Comments of the Electronic Frontier Foundation to the Review Group on Intelligence and Communications Technologies

Introduction

As many members of the Review Group on Intelligence and Communications Technologies ("Review Group") are aware, the Electronic Frontier Foundation ("EFF") is a membership-supported organization based in San Francisco, California. We fight for privacy and civil liberties primarily in the courts, bringing lawsuits and defending technology users. The EFF is at the forefront of litigation challenging the legality and constitutionality of the NSA's surveillance programs, which include the programs using Section 215 of the Patriot Act and Section 702 of the Foreign Intelligence Surveillance Act Amendments Act (FISA AA).[1] Blending the expertise of our lawyers, policy analysts, technologists, and activists, we educate policy-makers, the press, and concerned citizens.

On September 4, 2013 the Review Group issued a press release asking for public comment on issues the President has directed it to examine.[2] The presidential memorandum establishing the group did not mention the word privacy or civil liberties once.[3] Despite this, the group is requesting comments on how the United States can "employ [its] technical collection capabilities…while respecting our commitment to privacy and civil liberties." It is an encouraging sign that the Review Group acknowledges the privacy concerns regarding the government's technical collection capacities.

The Review Group can provide a new foundation for our modern technological surveillance capacities. We believe that a well-crafted policy will archive the important objectives of protecting national security while upholding the United States' strong commitment to respecting privacy and civil liberties. Moreover, the Review Group can foster the confidence of the public through an environment of sufficient transparency and promote America's foreign policy by respecting the interests of people around the world.

---

[1] See generally, Electronic Frontier Foundation, *NSA Spying on Americans*, https://www.eff.org/nsa-spying.

[2] Office of the Director of National Intelligence 2013. *Review Group on Intelligence and Communications Technologies Conducts Meetings with Privacy and Civil Liberties Experts and Information Technology Industry Experts*. September 9, 2013. Online at http://www.whitehouse.gov/the-press-office/2013/08/12/presidential-memorandum-reviewing-our-global-signals-intelligence-collec [Accessed: 3 Oct 2013].

[3] The White House Office of the Press Secretary 2013. *Presidential Memorandum: Reviewing Our Global Signals Intelligence Collection and Communications Technologies*. August 12, 2013. Online at http://www.whitehouse.gov/the-press-office/2013/08/12/presidential-memorandum-reviewing-our-global-signals-intelligence-collec [Accessed: 3 Oct 2013].

From the beginnings, signals intelligence has focused on collecting as much information as possible. Advancing technologies are expanding this capacity beyond any imagined in the last century by allowing for massive collection of any, and all, data that passes along the fibers of the Internet. At the same time, every aspect of modern life involves a data trail that persists on these networks.

To address the dangers enabled by this vast increase in technical capacity, it is critical to **stop the spying**. Dragnet or bulk collection of information must be replaced with particularized, and targeted acquisition.[4] The intelligence community must begin to think about questions like whether or not mass data collection is viable, if it's absolutely necessary, and what type of data is the most effective to acquire. With a frank and honest evaluation of these questions, the conclusion is inescapable—the mass spying program should be stopped.

Accordingly, the Review Group must take into consideration the following objectives during its review.

Objectives

The Review Group must first review the confluence of the technical collection capacities and advancing collection technologies with the Constitution, statutory authorities, and, more simply, users' privacy concerns. A full legal analysis is not expected in the Group's report; however, the Group should focus on the everyday practical concerns about the collection of innocent users' metadata, phone calls, and emails; and the collection of huge datasets that may provide voluminous amounts of intimate information.

"Metadata" is a vital aspect in answering the above questions. In today's modern age, metadata and other non-content information gleaned from modern telecommunications can reveal intimate details about one's life. It is imperative, in light of advancing technological collection capacities, that the Review Group analyze how the act of collecting innocent users' metadata impacts the public trust and public discourse around the NSA's surveillance capacities.

After a reporting on how these data mining techniques implicate users' privacy the Review Group should focus on:

1) Advancing transparency issues, and offering solutions to the broken classification system;
2) Obtaining an independent technologist to advise and provide assistance to the group; and,
3) Addressing the recent revelations around NSA's cryptographic strategy.

