot Act.[17]

In order for the Review Group to do a comprehensive review of this program to evaluate its lawfulness, necessity, and proportionality, we urge it to determine and report publicly on the following:

---

[15] See Philip Bump, "NSA Admits it Analyzes More People's Data than Previously Revealed," *The Atlantic Wire*, July 17, 2013, http://www.theatlanticwire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287 (accessed October 11, 2013).

[16] October 3, 2011 FISC Opinion Holding NSA Surveillance Unconstitutional, Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates), October 3, 2011, https://www.eff.org/document/october-3-2011-fisc-opinion-holding-nsa-surveillance-unconstitutional (accessed October 11, 2013), note 14 (internal citation omitted).

[17] Remarks of Senator Ron Wyden (D-Ore.), "Remarks As Prepared for Delivery for the Center for American Progress Event on NSA Surveillance," July 23, 2013, http://www.americanprogress.org/wp-content/uploads/2013/07/7232013WydenCAPspeech.pdf (accessed July 25, 2013).

- What specific current and past "minimization procedures" have been applied to data collected under this program? How greatly have they in fact narrowed communications subject to surveillance or limited the amount of metadata that is further scrutinized? What safeguards are applied when deciding how to access and use the data collected?
- How long may various kinds of data be retained?
- How is data transferred or shared between government agencies, and under what legal authority or criteria if any?
- The recently disclosed 2009 report from the Department of Justice Inspector General on the government's data collection programs indicates that a program in which bulk Internet metadata was collected ended in 2011. Redacted documents disclosed by the Director of National Intelligence on July 31, 2013 describe bulk collection programs conducted under both Section 215 of the Patriot Act and Section 402 of FISA.[18] What other bulk metadata collection, if any, is being or has been conducted under Section 215 of the Patriot Act or under any other authority? Can the Review Group clarify whether authorities are collecting any kind of Internet metadata in bulk under Section 215 or any other existing legal authority?
- How many and what kinds of other companies are required to produce bulk metadata information or other information under Section 215 of the Patriot Act or other authorities?
- To what extent are authorities compelling online service providers or other companies to disclose encryption keys under Section 215 or any other legal authority?

B. Section 702 of the FISA Amendments Act of 2008 and Upstream Collections

Unlike Section 215 of the Patriot Act, Section 702 of the FISA Amendments Act of 2008 does authorize the collection and surveillance of the content of communications. Under Section 702, the attorney general and director of national intelligence may issue one-year blanket authorizations for surveillance of non-citizens who are "reasonably believed" to be outside the United States ("non-US persons") in order to acquire "foreign intelligence information." The FISA court is tasked with approving safeguards (targeting and minimization procedures) ostensibly aimed at protecting US person communications "inadvertently" captured as part of the targeting of foreigners. However, these procedures, a 2009 version of which was leaked to the press (hereinafter "targeting procedures" and "minimization procedures"),[19] fail to adequately protect privacy interests of both US persons and non-US persons alike. Contrary to misleading or

[18] Office of the Director of National Intelligence, "DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents," July 31, 2012, http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf (accessed August 1, 2013).

[19] Glenn Greenwald and James Ball, "The Top Secret Rules that Allow NSA to Use US Data Without a Warrant," *The Guardian*, June 20, 2013, http://www.guardian.co.uk/world/2013/jun/20/fisa-court-nsa-without-warrant (accessed July 29, 2013).

misinformed public statements by US officials,[20] the procedures provide weak protections for US persons and no protection for the privacy interests of non-US persons.

The purpose of the targeting is supposed to be to gather "foreign intelligence information," but that term is defined very broadly. For example, for a non-US person, the communication need only "relate to" terrorism, intelligence activities of another government, the national defense, or the foreign affairs of the United States in order to be considered foreign intelligence information.[21] Even then, when looking at whether a particular foreign target is likely to communicate foreign intelligence information, the targeting procedures only require an assessment that the target is "associated" with, "has communicated" with, or is "listed in the telephone directory of," among other factors, "a foreign power or territory."[22] Also, the procedures state that the target is "presumed" to be a non-US person, unless such person can be positively identified as a US person or the nature and circumstances of the person's communications give rise to a reasonable belief that such a person is a US person.[23] For US persons, the standard, in the statute at least, is a bit higher, requiring the communication must be "necessary to" terrorism, intelligence activities of another government, the national defense or the foreign affairs of the United States in order to be considered foreign intelligence information.[24] Additionally, though communications about these issues may be targeted, it is not just the communications of individual targets that can be the subject of the surveillance but communications "about" the targets as well—potentially encompassing a very broad swath of communications.[25]

