The NSA, Mass Surveillance, and the Fourth Amendment

Michael Hopkins
Yale University
michael.hopkins@yale.edu

Abstract

In light of the recent Edward Snowden leaks, the NSA and its operations have come under increasing scrutiny by Americans. With NSA projects ranging from the acquisition and storage of internet data on a massive scale to the engineering of encryption backdoors that compromise internet security, it is important for U.S. citizens to consider what limits should be placed on U.S. intelligence organizations in an age of rapid technological development. In this paper, I focus on concisely summarizing the NSA’s recent projects, as well as the technological means through which the NSA achieves its objectives. Then, I draw upon Fourth Amendment precedents to determine which NSA actions should be considered unconstitutional. Finally, I close with policy recommendations for laws and regulations to constrain the government’s mass collection and use of data to ways congruous with the Fourth Amendment that still allow the government the flexibility and dynamism to provide security against terrorism and legitimate threats.

1. Legal Background on Surveillance

The Fourth Amendment marked the repudiation by the United States of general search warrants, known as writs of assistance in colonial America. The Fourth Amendment affirms, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Above all, the Fourth Amendment protects the privacy interests of U.S. citizens and legal aliens and their freedom from arbitrary searches. Justice Harlan in his concurring opinion in *Katz v. United States* provides a two-pronged test for determining whether the Fourth Amendment applies in a given situation, which has become the de facto standard today. In order to receive Fourth Amendment protection, a person must have a subjective expectation of privacy, and society has to deem that expectation reasonable. The emphasis on society – not Congress, law enforcement, the president, or judges – is important.

When the Fourth Amendment was originally enacted in 1792, the meaning of “unreasonable searches and seizures” was clear: A search entailed a law enforcement officer physically trespassing on a person’s private property, and a seizure involved an officer confiscating private property or detaining a person. However, as people and their data become increasingly mobile with efficient transportation and the internet, such a strict interpretation of the Fourth Amendment would fail to capture the spirit behind the amendment – to prevent an overreaching government and to provide a certain degree of privacy for U.S. citizens from the government. In 1967 *Katz v. United States* expanded the interpretation of searches and seizures under the Fourth Amendment from including only physical intrusion to also including immaterial intrusion. While *Katz v. United States* specifically concerned law enforcement officers eavesdropping on telephone conversations with the aid of a tape recorder, similar interpretations have been applied to data transmitted over the internet.

The Foreign Intelligence Surveillance Act of 1978 provided a framework for clandestine surveillance by the U.S. government. The act created the FISA court and congressional oversight committees to monitor secret government surveillance by entities such as the NSA. The goal of government surveillance was to obtain foreign intelligence information, which includes information about foreign terrorism, espionage, sabotage, and threats against the United States from real or potential attacks. Initially, surveillance of a non-U.S. person could be conducted for up to a year without a court order, while surveillance of a U.S. person could, surprisingly, be conducted in secret for three days without a warrant. A U.S. person is defined to be a U.S. citizen, a legal alien, an association comprised of a significant number of U.S. citizens or legal aliens, or a U.S. corporation. FISA has been amended on a handful of occasions...
since 1978, but there are still a few key points worth noting. First, no law can override or infringe upon the guarantees made by the U.S. Constitution and its amendments. In particular, U.S. persons are entitled to full protection under the Fourth Amendment. Government entities like the NSA do not, however, have to adhere to the same procedures when collecting information from non-U.S. persons. While the FISA court provides oversight, the NSA does not need a warrant to collect information on non-U.S. persons. Most objections to NSA activities center on whether they ensure protection of U.S. persons under the Fourth Amendment.

2. Summary of NSA Actions

2.1 Tapping into Fiber-Optic Cables

The United States has a unique advantage when it comes to monitoring internet traffic: Much of the world’s international internet traffic is routed through North America. This result stems from the current infrastructure of the internet. An astounding percentage of international bandwidth capacity passes through North America. According to a 2011 study by Telegeography research, the bandwidth capacity between the U.S. & Canada and Europe is 4,972 Gbps, between the U.S. & Canada and Latin America & the Caribbean is 2,946 Gbps, and between the U.S. & Canada and Asia & the Pacific is 2,721 Gbps. As a point of comparison, the bandwidth capacity between Europe and Latin America & the Caribbean is 5 Gbps, between Europe and Africa is 343 Gbps, between Asia & the Pacific and Africa is 40 Gbps, and between Asia & the Pacific and Europe is 1,345 Gbps. Clearly, much of the total international bandwidth capacity of the internet passes through the United States.