---

[4] By collection and acquisition we mean to encompass any placement of data on any system owned or operated by the intelligence community. As the Review Group doubtless knows, the intelligence community often uses unusual definitions of terms that can be misleading. See generally https://www.eff.org/nsa-spying/wordgames

A Review of the Programs In Light of Advancing Technologies and the Law

The Review Group should review the diverse collections of innocent users' data by the United States—including both undisclosed and disclosed programs—and explain to the public, if possible, on how the type, scope, and scale of that collection is sound intelligence policy despite collecting massive data sets on millions of innocent users.

Fundamental to this review is how intimate personal information can be uncovered by mining the collection of metadata and other information about users. A report must include the practical policy considerations of what type of data to collect, if any privacy issues are triggered by such a collection, if such collection is within the mission of the intelligence community agency, and the effectiveness of such huge data sets of information. As we've witnessed from the public discourse around these programs, such collection betrays the public trust in the intelligence community—a trust that is vital to its success.

The Review Group must incorporate the practical consequences of such mass data collection because the Executive Branch has placed an enormous reliance on an outdated Supreme Court case, *Smith v. Maryland,* and antiquated notions of what date users deem private.[5] Extending *Smith v. Maryland* to modern metadata is wrong. When comparing the records at issue in *Smith*—a list of phone numbers a person dialed—with the NSA's vast collection, it's clear *Smith* is not analogous.

First, the phone numbers at issue in *Smith* revealed far less information than the metadata collection as it exists. Second, *Smith* was predicated on the understanding that a phone customer understood they were conveying the numbers they dialed to the phone company, who even provided the customer with a list of the numbers in their monthly bill. Modern users rarely have a per call charge, and generally do not receive a detailed account of what types of metadata is being collected by the providers and whether that collection is for a provider's business purpose or for the government's surveillance collection.

---

[5] Smith v. Maryland 442 U.S. 735 (1979). *Smith v. Maryland* has been repeatedly criticized by legal scholars. See, e.g., Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal L. Rev. 1083, 1137-1138 (2002); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 Mercer L. Rev 507, 524-528 (2005); Anita Ramasastry, *Lost In Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 Santa Clara Computer & High Tech L.J. 757, 764-766 (2006); Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949, 982-989 (1996) (discussing the limited capacity of the pen/trap devices analyzed in Smith and explaining how modern pen/trap devices collect far more information).

Since *Smith*, the Supreme Court has repeatedly explained that merely exposing something to someone else is not enough to categorically defeat an expectation of privacy.[6] In its seminal 2012 opinion in *United States v. Jones*, a majority of the Supreme Court justices opined that an individual retained an expectation of privacy in their public movements even though those movements are at times exposed to the public.[7] Speaking directly to the issue here, Justice Sotomayor wrote in a concurring opinion that *Smith's* rationale "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."

It is time to put an end to the idea that *Smith* removes all constitutional protections for metadata, and understand, as the majority of the Supreme Court justices suggested in *Jones*, that privacy expectations can, and do, exist even in information turned over to third parties.

Stepping outside of the domestic perspective, this undifferentiated collection of all possible data creates new challenges when it comes to mass data collection's impact on foreign policy—especially when performed outside US borders, or upon untargeted non-US persons. United States law and practice has traditionally created a strong dividing line between spying on US persons, and other global intelligence collection. The strategy of the NSA to collect mass data within the United States, and on every possible outside source, has had several damaging effects on foreign policy.

First, American Internet companies frequently store the private data of billions of foreign users on American soil, including years of confidential email, online conversations, search terms, and metadata. To assert that none of this information has any statutory or constitutional protection, and to keep secret the use to which it is put, damages the reputation of these companies and the United States as a whole.