Furthermore, the entire program is based on the assumption that non US-persons abroad have far fewer privacy rights, if any, than US persons, a position with which Human Rights Watch strongly disagrees. There may be a strong state interest in subjecting specific foreign communications to surveillance. However, such intrusions on privacy rights must be narrowly tailored and

---

[20] Office of the Director of National Intelligence, "DNI Statement on Activities Authorized Under Section 702 of FISA," June 6, 2013, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa (accessed August 1, 2013); see also, Office of the Director of National Intelligence, "DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," June 8, 2013, http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/872-dni-statement-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act (accessed August 1, 2013).

[21] 50 USCA § 1801(e).

[22] "Procedures Used By The National Security Agency For Targeting Non-United States Persons Reasonably Believed To Be Located Outside The United States To Acquire Foreign Intelligence Information Pursuant To Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended," (hereinafter "targeting Procedures"), p. 4, http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document (accessed July 30, 2013).

[23] Ibid.

[24] 50 USCA § 1801(e).

[25] Targeting procedures, p. 1.

proportional to the particularly weighty state interest being protected and should not be based on arbitrary distinctions such as citizenship or non-citizenship of any particular state. Even in the case of US citizens, though the procedures call for domestic communications to be promptly destroyed, the content can be retained if it includes significant foreign intelligence information, evidence of a crime or a serious threat to life or property, technical information necessary to understand or assess communications, or encrypted information—all of which could implicate potentially broad swaths of communications.[26] Furthermore it is NSA analysts who make decisions on retention and on foreign targets with apparently scant ongoing review by the FISA court for compliance with targeting or minimization procedures.

In order for the Review Group to conduct a comprehensive review of this program to evaluate its lawfulness, necessity and proportionality, we hope it can determine and publicly report on the following:

- Greater clarity on, including specific descriptions of, the minimization and targeting procedures that are currently in place, as well as those that had been in place previously.
- The scope and breadth of the orders issued to Internet companies under FAA Section 702, including the number of individual users or accounts impacted by orders to the Internet companies named in the disclosed PRISM slides under this authority annually.
- To what extent is fiber optic cable tapping happening, where is it happening, how is it implemented from a technical perspective, and under what legal authority? What minimization or targeting procedures apply to this tapping if any? Are there any shortcomings in these procedures? Are they evaluated in any way on a periodic basis by the FISA court?
- The results of any auditing conducted by the DOJ or ODNI that according to the targeting procedures leaked to the media were to be conducted every 60 days.
- The results of any other audits conducted by any other oversight bodies regarding any over-collection under the authority of section 702.
- Were there any instances in which the NSA used its authority in Section V of the targeting procedures to depart from the procedures on a temporary basis to protect against an immediate threat to US national security?[27] If so, how often and what was the nature of the departure? Was the FISA court informed about these departures if any took place?

---

[26] "Minimization Procedures Used By The National Security Agency In Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended," p. 5, http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document (accessed July 30, 2013).

[27] According to a set of NSA targeting procedures released by the Guardian on June 20, 2013, the NSA may depart from the targeting procedures approved by the FISA court "in order to protect against an immediate threat to the national security," and where it is "not feasible to obtain a timely modification" of the targeting procedures. The NSA must still report the activity promptly to the DOJ and other authorities. Section V, Procedures Used by the National Security Agency

C. Justifications For Collection and Secrecy Under The Programs

The government has made the claim that there are 54 cases where the bulk metadata and Section 702 authorities have helped thwart terrorist plots, from potential bomb attacks to material support for terrorism.[28] Forty-one of the cases allegedly involved threats in other countries, including 25 in Europe.[29] However, only four specific cases have been mentioned publically.

