Comments of Human Rights Watch

Privacy and Civil Liberties Oversight Board
August 1, 2013
Docket ID: PCLOB-2013-0005-0001

Human Rights Watch submits the following comments to the Privacy and Civil Liberties Oversight Board (PCLOB) in response to its request regarding surveillance programs operated by the United States government pursuant to Section 215 of the Patriot Act and Section 702 of Foreign Intelligence Surveillance Act.

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. Since the internet and many global communications networks know no borders, they are subjects appropriately regulated by international law along with any applicable national or constitutional laws. Recent revelations about the extent of US surveillance practices have had and will have a strong impact on rights to privacy, free expression and association in the United States and elsewhere. Although they are subject to certain restrictions, these are rights held by US citizens and non-US citizens alike, both within and outside US territory. The United States has been a strong leader in the promotion of internet freedom around the world, but its credibility has been badly undermined by recent revelations about the vast extent of its surveillance programs. The impact these programs have on fundamental human rights that the United States is bound to uphold, not just in the US but also abroad, should be of concern to the PCLOB and fall within PCLOB's mandate.

Mandate and Capacity

Part of PCLOB's mandate under its authorizing statute is to (1) "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the nation against terrorism." 42 USC §2000ee(c)(1)-(2). When providing advice on proposals to retain or enhance a particular governmental power, the PCLOB is to also consider whether: (i) the need for the power is balanced with the need to protect privacy and civil liberties; (ii) that there is adequate supervision of the use by the executive branch of the power to ensure protection of privacy and civil liberties; and (iii) that there are adequate guidelines to properly confine its use. 42 USC §2000ee(d)(1)(D).

Beginning in 1992 until the present day, the United States is 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.[1] Article 17 of the ICCPR refers specifically to the right to be free from arbitrary and unlawful interference with

[1] 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).

"correspondence," a term that is authoritatively interpreted to encompass all forms of communication, both online and offline.[2] These rights must be upheld by governments wherever they exercise their sovereign powers, and they apply to all categories of persons.[3] 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 be proportional – that is they must be narrowly tailored to achieve a legitimate aim, prescribed by law, and proportionate to the interest being protected.[4] These principles of proportionality are strikingly similar to those the board itself is tasked with applying under its authorizing statute.

The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, stated in his most recent 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 and expression.[5] Human Rights Watch urges the board to conduct a comprehensive review of current surveillance programs to evaluate their lawfulness, necessity, and proportionality. We ask the board to make recommendations on the reforms necessary to ensure the programs' consistency with both US constitutional requirements and the US's obligations under international human rights law.
How vigorously this board, 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.

Need For Board Authority

Though HRW welcomes the opportunity to comment and make suggestions for reform, it notes there are some obvious limitations in doing so. While some information about these programs are public, or have become public through disclosures, many important aspects, such as how the statutory authority is being interpreted and how supposed "minimization" and "targeting" procedures are being applied and enforced, remain classified. 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.

The board has been provided with authorization to access classified information, to take statements or public testimony from witnesses, and to request the Attorney General to subpoena certain persons, relevant reports, documents, information or other testimonial evidence. This access is incredibly important for assessing whether current programs appropriately safeguard the right to privacy. Should

[2] ICCPR, art. 17; also, 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. 24 (omitting citation), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf (accessed August 1, 2013).
[3] 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).
[4] April Report of the Special Rapporteur, *supra* note 2, para. 29.
[5] Ibid., para. 3

the board's access to information be denied or obstructed, we urge the board to raise the issue quickly and publicly so that swift, thorough and independent review can be undertaken.

The following sections of this document outline questions raised by the disclosures to date that the Board should strive to answer in its public report to the fullest extent possible.

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.[6] This interpretation has 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 by others.[7] Metadata, while not including the substantive content of communications, can be highly revealing, demonstrating patterns of behavior, associations, and beliefs, as this board is aware.

The government claims that the metadata being collected cannot be queried unless there is a reasonable suspicion that a particular telephone number is associated with a specified foreign terrorist organization.[8] 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 a court order based on probable cause that the person under investigation is an agent of a foreign power.[9] 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 Intelligence has said fewer than 300 "identifiers" were approved searching this data. However, what is actually meant by the term "identifiers," and how many individuals an identifier may implicate, is not yet clear.

---

[6] "Primary Order for Business Records Collection Under Section 215 of the USA PATRIOT Act," released by Office of the Director of National Intelligence, July 31, 2012, http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf (accessed August 1, 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).

[7] Ibid.

[8] 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).

[9] Ibid.

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."