Second, even outside the United States, in the realm of expected NSA global signals intelligence practice, mass collection means that whole nations' private communications are being vacuumed up into a database, rather than the targeted pursuit of agents of foreign powers. To set the precedent that this is acceptable practice will not only leave the US intelligence services open to the accusation of political and economic espionage, but will also create an online world where American citizens' data is freely collected, used and abused by other country's intelligence agencies, with no coherent diplomatic or political response by the United States.

---

[6] In 2000, the Supreme Court ruled in *Bond v. United States* 564 US 334 (2000) that a passenger still maintained an expectation of privacy in his luggage even though other passengers and personnel may handle it. In 2001, it ruled in *Ferguson v. City of Charleston* 532 US 67 (2001) that a medical patient retained a right of privacy in a urine sample given to medical professionals.

[7] United States v. Jones 565 *US* ___, 132 S.Ct. 945 (2012)

Third, the United States' massive surveillance programs have given comfort to non-democratic regimes throughout the world that would use the programs to justify spying on their opposition and political enemies. The State Department and USAID have awarded millions of dollars to groups working to advance Internet freedom around the world, including supporting counter-censorship and secure communications technology. The NSA's surveillance programs and efforts to weaken secure communications technologies undermine this message.

Furthermore, to advance its foreign policy, the United States needs to meet its international human rights obligations in relation to communications surveillance. To do so, the United States should comply with the set of International Principles on the Application of Human Rights to Communications Surveillance.[8] These Principles, signed by over 274 human rights, media, and digital rights groups from across the world, explain how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques. These 13 Principles apply to surveillance conducted within a state or extraterritorially. The 13 Principles also apply regardless of the purpose for the surveillance—law enforcement, national security or any other regulatory purpose. Any measure of communications surveillance should not be applied in a manner that discriminates on the basis of, inter alia, nationality or other status.

The 13 Principles in particular, and international human rights law generally, are premised on the assumption that interference with fundamental rights must be dealt with on a case-by-case basis. This means that any decision about surveillance must weigh the benefits to be gained from acquiring the information against potentially violating an individual's privacy or other rights like freedom of expression and association. This obligation will generally require convincing an independent and impartial competent judicial authority that the privacy invasion in question will lead to information necessary to resolving or preventing a serious offence. Current, US mass surveillance practices ignores any consideration of proportionality in favor of the unchecked interference of the right to privacy, and hence it's incompatible with the United States' international human rights obligations.

From the position of strengthening the rule of law, the United States should bolster its own economic pre-eminence online, and pressure others to comply with the same principles.

Beyond the issue of mass metadata collection and its privacy implications in relation to sound intelligence policy, the Review Group must keep in mind how Section 215 of the Patriot Act violates the First and Fourth Amendments of the Constitution. For instance, the First Amendment right of association is a well established doctrine that prevents the government "interfering with the right to peaceably assemble or

[8] See http://necessaryandproportionate.net. [Accessed: 3 Oct 2013].

prohibit the petition for a governmental redress of grievances."[9] The right stems from the simple fact that the First Amendment protects the freedom to associate and express political views as a group. When the government gets access to the phone records of political and activist organizations and their members, it knows who is talking to whom, when, and for how long. A first step towards regaining the public trust is to address the guidance provided by the Constitution and case law relating to modern technologies in light of the NSA's collection of massive data sets.

Even though the Review Group does not consist of a cadre of lawyers, it is imperative the Review Group apply its eclectic skill-set to review the above aspects of data collection. This includes how the intelligence community's inability to acknowledge core privacy concerns affects the public trust and whether the mass collection of innocent American's telephony metadata correctly weigh the invasiveness of such a search with the supposed goal of national security. By answering these questions, the Review Group can provide a new foundation for the collection of data in light of advancing modern technologies and core privacy concerns.

Government Transparency and the Classification System

After reviewing the privacy implications, the Review Group must examine issues around transparency, the lack of which is corrosive to democracy and the rule of law. At the core of any discussion on these programs is the unsustainable classification system. Congress, litigants, and the general public cannot have a full dialogue on these issues when overclassification is rampant. The recently disclosed information about the NSA programs strongly indicates that information is classified primarily to ensure that the public is unaware of the scope of domestic surveillance.

