COMMENTS OF ACCESS (AccessNow.org)
Docket ID: PCLOB-2013-0005-0001
Agency: Privacy and Civil Liberties Oversight Board

Dear members of the Privacy and Civil Liberties Oversight Board,

Access - a 501(c)(3) organization with staff based in New York City, Washington, D.C., Chile, Belgium, and Tunisia - supports the objectives of the Privacy and Civil Liberties Oversight Board (PCLOB) and welcomes the opportunity to participate in PCLOB's evaluation of PATRIOT Act Section 215 (PATRIOT 215) and FISA Amendments Act Section 702 (FAA 702).

Pursuant to 42 U.S.C.§ 2000ee,[1] PCLOB is charged with assisting the executive branch to ensure privacy and civil liberties are respected in the government's efforts to protect against terrorism. Access commends PCLOB's endeavor to closely evaluate the implications of U.S. efforts to guard against terrorism and make sure that legislation, regulations, and policies are consistent with privacy and civil liberties. In this submission, Access seeks to address the impact of the surveillance programs conducted by the U.S. government on both U.S. and non-U.S. persons.

The protections built into the laws -- the relevancy requirement in PATRIOT Act 215, the targeting and minimization procedures in PATRIOT 215 and FAA 702, and the oversight of the Foreign Intelligence Surveillance Court (FISA Court) -- have consistently and pervasively failed to adequately protect civil liberties and privacy. A thorough and public review by PCLOB will be an instrumental step in progressing the debate on U.S. surveillance practices towards reforms that ensure a greater respect for the fundamental rights to access to privacy, free speech, freedom of association, and access to information.

Current U.S. laws and practices have failed to uphold privacy and other civil liberties, and legislative reform must include limits on the scope of PATRIOT 215 and FAA 702 along with the introduction of legitimate due process and transparency standards. In summary, Access makes the following recommendations:

1. **Promote the fulfillment of U.S. obligations under international human rights**
2. **Consider the impact of U.S. national security efforts on the rights of all people**
3. **Investigate the activities of U.S. agencies that conduct surveillance**
4. **Place legal limitations on the ability to acquire and query content of U.S. and non-U.S. persons**
5. **Place legal limitations on the ability to acquire and query telephony metadata of U.S. and non-U.S. persons**

[1] 42 USC Section 2000ee *available at* http://www.pclob.gov/All%20Documents/PCLOB%20enabling%20statute_42_USC_SE_2000ee.pdf

6. **Increase transparency on how the government operates its surveillance program and how it compels the private sector to provide access to user data**
7. **Reform the composition and decision-making processes of the FISA Court**
8. **Investigate the sharing of surveillance data between the U.S. and other countries**

I. Promote the fulfillment of U.S. obligations under international human rights

The United States is bound by various international human rights instruments that prohibit the massive surveillance recent news articles and admissions from the Administration reveal it is currently conducting. The International Covenant on Civil & Political Rights, which the U.S. has ratified, along with the Universal Declaration of Human Rights, the Convention on the Rights of the Child, the Convention on the Rights of Persons with Disabilities, the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, the American Convention on Human Rights, and other regional charters all protect the right to privacy and other civil liberties implicated by surveillance.

Privacy, as a right with near universal recognition, is deserving of protection as part of the fabric of customary international law, and should be extended to the digital content of all users. In April of this year, UN Special Rapporteur on the Promotion and Protection of Freedom of Opinion and Expression Frank La Rue published a report stating:

> Traditional notions of access to written correspondence, for example, have been imported into laws permitting access to personal computers and other information and communications technologies, without consideration of the expanded uses of such devices and the implications for individuals' rights.[2]

Extraterritorial application of human rights

Not only do human rights standards apply to digital communications, but decades of interpretation by legal scholars and the U.N. Human Rights Committee, the expert body principally tasked with interpreting the ICCPR, have made clear that human rights are universal and apply extraterritorially.