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.[10]

In order for the PCLOB to do a comprehensive review of this program to evaluate its lawfulness, necessity and proportionality, we hope it can determine (as part of its Access to Information authority under 42 USC §2000ee(g)) and report publicly on the following:

- 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 criteria if any?
- How is an "identifier" defined and applied in relation to data searches and analysis?
- 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.[11] 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 PCLOB 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?
- Representatives from the US intelligence community claim the information being collected does not include cell phone location information. However, they have also reportedly told the press that they do have the authority to collect such information.[12] Do authorities collect cell phone location information in bulk under any existing FISA, National Security Letter statutes, or other authority?

[10] Remarks of Senator Ron Wyden (D-Ore.) titled "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).
[11] "DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents," Office of the Director of National Intelligence, July 31, 2012, http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf (accessed August 1, 2013);
[12] Remarks of Senator Ron Wyden at the Center for American Progress, July 23, 2013, *supra* note 10.

Section 702 of the FISA Amendments Act of 2008:

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 FISC 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"),[13] fail to adequately protect privacy interests of both US persons and non-US persons alike. Contrary to misleading or misinformed public statements by US officials,[14] the procedures provide weak protections for US persons and virtually 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 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.[15] 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."[16] 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.[17] 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.[18] 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.[19]

Furthermore, the entire program is based on the assumption that non US-persons have far fewer privacy rights, if any, than US persons, a position with which Human Rights Watch strongly disagrees.

---

[13] 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).

[14] James R. Clapper, "DNI Statement on Activities Authorized Under Section 702 of FISA," Office of the Director of National Intelligence, 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 James R. Clapper, "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).

[15] 50 USCA § 1801(e).

[16] "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") *The Guardian*, p. 4, http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document (accessed July 30, 2013).

[17] Ibid.

[18] 50 USCA § 1801(e).

[19] "Targeting procedures," p. 1.

While there may be a strong state interest in subjecting specific foreign communications to surveillance, the restrictions on privacy rights must be narrowly tailored and 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.[20] Furthermore it is NSA analysts who make decisions on retention and on foreign targets with apparently no review by a FISC court for compliance with targeting or minimization procedures.

In order for the PCLOB to conduct a comprehensive review of this program to evaluate its lawfulness, necessity and proportionality, we hope it can determine (as part of its Access to Information authority under 42 USC §2000ee(g)) 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.
- What safeguards are in place to protect non-US persons from unnecessary or arbitrary targeting?
- 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. What oversight does the FISC court have over how minimization and targeting procedures are implemented over the course of the authorization period?
- To what extent is fiber optic cable tapping happening 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 FISC?
- 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? If so, how often and what was the nature of the departure? Was the FISC informed about these departures if any took place?

Justifications For Collection and Secrecy Under The Programs:

The government makes 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. [21] Forty-one of the cases allegedly involved threats in other countries, including 25 in

[20] "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, *The Guardian*, http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document (accessed July 30, 2013).
[21] 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).

Europe.[22] However, only four specific cases have been mentioned publically. Of the 54, it is unclear how many of these alleged thwarted plots were due to the bulk metadata collection program versus 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.[23]

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."[24]

Given the enormous public interest in what communication information the US government is able to collect from its citizens, let alone from others around the globe, as well as in how the government retains that information and conducts searches, it is hard to understand what national security interest might be strong enough to justify the levels of secrecy around these two programs. However, we urge the board under its Access to Information authority under 42 USC §2000ee(g), 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.

Lack of Transparency and Oversight:

One of the most problematic aspects of the US surveillance programs at issue has been the lack of transparency. 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."[25] Though some level of secrecy regarding procedures and practices that relate to the gathering of foreign intelligence information and national security is justifiable, the overwhelming secrecy regarding these programs and the FISA court seems disproportionate to the impact on privacy and associated rights and inconsistent with the protection of such rights in a democratic society. The government has not clearly described what restrictions to privacy it imposes through these programs, so that individuals understand and can evaluate the limits to their rights. The fact that most US citizens as well as many members of Congress, did not understand the extent to which their own government had been collecting information about their telephone records in bulk, as revealed by the Verizon order, was the first evidence of this.

[22] Ibid.
[23] "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).
[24] 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).
[25] April Report of the Special Rapporteur, *supra* note 2, para. 83.

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.[26] Even less is known about the breadth of orders currently being used to obtain communications content from Internet companies under Section 702. Though the government has claimed checks exist through the judiciary via the FISA court and through Congress by regular reporting, these checks are hardly adequate. Only some members of Congress are apprised of various aspects of the program and even when they are, the information is provided in secret. In such circumstances, no incentives exist for reform because a legislator's constituency is left in the dark and therefore will not put pressure on their representatives for change.