First, the committee must conduct itself in the most transparent way possible. This includes following the procedures in the Federal Advisory Committee Act (FACA). Currently the Review Group is not following the requirements of FACA, which would provide added transparency of, and public trust in, the Review Group. The committee must also hold public testimony and publish public reports—including its final report and recommendations to the Director of National Intelligence and to the President. This Review Group should follow up on the recent declassification of documents by recommending the declassification of documents it receives, or provide a listing of documents it has reviewed so that the public can be fully informed.

The broken classification system also extends to the oversight model established by Congress—the establishment of the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI). A key process of oversight is the communication between the intelligence community and the intelligence committees. The dispersal of information to users' Congressional

[9] *NAACP v. Alabama*, 357 U.S. 449, 460 (1958).

representatives is vital to maintaining the public trust. Yet a constant pattern is the inability for the intelligence committees—and other members of Congress—to receive adequate information from the President and the intelligence community. In 2007, the Chair of SCCI, Senator Jay Rockefeller, noted how the Executive, "responds to legislative oversight requests with indifference, if at all, and with usually outright disdain" and how:

> For 5 years after 9/11, the administration refused to brief the full membership of the oversight committees on the existence of NSA's warrantless surveillance program and the CIA's secret prison system and interrogation techniques, the two programs the administration publicly touts as indispensable tools in the war against terrorism.

The extent of Congressional oversight should not be limited by the personality of the President or the intelligence community's leaders.

The Review Group should recommend changes to the oversight regime to allow for all members of Congress to be fully informed of the intelligence community. Currently, trust is placed in the Committee chairs to disperse information. But as recently as last year, we've seen news reports note that members were not fully informed of the nuances of the programs.[10] The intelligence community should be offering more briefings, and more information to members who request briefings and who do not serve on the intelligence committees. And the Review Group should conduct a review of the current policies and practices of disseminating information to Congressional committees other than the intelligence committees.

Far too often, the government has used classification as a method to hide wrongdoing, and stop legitimate legal challenges to the spying. Public trust and public discourse demands court hearings that can draw from a publicly accessible—and accountable—record.

The public's access to these documents is vital because time after time we have seen a lack of technical knowledge on the part of the overseers of these programs. For instance, the NSA has admitted that their systems' own complexity led to the inability for a "complete understanding among the key personnel" of the programs.[11] In addition, it took the FISA Court a number of years to even understand the technical processes of the collection of telephony metadata.[12] With

---

[10] Ackerman, S. 2013. *Intelligence committee withheld key file before critical NSA vote, Amash claims*. Available at: http://www.theguardian.com/world/2013/aug/12/-intelligence-committee-nsa-vote-justin-amash [Accessed: 3 Oct 2013].

[11] See generally, In Re Production of Tangible Things From [REDACTED], No BR 08-13 (March 2, 2009), available at http://www.dni.gov/files/documents/section/-pub_March%202%202009%20Order%20from%20FISC.pdf

[12] See generally, In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [REDACTED], No. BR 09-13 (September 3, 2009), available at https://eff.org/r.c8cj

publicly accessible documents, learned technologists, computer scientists, and others can thoroughly vet any decisions or conclusions the Review Group conducts. Such oversight is an added reassurance in a representative democracy that is contingent upon properly informing members of the public and Congress.

In short, the Review Group must review and report on ways the technical collection capacities of the United States can be effectively publicly reviewed and discussed without an overriding risk to national security or exposing "sources and methods." It must release documents it receives, hold public meetings, and offer recommendations about how to increase the release of information about these programs. It is paramount that users understand the NSA's collection capacities and authorities in order to engage in robust public discourse.

Lack of an Independent Technologist on the Panel

As noted above, a recurring challenge with effective oversight of the NSA spying is that major actors in the program lack sufficient technical knowledge to fully understand what NSA is doing or the implications of NSA activities. This extends from political officials to Congress to the FISA Court judges. No person or entity can successfully oversee programs without understanding the technical details of how that spying takes place and what its implications are. The panel should have an individual intimately familiar with computer technologies at both the level of "code" and in the broader network environment. That person needs to have a clearance at least as high as the members of the review committee.