To see why the United States’ leading position in internet bandwidth capacity results in much of the world’s internet traffic being routed through the United States, it is important to examine the business model for the internet: Internet providers connect their customers to the rest of the internet for a fee. When a customer sends or receives data, the internet provider must determine a path to transmit the data along. Occasionally, this path will not be completely contained within the internet provider’s network. As a result, the internet provider will have to pay another internet provider some fee to transmit the data for some sub-path.

The goal of an internet provider is to maximize profits and thus to minimize fees paid to other internet providers for using their networks. The price of transmitting data along a path is related to the traffic along the path at a given point in time and the capacity along the path. If traffic is low relative to capacity, the price will be low, and if traffic is high relative to capacity, the price will be high. As a result, data travelling across the internet can take seemingly strange, roundabout paths because internet providers seek to minimize cost, not distance. For this reason, data sent from Europe to Asia, rather than taking a direct path between the two continents, could pass from Europe to the United States and then finally to Asia. As a result, the United States can gather a great amount of foreign intelligence by intercepting internet data that crosses into U.S. territory.

The NSA realized what a good opportunity this situation provided to gather foreign intelligence. Affidavits submitted in Tash Hepting et al. v. AT&T Corporation et al. in early 2006 detail the NSA’s wiretapping of telephone and internet cables. The affidavits explain how the NSA set up surveillance equipment at a number of AT&T’s switching centers, hubs for AT&T’s internet traffic where transmitted data can be exchanged with other internet service providers. AT&T switching offices in Seattle, San Jose, Los Angeles, and San Diego were a few of the AT&T switching centers that were monitored by the NSA.

In these switching centers, the NSA used fiber tapping to replicate inbound internet traffic for its own use. Fiber tapping allowed the NSA to split incoming internet data so that 50% of the signal strength was diverted along separate fiber cables, while the other 50% of the signal strength remained on its original path. In essence, a copy of the internet traffic was made. 50% of the initial signal strength is still sufficient for the signal data to be properly interpreted. The replicated signal was diverted to a secure room monitored by the NSA. In this room, the NSA used traffic analyzers made by the big data analytics company Narus, which were capable of processing incoming data in real-time at data rates of 10 Gbps. These traffic analyzers selected a subset of incoming data to forward over private internet cables to a central NSA location. J. Scott Marcus, a former senior advisor on internet
technology at the U.S. Federal Communications Commission, alleges that these traffic analyzers forwarded almost all data to the central NSA location. In other words, very little effort was made to exclude data associated with U.S. persons.

There are a number of alarming problems with the NSA’s monitoring of AT&T’s internet traffic. First, data interception was occurring within the U.S., rather than at its borders, increasing the amount of domestic data that was intercepted. This problem was further compounded by the lack of adequate data filtering to exclude data that could reasonably be inferred to be associated with domestic traffic. This resulted in the NSA storing a large amount of data on U.S. citizens at its central location. However, the problem is more fundamental than just the location at which the NSA chooses to intercept data. The internet is largely a decentralized system that transcends political boundaries. Data sent between two U.S. persons residing in the U.S. could cross U.S. borders and then reenter the U.S. at a later point along its path if this path happens to be the cheapest. Just because data enters the U.S. from another country does not necessarily mean that the data constitutes foreign intelligence. While trying to limit the amount of domestic data collected is a tough challenge, setting up data interception posts only at U.S. borders and developing good filtering algorithms could significantly reduce the data collected on U.S. persons.