In a Senate Judiciary Committee FISA oversight hearing on October 2, General Keith Alexander confirmed under questioning by Senator Patrick Leahy (D-Vt) that of the 54 cases, only thirteen had a nexus with the US and only one or possibly two threats were thwarted as a direct result of bulk metadata collection.[30] Senator Leahy argued that citing misleading statistics to justify massive collection programs undermines the credibility of the government's arguments. Of the 54, it is unclear how many of these alleged thwarted plots were due to the information obtained under section 702 authority. Both Senators Ron Wyden (D-Ore.) and Mark Udall (D-Colo.), outspoken critics of the surveillance programs, have said "multiple" terrorist plots appear to have been disrupted at least in part because of Section 702, but the bulk phone records collection program under section 215 of the Patriot Act played little or no role.[31]

As Bob Litt, General Counsel for ODNI admitted in testimony before the House Judiciary Committee on July 17, 2013, it was clearly the intent of the administration to keep the extent of the collection and other aspects of these programs secret. When asked by Judiciary Committee Chairman Bob Goodlatte, (R-Va): "Do you think a program of this magnitude, gathering information involving a large number of people involved with the telephone companies and so on, could be indefinitely kept secret from the American people?" Litt replied: "Well, we tried."[32]

---

for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended, Exhibit A, July 28, 2009, at p. 9, http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document (accessed October 11, 2013).

[28] See Robert Litt, General Counsel for Office of Director of National Intelligence, Prepared Remarks for an address on "Privacy, Technology and National Security: An Overview of Intelligence Collection," at the Brookings Institution, July 19, 2013, http://www.lawfareblog.com/wp-content/uploads/2013/07/Bob-Litt-Brookings-Speech1.pdf(accessed July 23, 2013).

[29] Ibid.

[30] Senate Judiciary Committee Hearing, "Continued Oversight of the Foreign Intelligence Surveillance Act," October 2, 2013, video at http://www.judiciary.senate.gov/hearings/hearing.cfm?id=0c23b88fc3b21bc51f6445cd14baddfe (accessed October 11, 2013).

[31] "Wyden, Udall Issue Statement on Effectiveness of Declassified NSA Programs," June 19, 2013, http://www.wyden.senate.gov/news/press-releases/wyden-udall-issue-statement-on-effectiveness-of-declassified-nsa-programs (accessed July 23, 2013).

[32] Ryan Abbott, "Congress Up in Arms Over NSA Surveillance," *Courthouse News Service*, July 18, 2013 http://www.courthousenews.com/2013/07/18/59497.htm, (accessed July 30, 2013).

Given the enormous public interest in what data or communications the US government is able to collect about its citizens, let alone from others around the globe, as well as in how the government retains or uses that information, it is hard to understand what national security interest might be strong enough to justify the levels of secrecy around these two programs. Certainly the evidence put forward so far on actual threats directly prevented by these programs is hazy and slight. However, we urge the Review Group to gather information that will provide greater clarity about how necessary and effective information obtained under Section 215 and Section 702 respectively has been in protecting the United States against terrorism and whether such information or similar information would have been obtainable by alternate means, in order to provide objective analysis about the alleged justifications under the programs.

III. Impact on Internet Freedom, Human Rights, and Global Internet Governance

The impact surveillance programs have on fundamental human rights and on Internet governance policies globally should be of concern to the Review Group and fall within the Review Group's mandate.

A. Internet Freedom and Human Rights

Since at least 2010, the Obama administration has made Internet freedom a signature foreign policy priority.[33] The US has been instrumental in attracting allies to take part in the Freedom Online Coalition[34] of governments and promoting human rights online at key international venues like the UN Human Rights Council and the Internet Governance Forum. In 2013 alone, the State Department and USAID awarded $25 million to "groups working to advance Internet freedom -- supporting counter-censorship and secure communications technology, digital safety training, and policy and research programs for people facing Internet repression."[35]

Today, however, the US government's ability to promote Internet freedom at the global level has been deeply undermined by revelations about US surveillance programs. By ignoring the privacy interests of non-US persons, in both law and rhetoric, the US has alienated key allies and

[33] See Secretary of State Hillary Rodham Clinton, "Remarks on Internet Freedom," Washington, DC, January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm (accessed October 11, 2013).

[34] The Freedom Online Coalition is a group of around 20 governments who have made public commitments to promote Internet freedom. The coalition coordinates action at international venues and in response to specific developments. See, e.g., Freedom Online Coalition, "Joint Statement on the Socialist Republic of Vietnam's Decree 72," August 26, 2013, http://www.state.gov/r/pa/prs/ps/2013/08/213505.htm (accessed October 11, 2013). See also U.S. Department of State, "Fact Sheet: Freedom Online Coalition," November 20, 2012, http://www.humanrights.gov/2012/11/20/fact-sheet-freedom-online-coalition (accessed October 11, 2013).