As for the FISA court being a judicial check, recent disclosures have exposed numerous problems related to the court's ability to rein in the inevitable attempts by the government to maximize its authority. As the Honorable James Robertson, former judge on the FISA court told the board on July 9, 2013, the court lacks sufficient safeguards to protect the interest of those on the other side of the government's argument. "It's quite common, in fact it's the norm to read one side's brief or hear one side's argument and think, hmm, that sounds right," Robertson told the board, "until we read the other side." Judge Robertson saw the need for some form of institutional advocate that can present that other side to the FISA court. Had there been that institutional advocate, for example, the very broad interpretation of "relevance" under Section 215 may not have been approved.

In addition to the lack of transparency regarding interpretation of the law, the level of supervision by the court regarding programmatic surveillance and the lack of an institutional advocate, the court also issued orders that greatly limited the amount of information the public could have about exactly how much information the US government was obtaining. These orders leave the public in the dark as to how often such disclosures are made, the scope of information disclosed, and whether the companies have ever objected to or challenged disclosure orders.

Transparency regarding the use of surveillance powers is important for ensuring oversight, assessing whether safeguards are working, and enabling individuals to seek redress if abuses occur. We urge the board to gather information that will provide greater clarity about the justifications for the high level of secrecy surrounding the Court and public reporting about collection and surveillance practiced under these two programs.

Role of Telecommunications and Internet Companies 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.[27] HRW is a founding member of the Global Network Initiative, an organization that has established standards for corporate responsibility in the technology sector for the rights of freedom of expression and privacy.[28] Several major Internet companies named in recent disclosures about the "PRISM" program are members of the GNI and the US government has been a strong advocate for the GNI's objectives and work.

[26] Jim Sensenbrenner, "This Abuse of the Patriot Act Must End," The Guardian, June 9, 2013, http://www.guardian.co.uk/commentisfree/2013/jun/09/abuse-patriot-act-must-end, (accessed July 31, 2013).
[27] 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).
[28] Global Network Initiative, "Core Commitments," undated, http://www.globalnetworkinitiative.org/corecommitments/index.php (accessed August 1, 2013).

Under the GNI's standards, companies have a responsibility to resist arbitrary and overbroad government requests for information about their users. To meet this responsibility, 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 responded to those requests. Several US Internet companies now issue such "transparency reports."[29] This 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 board should examine and make recommendations on 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 if they believe a government order for information is too broad or poses a serious risk to human rights.

The board should also recommend procedures to allow companies to notify users when their information has been divulged under FISA, NSL statutes, or other national security authorities. As the UN Special Rapporteur Frank La Rue stated in his 2013 report to the Human Rights Council, such notification is critical in enabling individuals to challenge unlawful practices where they occur and to seek redress.[30]

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.[31] This opinion effectively shielded the United States' national security surveillance policies from judicial review and presents a major barrier for redress.

We recognize that advance or concurrent notification may not be possible while an investigation is ongoing. However, PCLOB 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 FISC that national security interests outweigh the public interest in disclosure of the request.

Recommendations:

Regarding Sections 215 and 702 we ask the board 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.

[29] 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 Enforcement Requests Report," Microsoft, https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/ (accessed July 29, 2013).
[30] April Report of the Special Rapporteur, *supra* note 2, para. 82.
[31] *Clapper v. Amnesty Int'l USA*, No. 11–1025, slip op. (U.S. Feb. 26, 2013).

- At a minimum, the board should recommend requiring the government to state "specific and articulable" facts showing that there are reasonable grounds to believe that the tangible things sought under Section 512 are not just "relevant" to an authorized investigation but also "material."
- In addition, the board should make recommendations 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 requires "presumptive relevance" if the applicant shows in the statement of facts that the items being sought pertain to certain things currently enumerated, requiring instead that they be relevant on their 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.
- If programmatic authorization continues, 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 FISC 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 FISC 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 evidence of not all "crimes" but rather only that for important investigations of federal crimes or crimes involving the threat of death or serious bodily injury be retained.
- If targeting procedures continue to be used, support reforms that ensure that the FISC 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.

Under both programs

- The board should recommend the initiation of an institutional adversarial advocate for the FISA court so that interests other than those of the government are represented when considering interpretations and applications of the law.
- 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 legislative changes that would restore requirement that foreign intelligence be the primary 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 board 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. For prior cases, if declassifying full opinions is not possible because of legitimate national security concerns, then declassified summaries 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 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 board 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 board 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 FISC should play a meaningful role in assessing whether the danger to national security posed by disclosure outweighs the public interest in a democracy in allowing disclosure.