Article 2, paragraph 1 of the ICCPR states each State Party "undertakes to respect and to ensure to all individuals within its territory and *subject to its jurisdiction* the rights recognized" (emphasis added). The U.S., however, has rejected the idea that individuals subject to its jurisdiction but not located in its territory are protected by international human rights law. Much pressure has been placed on the U.S. to change its position. The Human Rights Committee, for example, stated in a report in 1996 that it did not share the views of the U.S. on extraterritoriality.[3]

[2] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
[3] https://www.un.org/documents/ga/docs/50/plenary/a50-40.htm

The judicial bodies that have addressed the question of extraterritorial application of human rights, including the European Court of Human Rights and the Inter-American Commission, have found extraterritorial application when States have "effective control" of either an individual or a situation that led to the potential violation.[4] The NSA not only exercised control over non-U.S. individuals by gathering content, including their private emails, phone calls, and browsing data, but also has near complete control over the surveillance that led to the potential violation.

Privacy in international law and norms

Whether there is an actual violation of the ICCPR is a simpler question. Article 17 of the ICCPR states that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence . . . *Everyone* has the right to the protection of the law against such interference" (emphasis added). The United States' own trepidation in querying data of U.S. persons demonstrates the belief that bulk collection of internet data is a likely violation of privacy.

The Human Rights Committee's General Comment No. 31 states that under article 2, paragraph 1 of the ICCPR, the government must take "appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities." Instead, the U.S. government pressured corporations to help facilitate surveillance. The businesses themselves should be legally allowed and publicly encouraged to report on activities that potentially abuse human rights in order to implement the U.N. Guiding Principles on Business and Human Rights, which the U.S helped to foster and has endorsed.

The U.S. is not only beholden to the ICCPR, but other human rights documents that reinforce the rights to privacy, association, and due process. The U.S. is a State Party to the Organization of American States (OAS), which has adopted the American Declaration on the Rights and Duties of Man (ADRDM). The ADRDM contains protections for the rights to privacy, expression, and information. In at least one instance, the Inter-American Commission on Human Rights has found the U.S. responsible for violating rights under the ADRDM.[5] Article 4 of the Inter-American Democratic Charter, also adopted by the OAS, calls for State Parties to respect "[t]ransparency in government activities."

For clarification on human rights in the surveillance context, the International Principles on the Application of Human Rights to Communications Surveillance (Principles)[6] is a proposed framework in which States can evaluate whether current or proposed surveillance laws and practices are consistent with their human rights obligations.

[4] http://www.law.yale.edu/documents/pdf/cglc/Hathaway_HumanRightsAbroad.pdf
[5] http://www.cidh.oas.org/annualrep/2003eng/USA.11204.htm
[6] https://necessaryandproportionate.org/

For example, the Principles say that, in order to comply with human rights norms, surveillance should be proportionate — meaning that the benefit of the surveillance must be weighed against the potential harm caused to users' rights. Frank La Rue, in his latest report, similarly warned against surveillance practices which cause disproportionate harm in that they endanger free expression.[7] Everyone should feel safe using the internet to express opinions and obtain any type of information.

We urge PCLOB to exercise its considerable authority to educate the Administration, law enforcement, and intelligence agencies on the U.S.'s obligations under international law with an eye to bringing surveillance activities into line with human rights norms.

II. Consider the impact of U.S. national security efforts on the rights of all people

We respectfully urge PCLOB to consider all persons impacted by the actions of the U.S. government in its national security efforts. Subject to 42 § 2000ee(c)(2), PCLOB must ensure that liberty concerns are considered without drawing distinctions based on nationality, location, immigration status, race, political opinion, religion, or any other condition.