[35] U.S. Department of State, "Internet Freedom," undated, http://www.state.gov/e/eb/cip/netfreedom/index.htm (accessed October 1, 2013).

undermined its moral standing on Internet freedom, making diplomatic efforts to challenge abuses to the right to privacy and freedom of expression abroad less effective.

Since 1992, the United States has been a party to the International Covenant on Civil and Political Rights (ICCPR) and other international treaties, which obligate it to recognize and protect, among other rights, the right to privacy, free expression, and free association.[36] A 2011 UN Human Rights Council resolution affirmed that "the same rights that people have offline must also be protected online."[37] Although these rights may be subject to certain restrictions, these are universal rights held by US citizens and non-US citizens alike, both within and outside US territory.

Article 17 of the ICCPR guarantees the right to be free from arbitrary and unlawful interference with privacy and "correspondence," a term that is authoritatively interpreted to encompass all forms of communication, both online and offline.[38] These rights must be upheld by governments wherever they exercise their sovereign powers, and they apply to all categories of persons.[39] These rights are essential to the functioning of any free democracy, but they are also not absolute. They may be subject to certain restrictions for reasons necessary for national security or the maintenance of public order. However, any restrictions must not be arbitrary or unlawful—that is, they must be prescribed by law, proportionate, and narrowly tailored to achieve a legitimate aim.[40]

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, stated in his April 2013 report, "[i]nadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion

---

[36] International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, G.A. Res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, entered into force March 23, 1976, ratified by the United States on June 8, 1992, http://www.ohchr.org/english/countries/ratification/4.htm (accessed July 31, 2013).

[37] United Nations Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet," Resolution 20 (2012), U.N. Doc A/HRC/20/L.13, http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf (accessed October 11, 2013).

[38] ICCPR, art. 17; also, April Report of the Special Rapporteur, *supra* note 3, para. 24 (omitting citation), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed August 1, 2013).

[39] According to the General Comment No. 31 of the ICCPR by the Human Rights Committee, the body that monitors international compliance with the ICCPR, "a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party." The General Comment further states that "the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons." UN Human Rights Committee, General Comment No. 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (2004), at para. 10, http://www.unhchr.ch/tbs/doc.nsf/0/58f5d4646e861359c1256ff600533f5f (accessed August 1, 2013).

[40] April Report of the Special Rapporteur, *supra* note 3, para. 29.

and expression."[41] While the US's Internet freedom agenda has largely focused on the rights of freedom of expression, association, and assembly, protecting the right to privacy is fundamental for the enjoyment of these rights and cannot be separated.[42]

Recent revelations also suggest that the government may be systematically undermining international encryption standards and security practices adopted by online service providers.[43] This represents not only a severe breach in public trust, but a sharp example of policy incoherence within the US government. Through programs run by the State Department, USAID, and the Broadcasting Board of Governors, the US has spent over $100 million on security training and the development of privacy tools used by Internet activists and human rights defenders all around the world.[44] If the revelations are true, then the US government has acted to weaken the security of all Internet users, including those online activists in closed societies that the US has spent millions to protect. As security expert Bruce Schneier has explained, "[the NSA is] deliberately weakening Internet security for everyone—including the good guys. It's sheer folly to believe that only the NSA can exploit the vulnerabilities they create."[45]

The widening gap between what the US promotes and what it actually practices has damaged the government's ability to advance core foreign policy goals. The US must lead by example or risk undermining gains made to the promotion of Internet freedom at the global level. How vigorously this Review Group, Congress, and other relevant bodies review and reform the surveillance programs at issue will set a standard for oversight and the protection of the right to privacy and civil liberties for countries around the world going forward.

Human Rights Watch urges the Review Group to conduct a comprehensive review of current surveillance programs to evaluate their lawfulness, necessity, and proportionality, and their impact on core foreign policy goals like Internet freedom. The UN Special Rapporteur's report provides guidance in this regard.[46] We ask the Review Group to make recommendations on the reforms necessary to ensure the programs' consistency with both US constitutional requirements

---

[41] April Report of the Special Rapporteur, *supra* note 3, para. 3.

[42] April Report of the Special Rapporteur, *supra* note 3, paras. 19-24.

[43] See Nicole Perlroth, Jeff Larson, and Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," *New York Times*, September 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html (accessed October 11, 2013).