A more recent project, detailed in the Edward Snowden leaks, that intercepts data traveling along fiber-optic cables is Tempora. Tempora is a program created by the British GCHQ in 2011 that intercepts internet and telephone data at locations in the United Kingdom and abroad. In typical foreign intelligence rhetoric, the GCHQ dubbed two of Tempora’s subprojects “Mastering the Internet” and “Global Telecoms Exploitation.” The Tempora project maintains data for three days and metadata for thirty days before making a determination about what data to preserve long-term. The scope of data obtained is broad, ranging from telephone call recordings to email messages to HTTP requests, and The Guardian claims that domestic data is not differentiated from foreign data. The GCHQ handles 200 million “telephone events” per day and has tapped a total of 200 fiber-optic cables, which have a combined maximum capacity of over 21 petabytes per day. Edward Snowden has characterized Tempora as “the largest program of suspicionless surveillance in human history.”

As a partner of the GCHQ, the NSA has access to all of the data collected by Tempora. GCHQ lawyers have advised the NSA, “We [the United Kingdom] have a light oversight regime compared with the US.” One of the dangers of Tempora is that the NSA has access to a vast collection of data, some of which is data concerning U.S. persons. The fact that Tempora is a loosely regulated British program is worrisome because it means that the NSA isn’t even in control of what information is collected and stored long-term. A significant portion of the data collected by Tempora is data originating in the U.S. that crosses the Atlantic Ocean with a final destination somewhere in Europe. Alarming, with dwindling storage costs and increasing technological sophistication, many foreign intelligence agencies are tending towards an approach of gathering all possible sources of data in bulk, rather than engaging in a cost/benefits analysis of collecting different types of data.

2.2 PRISM: Obtaining Data Directly from the Source

In addition to acquiring data through tapping fiber-optic cables, the NSA also gathers data directly from the servers of U.S.-based corporations through a program known as PRISM. PRISM allows for the NSA to request all information pertaining to a FISA court approved search request from internet companies. Companies that have had to produce information to comply with PRISM include Google, Microsoft, Yahoo, AOL, Facebook, and Apple. Approximately 98% of PRISM data has been obtained from Google, Microsoft, and Yahoo. The cost for companies to become PRISM-compliant can be millions of dollars, which is reimbursed by the NSA. Data obtained through PRISM includes email messages, video and voice chats, photos, VoIP conversations, files, video sessions, login information, and other forms of online data. One manner in which the NSA can exploit PRISM is by obtaining data that was encrypted when traveling across the internet. Tapping fiber-optic cables does not yield much useful information when data is encrypted. However, the NSA can easily query for the
unencrypted data if the data’s destination is a U.S.-based internet corporation.

The requirements to obtain a FISA warrant for a PRISM query are relatively lax. A FISA judge only requires 51% confidence that the search terms requested in the warrant target a foreign national not on U.S. soil.\textsuperscript{10} In practice, the NSA usually satisfies this requirement by verifying that the selector chosen does not match any known Americans in any of its databases.\textsuperscript{10} Currently, there are 117,675 active PRISM targets.\textsuperscript{10}

Recently, U.S. internet companies reached an agreement with the NSA to be able to report very rough statistics on the frequency of NSA queries through PRISM. As an example of the approximate scale of PRISM, Google said that for the time period between January and June of 2013, it received 0-999 FISA requests involving 9,000-9,999 user accounts.\textsuperscript{13} Technology companies are still fighting to be able to give a more precise depiction of the information they communicate through PRISM, including the exact number of affected accounts and the exact nature of the issued PRISM requests.

2.3 Bulk Collection of Metadata

In a similar vein to PRISM, the NSA requested and received call records from Verizon customers from April 25, 2013 through July 19, 2013.\textsuperscript{14} In contrast to PRISM, though, the NSA received the metadata for all phone calls involving Verizon customers over this time period, including calls that were solely domestic.\textsuperscript{14} Phone call metadata includes phone numbers, phone locations, call duration, time of call, and call identifier.\textsuperscript{14} The NSA did not need a warrant to view any of the metadata.

It is very likely that Verizon was not the only telephone company to be given an order like this and that this 3-month time period was not the only time period over which Verizon had to comply with an NSA request. Recent decisions made by the FISA court spurred Senators Ron Wyden and Mark Udall, members of the Senate Intelligence Committee, to remark, “There is now a significant gap between what most Americans think the law allows and what the government secretly claims the law allows.”\textsuperscript{15}

2.4 Infiltrating Private Networks

Ostensibly, PRISM would provide the NSA with all of the information from U.S.-based internet companies that it could need. However, there is strong evidence that through a program known as MUSCULAR the NSA tapped the communication links between Google’s data centers and the links between Yahoo’s data centers.\textsuperscript{16,17} In a rather coy sketch made by an NSA official of the public internet and Google’s private network, there is an arrow pointing to a drawing of Google’s front end with the description “SSL added and removed here!” with a smiley face.\textsuperscript{16} There is also an arrow pointing to Google’s private network with the description “Traffic in clear text here.”\textsuperscript{16} This drawing suggests that the NSA at least had intentions of intercepting data in Google’s private network while the data was in clear text.