Read as a whole, the law that creates PCLOB entrusts it with safeguarding the rights of all persons. As such, Access has joined Best Bits, an international network of civil society organizations, in calling on PCLOB to investigate the human rights implications of FAA 702 for non-U.S. persons.[8]

Access believes the National Security Agency (NSA) has gone too far by bulk gathering content data under FAA 702 and metadata under PATRIOT 215. It is believed that the NSA gathers the metadata of nearly all U.S. telecommunications consumers, and the content of millions of those it deems to be non-U.S. persons. It is unclear just how many millions of people are affected by the NSA's surveillance programs—though this is a question which PCLOB should help answer—but recent revelations make clear that the number is disproportionately large.

The Director of National Intelligence has argued that the programs authorized under FAA Section 702 contain safeguards to protect the data of U.S. subjects,[9] and while the effectiveness of those protections is questionable, non-U.S. users have few legal protections to prevent the bulk acquisition and analysis of their internet content. While U.S. authorities point to targeting and minimization procedures[10] as evidence of programmatic restraint, those procedures contain few protections for non-U.S. persons. They mainly serve

[7] http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
[8] http://bestbits.net/pclob/
[9] http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa
[10] http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document

to ensure 51% confidence that a target is not from the U.S.

The targeting procedures, signed by FISA Court judges, contain a number of factors that are used to develop confidence the target will communicate foreign intelligence, but the standards are underwhelming as one of the few protections for non-U.S. internet users. Those factors, for example, include whether a telephone number is suspected of use for direct communications with someone who is suspected of association with a foreign authority. Another factor is whether the target is on the "buddy list" of a user suspected of association with a non-U.S. target.

While the targeting procedures list a number of factors, they do not make clear what level of confidence is needed by an individual NSA analyst to justify the querying of user data. The standards are vague and potentially harmful. They seemingly grant authority to analyze the data of users who are not actually suspected of terrorism or holding foreign intelligence and might only have a tangential, or non-existent, relationship to anyone who is suspected.

We therefore urge PCLOB to investigate the total amount of information acquired and queried under FAA 702 and the number and percentage of times that the targeting procedures have been disregarded for emergencies. Even with the targeting procedures in place, FAA 702 grants the NSA the authority to intrude into fundamental human rights of all internet users and must be curtailed.

III. Investigate the activities of U.S. agencies that conduct surveillance

While we would also like to see the formation of a special Congressional committee to investigate, report, and reveal to the public the extent of domestic spying—along the lines of the historical Church Committee—we do see an important need for PCLOB to also exercise its broad statutory powers to investigate abuses.

Pursuant to 42 § USC 2000ee(g)(1), PCLOB is authorized to access classified records and interview personnel from executive branch agencies. That power, along with the power to request the Attorney General to subpoena persons, should be used to fully investigate surveillance practices by the NSA, the FBI, the Office of the Director of National Intelligence, the Department of Justice, and other relevant agencies and departments. Access believes PCLOB should fully utilize its statutory power in investigating PATRIOT Act 215 and FAA 702 along with other surveillance authorities in particular.

While information has been revealed on the use of PATRIOT Act 215 and FAA 702, there are other programs with less public information available. Those programs also deserve oversight and transparency and we urge PCLOB to investigate those programs—to get at the "unknown unknowns."

For example, the NSA used Section 214 of the PATRIOT Act, the provision on pen register and trap and

trace devices, to authorize a program which collected internet metadata from 2007 to 2011. That program operated with similarities to the telephony metadata collection under PATRIOT Act 215; the NSA practiced bulk acquisition and queried the database using certain qualifiers. PCLOB should investigate, along with PATRIOT Act 215, whether PATRIOT Act 214 still authorizes surveillance and whether it could be used to do so in the future.

The legality of other programs also remains unclear. The United States is reportedly operating programs that are catching data passing "upstream" on fiber optic cables, including those underseas as well as those across continents, and through internet infrastructure like IXPs. Identified by the codenames FAIRVIEW, STORMBREW, BLARNEY, and OAKSTAR, these government surveillance programs are also likely to affect non-U.S. internet users. Users should know what type of information is gathered through the tapping of these undersea cables, as well as the laws that authorize such practices. With laws that are accessible and clear, and specific limits set to these operations, the impact to non-U.S. users will be more foreseeable and clear.