[44] See U.S. Department of State, Internet Freedom, undated, http://www.state.gov/e/eb/cip/netfreedom/index.htm (accessed October 11, 2013). See also, Broadcasting Board of Governors, "Internet Anti-Censorship Fact Sheet," May 2013, http://www.bbg.gov/wp-content/media/2013/05/Anti-Censorship-Fact-Sheet-May-2013.pdf (accessed October 11, 2013).

[45] David Talbot, "Bruce Schneier: NSA Spying Is Making Us Less Safe," *MIT Technology Review*, September 23, 2013, http://www.technologyreview.com/news/519336/bruce-schneier-nsa-spying-is-making-us-less-safe (accessed October 11, 2013).

[46] April Report of the Special Rapporteur, *supra* note 3.

and US obligations under human rights law. To the extent a comprehensive review isn't possible within the Review Group's tenure, we ask that the Review Group make recommendations for ensuring greater transparency and disclosure so that such a review can be taken forward by other actors, including Congress or the Privacy and Civil Liberties Oversight Board.

B. Corporate Responsibility and Access to Redress

As the United Nations recognized in 2011, companies have a responsibility to respect human rights and ensure they do not contribute to abuses.[47] HRW is a founding member of the Global Network Initiative (GNI), an organization that has established standards for corporate responsibility in the technology sector for the rights of freedom of expression and privacy.[48] Several major Internet companies named in disclosures about the PRISM program are also members of the GNI. Under the GNI's standards, companies have a responsibility to resist arbitrary and overbroad government requests for information about their users. The US government has been a strong advocate for the GNI's objectives and work, especially as US-based Internet companies expand globally.[49]

Human Rights Watch is concerned that the US has now provided a roadmap to all governments for how to secretly enlist information and communications technology (ICT) companies in mass collection of user data. Other governments are likely to demand the same access to user communications and data that the US commands, making it more difficult for US-based companies to resist overbroad requests wherever they operate—undermining a key component of the US's Internet freedom agenda. Allegations that the US may be demanding ICT companies to hand over encryption keys or deliberately weaken security practices, while forbidding companies from reporting on these demands, only exacerbate the problem.

To meet their responsibility under the GNI and international human rights standards, HRW has urged Internet and telecommunications firms to regularly report on the number of government requests for user data they receive around the world, as well as how companies respond to those requests. Several US Internet companies now issue such "transparency reports."[50] This

---

[47] UN OHCHR, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework," UN Doc. HR/PUB/11/04, 2011, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf (accessed August 1, 2013).

[48] Global Network Initiative, "Core Commitments," undated, http://www.globalnetworkinitiative.org/corecommitments/index.php (accessed August 1, 2013).

[49] See Assistant Secretary of State for Democracy, Human Rights, and Labor Michael H. Posner, "Internet Freedom and the Digital Earthquake of 2011," Remarks to the State of the Net Conference, Washington, DC, January 17, 2012, http://www.humanrights.gov/2012/01/17/internet-freedom-and-the-digital-earthquake-of-2011 (accessed October 11, 2013).

[50] See, for example, "Google Transparency Report," Google, http://www.google.com/transparencyreport (accessed July 29, 2013); "Twitter Transparency Report," Twitter, https://transparency.twitter.com/ (accessed July 29, 2013); "2012 Law

information is important not only to hold companies accountable where they contribute to abuses, but also to discourage overbroad or arbitrary use of surveillance powers by governments. HRW believes the same principle applies to these companies' operations in the US. The Review Group should examine and make recommendations for how to remove barriers on disclosure around how companies are responding to government requests for interception, access to metadata, or access to the content of communications. It should also examine whether third parties, such as companies, have a reasonable form of recourse and transparency if they believe a government order for information is too broad or poses a serious risk to human rights.

The Review Group should also recommend procedures to allow companies to notify users when their information has been divulged under FISA, National Security Letter statutes, or other authorities. As the UN Special Rapporteur Frank La Rue stated in his 2013 report to the Human Rights Council, such notification is critical to enabling individuals to challenge unlawful practices where they occur and to seek redress.[51]

In 2008, Human Rights Watch joined Amnesty International and other human rights and labor organizations to challenge the constitutionality of Section 702 of the FISA Amendments Act. In its February 26 opinion in *Clapper v. Amnesty*, the Supreme Court rejected the challenge based on lack of standing, arguing that because the surveillance was secret, the organizations could not prove that they were under surveillance.[52] This opinion effectively shielded the United States' national security surveillance policies from judicial review and presents a major barrier for redress.[53]

We recognize that advance or concurrent notification may not be possible while an investigation is ongoing. However, the Review Group should make recommendations on procedures for imposing a reasonable time limit on gag orders or other limitations on disclosure imposed on companies. When that time limit has run, government authorities should bear the burden of demonstrating to the FISA court that an immediate national security interest outweighs the public interest in disclosure of the request.