NSA documents indicate that a total of 181,280,466 records were obtained from the internal networks of Yahoo and Google in December 2012 alone.\textsuperscript{18} These records were obtained from data centers abroad. Performing similar operations on U.S. soil would be illegal. However, the sharp difference in regulations in these two scenarios is puzzling. For data consistency and availability, databases often replicate data at three different locations, each at least 500 miles away from the other two locations. This makes it very possible for the data of a U.S. person to reside outside of U.S. borders. Because of such data replication, the significant incongruity between NSA rules for gathering data domestically and gathering data abroad needs to be addressed.

Google’s chief legal officer, David Drummond, did not seem very surprised by this NSA revelation, saying that Google has “long been concerned about the possibility of this kind of snooping.”\textsuperscript{18} He added that Google was “outraged at the lengths to which the government seems to have gone to intercept data from [Google’s] private fiber networks, and [such snooping] underscores the need for urgent reform.”\textsuperscript{18} Eric Grosse, the vice president for security engineering at Google, said that Google is planning to encrypt data traveling between its data centers as quickly as possible.\textsuperscript{19}

The MUSCULAR project is certainly one of the more puzzling NSA projects. The only reason that the NSA could have for creating MUSCULAR
when PRISM can be used to gather data constrained to particular search terms is to expand the scope of the data that it collects. The optimization problem that the NSA seeks to solve is how to maximize the amount of data it collects subject to existing regulations. In particular, the NSA does not seem to give strong weight to the utility of information or to the privacy considerations implicated with the information that it collects.

2.5 Backdoors

The NSA project BULLRUN involves attempts to undermine encryption in various network communication technologies.² The NSA reports that it has found certain vulnerabilities in the encryption in TLS/SSL, HTTPS, SSH, VPN’s, VoIP, and WEBSMAIL.²

There are a handful of different approaches that the NSA uses to try to circumvent encryption on the internet. First, the NSA lobbies to try to influence international encryption standards, particularly through its influence on the National Institute of Standards and Technology.²⁰ Another approach that the NSA pursues is brute force attempts at breaking encryption using supercomputers.²⁰ This approach has particular appeal for obtaining a window into the past. While the NSA might not be able to ever launch a brute force attack against modern encryption standards, since key sizes increase over time, the NSA might be able to store data long enough so that it can decrypt communications from the past when smaller key sizes were used. The last broad approach that the NSA uses is working with internet service providers and technology companies to engineer backdoors in commercial encryption software.²⁰ The danger inherent in this approach is that anyone who discovers the backdoor can exploit it. This severely compromises the security of the internet.

One alarming example of such a backdoor in commercial encryption software is a random number generator deployed in RSA’s Bsafe that allowed the NSA to exploit knowledge about how the random numbers were generated.²¹ The random number generating method, which was approved by the National Institute of Standards and Technology, was known as the dual elliptic curve method, which is now recognized to be flawed.²¹ Apparently, the NSA intentionally engineered a backdoor in the algorithm in order to compromise RSA encryption.

A $10 million contract that the NSA signed with RSA casts suspicion on RSA, although the security industry pioneer denies complicity.²¹

Specific details of the NSA’s recent progress in undermining encryption have not been revealed, but already released NSA documents celebrate the NSA’s “defeating [of] network security and privacy.”²⁰ Furthermore, GCHQ officials that were recently briefed on NSA progress were described as “gobsmacked.”²⁰ Any vulnerabilities in encryption, which is seen as one of the best defenses against a prying government, are certainly very concerning.