The U.S. government has also compelled action from private companies that control those fiber optic cables in order to retain the ability to gather data from those cables. Over concern that non-U.S. companies were taking ownership of the companies that control the cables, the U.S. has ensured they have secure access to the cables operated by private companies.[11] In at least one instance, the Federal Communications Commission held up approval of cable licenses until a company built infrastructure that went above and beyond what is required in law, by ensuring government officials could access their facilities with half an hour's notice. According to Susan Crawford, a law professor and one-time science and technology advisor to the Obama administration, the communications companies do not have the independence to fight government requests. PCLOB should investigate to ensure that the government does not exert undue pressure or illegally interfere with the rights of users and with corporate entities to access their networks for access to users' data.

While the extent of the NSA's surveillance remains unknown, it is clear that there is much more depth to the NSA's activities than has so far been revealed. The U.S. government's intrusion into private communications data goes beyond PATRIOT Act 215 and FAA 702; PCLOB should also investigate and report on potentially abusive programs outside of these statutory authorities.

IV. Place limitations on the ability to acquire and query content of U.S persons and non-U.S. persons

As the Principles on the Application of International Human Rights to Communications Surveillance make

---

11

http://articles.washingtonpost.com/2013-07-06/business/40406049_1_u-s-access-global-crossing-surveillance-requests

clear, the traditional distinction between content and metadata is no longer appropriate. With the depth of surveillance, the acquisition of metadata can reveal the personal relationships, political leanings, or daily routine of a person. The extent of metadata acquisition, therefore, can be as revealing as the content itself.

In fact, distinguishing information by type is an antiquated way of determining whether it deserves protection. According to the Principles on the Application of Human Rights to Communication Surveillance, "all information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public, should be considered to be 'protected information,' and should accordingly be given the highest protection in law." We urge PCLOB to advocate for a change in the collection of metadata, under PATRIOT 215 and any other authorities which are or could be used for the bulk acquisition of metadata. PCLOB should encourage the reform of the Foreign Intelligence Surveillance Act to narrow the focus of acquisition and collection of data from non-U.S. targets.

The government has historically used questionable legal reasoning in the interpretation of FAA 702. That section, which authorized PRISM and upstream data collection, allowing the sweeping collection of communications, potentially violates the human rights of nearly all internet users, whose data can be accessed under the discretion of an individual NSA analyst.

A training manual advised new NSA analysts that the accidental collection of content of U.S. persons is "nothing to worry about."[12] As civil liberties advocates, we are indeed worried that users' content is being acquired and queried without adequate protection. A recently released 2012 report showed 2,776 instances where the NSA violated rules or court orders over the course of a year, some of those willful, but the number of people affected by those errors is unclear.[13] One of those instances involved the unlawful collection of data from 3,000 U.S. persons. Typos and insufficient specificity have also led to the improper querying of personal data. According to the *Wall Street Journal*, the NSA has the potential to collect data from 75 percent of U.S. internet traffic, which includes data from both U.S. and non-U.S. persons.[14] PCLOB should investigate the exact number of individuals whose data is gathered despite no connection to international terrorism.

The Deputy Director of the NSA John C. Inglis revealed that the intelligence agency can perform a three-hop contact chaining analysis of communications metadata. That means the NSA can query the data of a person three steps away from the subject of an investigation in the communication chain. In other words, a terrorism suspect's former landlord's cousin's old dog walker from ten years ago may have their

---

12 http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html, page 3

13 http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/

14 http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html

data analyzed by the NSA. Moreover, according to recent reports, the U.S. has over one million individuals on their terrorist watch list.[15] If each individual on the terrorist watch list has twenty contacts and each of their contacts has 20 contacts (a highly conservative estimate), then the NSA is querying the content of billions of users. That number is huge, the search is disproportionate, and the government's access is hardly restricted by its territorial or investigatory reach.