C. Global Internet Governance

Enforcement Requests Report," Microsoft, https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (accessed July 29, 2013).

[51] April Report of the Special Rapporteur, *supra* note 3, para. 82.

[52] *Clapper v. Amnesty Int'l USA*, No. 11–1025, slip op. (U.S. Feb. 26, 2013).

[53] In light of new information about the breadth of metadata collection revealed by the disclosed Verizon order, Human Rights Watch has joined a broad coalition of organizations to challenge bulk metadata collection programs as unconstitutional. See Electronic Frontier Foundation, "Unitarian Church, Gun Groups Join EFF to Sue NSA Over Illegal Surveillance," July 16, 2013, https://www.eff.org/press/releases/unitarian-church-gun-groups-join-eff-sue-nsa-over-illegal-surveillance (accessed October 11, 2013).

In 2012, the US played a critical role in ensuring the International Telecommunication Union's World Conference on International Telecommunications treaty negotiation did not result in international telecommunications regulation that would have undermined the very nature of the free and open Internet.[54] This treaty conference was only the latest episode in a much larger debate over how the Internet should be governed, whether through a top-down, government-centric model or through the current multi-stakeholder model (with civil society, industry, and governments each playing a meaningful role).[55] In all these efforts, the US, along with its allies, has acted as a critical counterweight to those states that would move away from the multi-stakeholder model of governance or transform the Internet into a convenient tool for those governments bent on repression and control.

The recent revelations have alienated key allies and actors in this debate. Though the Internet was born in the US, the revelations suggest that the US has been a poor steward of an increasingly global resource. There is a growing perception that the US is exploiting its unique position within the Internet's ecosystem: the most popular online service providers store most of their data within US territory and much of the world's Internet traffic still transits through the US, giving the government unparalleled access to the world's metadata and communications. Yet the US does not recognize the privacy rights of non-Americans outside the US. This two-tiered approach to privacy, a universal right, is fueling international outrage and leading to calls for greater regulation at the international level. It is also placing pressure on technology companies to localize data storage practices to keep data out of US hands.

For example, in her opening statement to the 68th session of the United Nations General Assembly, Brazilian President Dilma Rouseff excoriated the US for its surveillance activities directed at Brazil, asserting:

> A sovereign nation can never establish itself to the detriment of another sovereign nation. The right to safety of citizens of one country can never be guaranteed by violating the fundamental human rights of citizens of another country. The arguments that the illegal interception of information and data aims at protecting nations against terrorism cannot be sustained. Brazil, Mr. President, knows how to protect itself.... We expressed to the Government of the United States our disapproval, and demanded explanations, apologies and guarantees that such procedures will never be repeated. Friendly governments and

[54] See Ellery Biddle, "What does the WCIT really mean for Internet users?" Global Voices Advocacy, December 20, 2012, http://advocacy.globalvoicesonline.org/2012/12/21/what-does-the-wcit-really-mean-for-internet-users (accessed October 11, 2013).

[55] See Assistant Secretary of Commerce for Communications and Information Lawrence E. Strickling, "Opening Session Remarks," Remarks to the Internet Governance Forum, Baku, Azerbaijan, November 6, 2012, http://www.ntia.doc.gov/speechtestimony/2012/remarks-assistant-secretary-strickling-internet-governance-forum (accessed October 11, 2013).