2.6 Storing Collected Data in Massive Databases

As has been detailed up to this point, the NSA collects vast amounts of data. In the case of AT&T switching centers, the NSA stored data at a rate of approximately 10 Gbps per AT&T switching center (of which there were many), and in the case of Tempora, the GCHQ could potentially gather up to 21 petabytes of data per day. Clearly, massive databases with strategic design and organization are needed in order to be able to handle and efficiently query such large quantities of data.

One project that seeks to make the NSA’s vast collection of data useful to NSA operations is XKeyscore. XKeyscore is a project that allows for NSA agents to monitor the internet activity of suspects in real-time or through mining a huge database of internet data captured from sources like tapped fiber-optic cables and PRISM.¹ The scope of information that can be accessed through XKeyscore is broad, including email messages, web traffic through HTTP requests, address book entries indexed by phone number, and website specific data indexed by user login ID.¹ In order to access this data, queries can be issued involving an email address, email domain, filename, file extension, IP address and port, any of the headers in an HTTP request, phone number, or user login ID.¹ The NSA is seeking to target VoIP in the future and to exploit additional networking protocols.¹ Similar to Tempora, XKeyscore stores all intercepted data for three days and all metadata for thirty days.¹ The central purpose of XKeyscore is to “slow down the internet.”²² In other words, XKeyscore serves as a buffer for internet data while determinations are made about what data should be preserved longer.
The database infrastructure of XKeyscore consists of 500-700 Linux servers spread out over 150 sites around the world, predominantly in Europe, Central America, and the Middle East.\(^1\)

The traffic volume for XKeyscore, like most NSA projects, is massive. 1-2 billion records are added daily.\(^2\) A 2007 NSA report estimated that 850 billion “call events” and 150 billion internet records are stored within XKeyscore databases at any given point in time.\(^3\) William Binney, a former NSA mathematician, estimates that 20 trillion phone and email records concerning only U.S. citizens are stored at any given point in time across all NSA databases.\(^4\)

By law in order for NSA personnel to access XKeyscore data on US citizens, they have to obtain a FISA warrant. The NSA does not need a warrant to collect information on a US citizen though if the US citizen is in communication with a foreign target. However, Edward Snowden reports that oversight is minimal. He claims, “I, sitting at my desk, could wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email.”\(^5\) If such claims are true, American civil liberties are being severely compromised, and programs like XKeyscore need to be addressed.

3. Examining the Constitutionality of NSA Actions

3.1 The Objectives of U.S. Intelligence Agencies

The five major goals of U.S. intelligence include countering terrorism, preventing nuclear proliferation, obtaining foreign intelligence through computer hacking, monitoring critical events abroad, and combating espionage directed against the United States.\(^6\) Of these five goals, combating terrorism is the biggest priority: 1 in 4 employees for U.S. intelligence agencies are working towards combating terrorism.\(^7\)

The 2013 black budget – expenditures that go towards U.S. national intelligence programs that are intended to be kept secret – totaled $52.6 billion.\(^8\) Of this sum, $10.5 billion went towards the NSA.\(^9\) Since the September 11th terrorist attacks on the United States, these figures are estimated to have increased dramatically. Currently, the black budget and the U.S. military intelligence budget total $75.6 billion.\(^10\) This figure is even greater than estimates for Cold War intelligence spending, which was approximately $71 billion per year in today’s dollars at its peak in the 1980s.\(^11\)

Alarmingly, this trend towards spending significantly more money on national intelligence has been accompanied by a general lack of transparency in the U.S. intelligence community. Lee H. Hamilton, a former chairman of the House Intelligence Committee, aptly criticized the current state of affairs: “Nobody is arguing that we should be so transparent as to create dangers for the country… there is a mind-set in the national security community: ‘Leave it to us, we can handle it, the American people have to trust us.’ They carry it to quite an extraordinary length so that they have resisted over a period of decades transparency… The burden of persuasion as to keeping something secret should be on the intelligence community, the burden should not be on the American public.”\(^12\)

Indeed, the preservation of national security should not by itself be an automatic excuse for the secrecy of government actions.

Rapidly growing funds, a lack of transparency, sweeping technological innovation, and a rallying cry in the September 11th terrorist are a dangerous mixture of circumstances for the preservation of privacy from government intrusion.