Government officials have attempted to alleviate concerns over internet content collection by arguing that the NSA does not target U.S. persons. NSA guidelines, the Obama administration insists, require that analysts obtain a 51 percent confidence that targets are non-U.S. citizens before they query data. They do this through a "totality of the circumstances " test by examining the lead information received on the target, information already held by the NSA, and a technical analysis of the target facility. Examples of lead information factored into the test include information provided by other sources like the target's location or the destination of the target's communication. This subjective standard fails to provide adequate protection as the test is vague and grants discretion to the individual NSA analyst, who might use their own notions of "foreignness."

Targeting data of non-U.S. internet users will likely result in a number of negative externalities. More significantly, intruding into private information, as noted below, is a violation of international human rights law that binds the United States. The U.S. government should also be concerned over potential economic ramifications of widespread surveillance. Internet users are likely to develop distrust towards U.S. companies, including Facebook and Google, decreasing corporate growth.[16] Surveillance can similarly lead to political distrust of the U.S. government.

Stricter standards should be implemented to ensure targets of surveillance are actually suspects of international terrorism, espionage, or other similar transnational crimes for which surveillance is explicitly authorized. It is imperative that targeting and minimization guidelines should also be updated to improve protection for non-U.S. internet users.

V. Place legal limitations on the ability to acquire and query metadata of U.S. and non-U.S. persons

While the government claims authority for the bulk acquisition of metadata under PATRIOT Act 215, the plain language of the law does not appear to grant such authority. The law states that in order to receive authorization from the FISA Court, the government must provide "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are *relevant to an authorized investigation* . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities" [emphasis added].

[15] http://www.aclu.org/technology-and-liberty/terror-watch-list-counter-million-plus
[16] http://www.forbes.com/sites/kashmirhill/2013/09/10/how-the-nsa-revelations-are-hurting-businesses/

In theory, that relevancy requirement would mean that the government should not be gathering private records unrelated to an investigation into terrorism or clandestine intelligence activities. The Department of Justice has incorrectly argued that the relevancy requirement applies only once the NSA actually queries the data.[17] In other words, they interpret the law to allow the bulk gathering of metadata but require an actual reasonable suspicion when analysts want to review the metadata. Further, the Department of Justice argues for the need to gather all metadata in order to query the dataset in those circumstances when they actually develop a reasonable suspicion.

This standard is problematic because it expands the definition of "reasonable" and "relevance" to encompass any potentially related information. That standard is not only dangerous in the context of PATRIOT Act 215, where it has already been used to justify bulk acquisition, but in other surveillance contexts where the government might argue the need to collect data in bulk due to its potential use for a terrorism investigation. The government's legal interpretation of "reasonable" and "relevance" has failed to provide the protection originally intended in the word.

Further, the statement of facts required by PATRIOT Act 215 is intended to show relevance to an "authorized investigation," which, according to the *Attorney General's Guidelines for Domestic FBI Operations,*[18] requires a factual predicate. That means there need to be facts or circumstances indicating a crime, but surely there is no reason to believe every telecommunications customer in the United States has committed such a crime. The government has stretched the use of PATRIOT 215 to achieve bulk acquisition of metadata, in a way the law does not permit.

VI. Increase transparency on how the government operates its surveillance program and how it compels the private sector to provide access to user data

PCLOB should support, and possibly oversee, the creation of government surveillance transparency reports. Recently, a letter[19] was submitted to the President and Congress drafted by a coalition of companies and civil society groups, including Access, asking the Obama Administration and Congress to consider a number of reforms aimed at introducing transparency into the government's surveillance practices. We believe those requests are reasonable and would be a significant first step towards informing internet users of the risk they face when placing their private information online.