> societies that seek to build a true strategic partnership, as in our case, cannot allow recurring illegal actions to take place as if they are normal. They are unacceptable.[56]

President Rouseff went on to say that the UN "must play a leading role in the effort to regulate the conduct of States with regard to these technologies."[57]

In a September 25 joint communiqué from the sidelines of the UN General Assembly, the India, Brazil, and South Africa (IBSA) group of states criticized the practices revealed by the documents Edward Snowden disclosed as a "serious violation of national sovereignty and individual rights … incompatible with coexistence between friendly countries."[58] Policymakers in Brazil, Germany, and elsewhere in Europe have called for greater localization of their citizens' data to ensure better privacy protections, with serious implications for the structure and functioning of the global Internet.[59]

Just as troubling, US actions have now emboldened states that have terrible records in protecting the rights of their own residents online to demand a greater role in governing the Internet. At the 24th session of the Human Rights Council, Pakistan expressed concern about the extraterritorial impact of the US's surveillance practices and the lack of access to redress for non-US persons in a statement on behalf of a group of states that included Ecuador, Venezuela, Cuba, Zimbabwe, Uganda, Russia, Indonesia, Bolivia, Iran, and China.[60] This group of states argued that existing mechanisms like the Internet Governance Forum have not been able to "deliver desired results"—ostensibly, the monitoring of privacy abuses—and that a "strategic rethinking of the global Internet governance mechanism is inevitable," including through "enhanced cooperation." In the rarified vocabulary of Internet governance, this is a call to move away from the model of governance the US has promoted since the Internet's inception.

---

[56] President of the Federative Republic of Brazil Dilma Rousseff, "Statement at the Opening of the General Debate of the 68th Session of the United Nations General Assembly, New York, NY," September 24, 2013, http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf (accessed October 11, 2013).

[57] Ibid.

[58] "IBSA Joint Communique, New York, NY," September 25, 2013, http://www.itamaraty.gov.br/sala-de-imprensa/notas-a-imprensa/comunicado-conjunto-do-ibas-nova-york-25-de-setembro-de-2013 (accessed October 11, 2013). See also, Sandeep Dikshit, "Snooping is serious violation of national sovereignty and individual rights: Khurshid," *The Hindu*, September 27, 2013, http://www.thehindu.com/news/national/snooping-is-serious-violation-of-national-sovereignty-and-individual-rights-khurshid/article5172270.ece.

[59] See, e.g., Doug Palmer, "U.S. Lawmaker Worried NSA Snooping will Hurt Digital Trade," Reuters, Jul 24, 2013, http://www.reuters.com/article/2013/07/24/usa-trade-prism-idUSL1NoFU1OZ20130724.

[60] "Joint Statement on Right to Privacy on Behalf of Group of Countries at the 24th Session of the United Nations Human Rights Council," September 19, 2013, https://www.apc.org/en/system/files/HRC24_Pakistan_20130919.pdf (accessed October 11, 2013).

The Review Group should assess the impact of US surveillance programs and the government's failure to recognize the privacy interests of non-US persons on these critical US foreign policy priorities.

IV. Recommendations

Regarding Sections 215 and 702 we ask the Review Group to consider and incorporate the following into its recommendations to the administration:

Collection of communications metadata:

- Support legislative reforms that would prevent bulk collection of communications metadata under Section 215 or any other authority and bar use of Section 215 for prospective surveillance.
- Support reforms to ensure that minimization procedures provide robust safeguards against arbitrary or overbroad privacy intrusions, including by ensuring the scope of collection is proportionate and by imposing limitations on retention, use, and dissemination. Such procedures should apply regardless of whether the individual implicated is a US person or whether the data collection occurs inside US territory.
- Support legislative reforms removing language from Section 215 (b)(2) that allows authorities to assert that the information or "tangible thing" they are seeking is "presumptively relevant" under specific circumstances. Reforms should require that authorities must demonstrate that the tangible thing sought is relevant on its own accord.

Programmatic surveillance under Section 702:

- Support an end to programmatic warrantless surveillance under Section 702 and require the government to obtain an individualized warrant to conduct surveillance on both US persons and non-US persons, irrespective of where the surveillance occurs.
- Recommend legislative fixes to ensure more rigorous safeguards to be incorporated into minimization procedures for Section 702 that apply to the collection of the content of communications and metadata. Such safeguards should apply to *both* US and non-US persons irrespective of where the surveillance occurs and should include, for example, limitations on retention, use, and dissemination. The FISA court should play a role in ensuring that distinctions made in minimization safeguards are not based on arbitrary factors.
- If programmatic authorization continues, support meaningful review by the FISA court or another arm of the judiciary about how the procedures authorized under the program are being implemented on an ongoing basis, and to what effect.