A technologist is necessary to serve as an issue-spotter, to explain things to the review committee, and to help answer questions like:

a. How the NSA can conduct its surveillance with minimal harms to privacy and civil liberties?
b. What minimum information the NSA needs to conduct its goals?
c. How can the NSA avoid collecting innocent users' information?
d. How can the NSA better audit the actions of technical personnel?

Having an aide in uncovering how effective the programs are and to what extent privacy can be protected using technical systems. It is reported that the Internet metadata program was stopped in 2011 partly due to its ineffectiveness.[13]

The Review Group must look into and release the metrics used to conduct such an evaluation. It must also develop metrics and evaluations for other collection programs. Fundamental questions like whether there is a consistent evaluation of these programs beyond 30, 60, or 90-day reports, or if an evaluation is only conducted when asked, are vital to overseeing the programs.

---

[13] Savage, C. 2013. New Leak Suggests Ashcroft Confrontation Was Over NSA Program. *New York Times*, June 27, 013.http://www.nytimes.com/2013/06/28/us/nsa-report-says-internetmetadata-were-focus-of-visit-to-ashcroft.html [Accessed 3 Oct 2013]

The Review Group must not rely exclusively on detailed employees from the Executive Branch or the intelligence community. It should reach out to the Technical Advisory Groups of both the SSCI and HPSCI. The Review Group could also hire an outside technologist to serve as an independent expert for the Review Group.

Review NSA's Cryptographic Strategy

Even before the latest information published about the NSA's strategies for cryptography, there was significant concern in the technical community about the potential the subversion of international security standards and the use of legal or extra-legal processes to gain access to private keys held by major service providers. Both actions compromise the privacy and security of domestic data and communications on a mass scale.

When the government pushes "cybersecurity" bills to protect our computer networks, and when law enforcement repeats its "going dark" talking point, it is unthinkable that the NSA is deliberately and covertly sabotaging our devices and networks. This seriously undermines privacy and security, as well as public trust in privacy and security technologies—and in all related government action. Moreover, the government has never explained how the NSA has the statutory authority to operate domestically to weaken or introduce vulnerabilities in the domestic data infrastructure.

Historically, backdoors built for—and by—governments have not remained accessible only to the government. Black hat hackers, criminals, and others have used backdoors to attack people ranging from innocent users to Prime Ministers. In one example, an unknown hacker used government backdoors to spy on Greek politicians—including the prime minister.[14] Infiltrating companies, creating backdoors, and undermining international cryptographic standards make everyone unsafe.

Backdoors are not only a security issue. Weakening commercial products with backdoors is a serious economic issue. Foreign government, foreign businesses, and the public will stop using products that possess vulnerabilities and backdoors. The leading edge of America's tech sector must not be lost. In short, the Review Group must investigate the extent to which the NSA's cryptologic strategy has decreased our national security.

Conclusion

The Reform Group has much to accomplish in a short period of time. First, it must engage in a complete review of how the modern technological collection capacities

---

[14] Prevelakis, V. and Spinellis, D. 2013. *The Athens Affair*. Available at: http://spectrum.ieee.org/telecom/security/the-athens-affair/0 [Accessed: 3 Oct 2013].

impact potential privacy concerns of everyday users, both of US and non-US persons. Second, it must offer recommendations to fix many of the aspects of the broken classification system it will encounter. This includes overclassification, keeping its documents away from public scrutiny, and not following FACA. Third, the Review Group must review the NSA's cryptographic strategy. The NSA should be conducting targeted, and individualized surveillance, not undermining security standards. Such a strategy is in direct contrast to many actions by the United States' own State Department, which promotes anonymizing and encryption technology as methods to advance free speech in authoritarian regimes. Lastly, the Review Group must obtain an outside technologist that is not a member of the intelligence community. These actions will be an encouraging start from the Review Group.

Respectfully submitted,

Mark M. Jaycox
Lee Tien

Electronic Frontier Foundation