(a) Greater detail in companies' transparency reports

The above-mentioned letter also asked that companies be granted far greater freedoms for

[17] http://sensenbrenner.house.gov/uploadedfiles/ag_holder_response_to_congressman_sensenbrenner_on_fisa.pdf
[18] http://www.justice.gov/ag/readingroom/guidelines.pdf
[19] https://www.documentcloud.org/documents/728793-transparency-letter-from-tech-companies-to-nsa.html

communications providers than currently exist: the ability to publish information on specific numbers of requests, the specific authorities making those requests, and the specific statutes under which those requests are made. Furthermore, the report calls for the ability to differentiate requests based on content versus metadata, and enumerate the number of persons, accounts, or devices affected. We reiterate our support for permitting greater detail in private companies' transparency reports.

(b) Government's transparency report

The release of transparency reports by the government could help provide a more complete portrait of surveillance, as many companies do not yet release their own transparency reports—and when they do, the information they release may be limited and not disaggregated enough to be meaningful.

The administration has claimed that revealing more information on the details of its surveillance programs would interfere with investigations, but years' worth of systemic transparency on investigatory authority in criminal investigations has had no apparent detrimental effect. Similarly, existing transparency reports published by companies offer no specific identifying information, ensuring ongoing investigations are not compromised while providing general clarity on the frequency of the practice.

In the U.K, the Interception of Communications Commissioner presents an annual report to Parliament.[20] The report presents details on information requests by type of request and by requesting authority, for example, and it breaks down requests by local authorities and police forces. However, the reports are lacking detail on communications surveillance by intelligence agencies. We believe that the U.S can too issue a transparency report and in fact include more detail than currently provided in the U.K. report.

While the recent announcement that the Office of the Director of National Intelligence will publish a transparency report of FISA orders based on probable cause (Titles I and III of FISA, and sections 703 and 704); Section 702 of FISA; FISA Business Records (Title V of FISA); FISA Pen Register/Trap and Trace (Title IV of FISA); National Security Letters issued pursuant to 12 U.S.C. § 3414(a)(5), 15 U.S.C. §§ 1681u(a) and (b), 15 U.S.C. § 1681v, and 18 U.S.C. § 2709; is a positive first step, as we have argued elsewhere, it is insufficient.[21]

For example, the DNI's report will only include the number of requests and targets, which will make the scope of the nation's surveillance machine to appear far more limited than it actually is. To put this in context, in 2012, there were 212 requests for business records justified under Section 215 of the Patriot

---

20 http://www.iocco-uk.info/docs/2012%20Annual%20Report%20of%20the%20Interception%20of%20Communications%20Commissioner%20WEB.pdf

21 https://www.accessnow.org/blog/2013/08/30/obama-administration-continues-to-thwart-meaningful-transparency-on-nsa-sur

Act, but that number also includes requests for the "ongoing, daily" disclosure of communications metadata of the millions of customers of AT&T, Verizon, and Sprint. And how do we know that? Because public disclosure of aggregate numbers of requests pursuant to most of the statutes to be included in the DNI's report is already required.[22]

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

Public disclosure by both the government and the communications providers who hold user data is crucial in keeping both accountable. The new information the Administration plans to release provides no basis for the government's continuing efforts to gag companies like Google and Microsoft from doing their own transparency reporting.

VI. Reform the composition and decision-making processes of the FISA Court

(a) Declassification and release of FISA Court opinions

In 2010, the Department of Justice and the Director of National Intelligence instituted a process for the declassification of FISA Court rulings, but after two years, few declassifications have been made.[23] As many of the requests lack specificity, there is surely a portion of opinions which can be released without endangering national security investigations. Releasing those opinions that do not endanger national security would provide further transparency in the operation of the programs and give an opportunity for challenges to current secret opinions.