- If programmatic surveillance continues, ensure that the category of information about criminal activity that can be retained be more narrowly tailored so that only evidence for important investigations of federal crimes or crimes involving the threat of death or serious bodily injury can be retained, and not all "crimes."
- Support reforms that ensure that the FISA court, in addition to DOJ and ODNI, be informed about any departures from them that take place, under the authority provided in Section V of the targeting procedures, on a temporary basis to protect against a national security threat.
- Support reforms that further narrow targeting requirements by limiting surveillance to communications to which a target is a party, rather than merely "about" the target.

Under both programs:

- The Review Group should recommend the creation of an institutional adversarial advocate for the FISA court so that interests of those other than the government are represented when considering interpretations and applications of the law.
- Make recommendations for how to ensure affected individuals and third parties (like ICT companies) have a reasonable form of recourse or ability to challenge unlawful requests.
- Support reforms that ensure there is clarity in the law regarding the kind of information that the government can obtain and any predicate for the use and dissemination of that information from US persons and non-US persons alike so that individuals have notice and can foresee how the law will be applied.
- Support reforms that would recognize privacy interests as implicated as soon as information is collected, not merely when queried or otherwise processed.
- Support legislative changes that would restore the requirement that foreign intelligence be the primary purpose not merely the significant purpose of any programmatic surveillance.
- Support reforms that would ensure that criminal defendants are provided notice of when evidence obtained using either 215 or 702 authority will be used in their case and ensure they have access to how the evidence was derived under these authorities so they can meaningfully challenge the validity and constitutionality of its collection.

Regarding transparency and oversight, we ask the Review Group to consider and incorporate the following in its recommendations to the administration:

- Create a declassification process for significant legal opinions of the FISA court and Foreign Intelligence Surveillance Court of Review, or other significant legal interpretations that apply to use of Section 215 and Section 702 authorities. Publication, with appropriate and conservative redaction where shown by evidence to be genuinely necessary, should be required unless substantial and particular justification is put forward. For prior cases, if

declassifying full opinions is not possible because of legitimate national security concerns, then declassified summaries and redacted versions of the opinion should be made available. Such declassification is necessary for assessing the lawfulness and proportionality of current programs, and to improve public oversight and enable a more informed public debate.

- The US government should lead by example and issue an annual public report on how it is using its various intelligence gathering authorities. Such a report could augment existing statutory reporting on use of wiretap authorities. Reporting should cover:
    - The number of government requests for information made under specific legal authorities such as Section 215 of the Patriot Act, Section 702 of the FISA Amendments Act, National Security Letter statutes, and others;
    - The number of individuals, accounts or devices for which information was requested under each authority; and
    - The number of requests under each authority that sought communications content, basic subscriber information, or other information.

- As proposed by some legislative initiatives, require that, in addition to having to share certain orders and interpretations with some relevant congressional committees, require that the Attorney General share these with all members of Congress within 45 days of submitting them to the committees and unclassified summaries of these items with the public within 180 days.

Regarding the role of companies and access to redress, we ask the Review Group to consider and incorporate the following in its recommendations to the administration:

- The US government should allow Internet and telecommunications companies to regularly report statistics on the number of national security-related requests they have received and how they have responded. In particular, the government should remove barriers to disclosure of the following:
    - The number of government requests for information about their users made under specific legal authorities such as Section 215 of the Patriot Act, Section 702 of the FISA Amendments Act, National Security Letter statutes, and other authorities;
    - The number of individuals, accounts or devices for which information was requested under each authority; and
    - The number of requests under each authority that sought communications content, basic subscriber information, or other information.
    - The occasions on which the companies have complied or challenged such requests.

- The Review Group should recommend procedures for allowing companies to notify users when their information has been divulged under FISA, NSL statutes, or other national security authorities.
- Allow production orders or non-disclosure orders to be challenged immediately, as proposed by some legislative initiatives. For example, some legislative proposals would eliminate the current provision in the law that prevents challenge of the legality of a production or non-disclosure order under Section 215 until one year after it has been issued, and, instead, allows these orders to be challenged immediately.
- For Section 215, as proposed by some legislative initiatives, eliminate the provision in the law that provides the Attorney General, Deputy Attorney General, Assistant Attorney General or Director of the FBI with the ability to defeat a petition challenging a non-disclosure order simply by "certifying" that disclosure of the order "may" endanger the national security of the US. The FISA court should play a meaningful role in assessing whether the danger to national security posed by disclosure is supported by sufficient and specific evidence that shows it outweighs the public interest in a democracy in allowing disclosure.