(b) Independent advocate versed in human rights

We support the introduction of an independent legal advocate to introduce elements of an adversarial process, thereby safeguarding due process in FISA Court proceedings. Scholars have introduced a number of suggestions of what form the independent advocate could take. Professor Orin Kerr from George Washington University suggested a government lawyer could have a mandate to challenge motions filed in the FISA Court. Another suggestion, by Professor Stephen Vladeck of American University, would introduce "special advocates," private lawyers with security-clearances, who would have a right to

[22] http://epic.org/privacy/wiretap/stats/fisa_stats.html
[23] http://www.govtrack.us/congress/bills/113/s1130/text

challenge FISA Court orders.[24]

The adversarial process is a tenet of common law legal systems which prevents the abuse of one-sided or inquisitorial approaches. No exception should be made for cases, such as those of the FISA Court, that implicate fundamental rights. Access believes PCLOB should consider these suggestions, and investigate and support the use of an independent advocate in the FISA Court.

(c) Presidential appointment of FISA judges

Under 50 USC Section 1803,[25] the Chief Justice of the Supreme Court appoints all FISA Court judges without Congressional confirmation. Granting this authority to a lone justice means there is little potential for diverse viewpoints on a critically important court. A report by *The New York Times* shows that Chief Justice Roberts is failing to select judges with diverse ideologies, instead appointing almost exclusively judges with executive branch backgrounds.[26] We ask that PCLOB review alternative methods for appointing FISA Court judges, potentially through Presidential appointment, as judges are appointed under Article III of the Constitution, or granting each circuit court chief judge the authority to appoint one FISA Court judge.

VI. Investigate the sharing of surveillance data between the U.S. and other countries

PCLOB should also investigate the extent of informal sharing of information obtained from FAA 702, PATRIOT 215, and any other surveillance authorities. As noted above, informal information sharing can be used to avoid domestic privacy protections. MLATs should be used to ensure information is shared with transparency and in accord with international human rights law. PCLOB can play a role in ensuring MLATs are properly utilized as the method of sharing and receiving information related to investigations.

Reports have indicated that there is widespread, informal intelligence sharing between the U.S. and other 'Five Eyes' nations—Canada, UK, Australia, and New Zealand, among other countries. With the existence of Mutual Legal Assistance Treaties (MLATs), which provide clear legal channels for the sharing of criminal investigation data between countries, ensuring respect for due process, there is no need to use informal information sharing. Such practices can allow countries to skirt their own privacy laws by using the intelligence gathering capabilities of allies to obtain data otherwise protected by domestic privacy laws.

---

[24] http://www.lawfareblog.com/2013/07/making-fisc-more-adversarial-a-brief-response-to-orin-kerr/

[25] http://www.law.cornell.edu/uscode/text/50/1803

[26] http://www.nytimes.com/2013/07/26/us/politics/robertss-picks-reshaping-secret-surveillance-court.html?pagewanted=all&_r=0

The International Principles on the Application of Human Rights to Communications Surveillance state one of the fundamental reasons why MLATs are so important: "MLATs should ensure that, where the laws of more than one state could apply to communications surveillance, the available standard with the higher level of protection for individuals is applied." While not every MLAT currently achieves this standard, PCLOB can play a role in ensuring that MLATs and other means of intelligence sharing are not used to bypass domestic privacy standards.

The U.S. has an extensive network of MLATs which can be used to send and receive such data. We also urge PCLOB to investigate the extent of informal intelligence sharing and to push for responsible reforms. Access believes that an open and honest evaluation process, with the guidance of PCLOB, FAA 702 and PATRIOT 215 can be reformed in accordance with human rights standards.

Conclusion

The Privacy and Civil Liberties Oversight Board is tasked with an enormous duty in investigating PATRIOT Section 215 and FAA Section 702. The investigation into PATRIOT 215 and FAA 702 is an opportunity for PCLOB to establish itself as a protector of the human rights of U.S. and non-U.S. persons around the world. We urge PCLOB to use its full resources and power to ensure a full investigation into surveillance programs. Access, along with many of the digital rights focused civil society organizations, stands ready to assist PCLOB with the important task of investigating U.S. surveillance programs.