3.2 The Bulk Collection of Metadata

Over a three-month period, FISA required Verizon to supply the NSA with the metadata of all phone calls placed with at least one party in the United States.\(^13\) To determine the legality of such a request, there are two important questions to ask: Does Section 215 of the Patriot Act authorize the bulk collection of telephone metadata, and is the bulk collection of telephone metadata congruous with the Fourth Amendment? The answer to both of these questions is no.

Section 215 of the Patriot Act, the business records provision, specifies that the Director of the FBI “may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities…” The collection of telephone metadata certainly falls
within the scope of Section 215: Telephone metadata would be considered records. Decomposing this statute, there are three valid justifications for collecting records under Section 215: to gather information on people who are neither U.S. citizens nor legal aliens, to provide security against international terrorism, and to provide security against secret intelligence activities.

In order to authorize the bulk collection of telephone metadata associated with millions of U.S. persons, a justification of protecting the United States from international terrorism or protecting it from secret intelligence activities must be used. Indeed, the Obama administration attempts to contend just that. It argues, “To identify potential terrorist communications ... requires collecting and storing a large volume and high percentage of information about unrelated communications.”26 Collecting the metadata of all Americans is necessary to “ensure that the much smaller subset of terrorist-related telephony metadata records are contained within the dataset... Because the telephony metadata must be available in bulk to allow the Government to identify the records of terrorist communications, there are ‘reasonable grounds to believe’ that the data are relevant to authorized investigations to protect against international terrorism, as Section 215 requires, even though most of the records in the database are not associated with terrorist activity.”26

It is important to step back for a second and to consider the crux of the Obama administration’s argument: In order to achieve the goal of combatting terrorism, it contends that it must indiscriminately collect all telephone metadata. However, if this were the intent behind Section 215 of the Patriot Act, then there would be no reason for lawmakers to have even listed justifications for the collection of tangible things. Instead, Section 215 wouldn’t have focused on the justifications for confiscating tangible items but rather on justifications for the usage of such items after indiscriminate confiscation. For this reason, a narrow interpretation of Section 215 is the only interpretation that seems reasonable. Certainly, a narrow interpretation of Section 215 would not support the systematic collection of telephone metadata of all U.S. persons.

A much more fundamental question is whether any law could grant the government the power to collect telephone metadata on all U.S. persons. In other words, does the Fourth Amendment permit the government to collect metadata indiscriminately?

The current precedent holds that the bulk collection of metadata is constitutional, but there is significant evidence that this could change. In 1979 Smith v. Maryland held that phone records are not protected by the Fourth Amendment.27 The justification relied on the “third-party doctrine,” the notion that one does not have a reasonable expectation of privacy when he or she transmits information (in this case phone numbers) through a third party.27

There are a number of flaws in the third-party doctrine. First, in an age of increasing interconnectedness and dependence on technology, the third-party doctrine completely misses the spirit of the Fourth Amendment.28 Based on an application of the third-party doctrine, one does not have a reasonable expectation of privacy in email messages, online photos, GPS location data, data stored in the cloud, social media data, credit card purchase histories, and numerous other forms of electronic data. It is unreasonable to suggest that a person could navigate present-day society without entrusting a significant amount of private data to third parties. Thus, to accept the third-party doctrine is to admit the defeat of privacy in a digital age.

Signs indicate that the Supreme Court could reverse its position on the third-party doctrine in the near future. In United States v. Jones (2012), the Supreme Court broke from established precedent, which upheld the constitutionality of law enforcement officers using GPS devices to track the movements of suspected criminals. Instead, the justices deviated from the “reasonable expectation of privacy” standard from Katz v. United States and, at least in the majority opinion, considered law enforcement officers attaching a GPS device to Jones’ car a trespass against Jones and thus an unreasonable search.29 Considering the Fourth Amendment through a combination of a property-based approach and the reasonable expectation of privacy standard is a step in the right direction for interpreting the Fourth Amendment in its original intent in a digital age.
Perhaps the greatest surprise from *United States v. Jones* was Justice Sotomayor’s relatively direct call by the standards of the Supreme Court to reevaluate the third-party doctrine: “It may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age...”\(^{30}\) Certainly, the verdict in *United States v. Jones* and Justice Sotomayor’s concurring opinion in the case are steps in the right direction for trying to preserve the spirit of the Fourth Amendment.

### 3.3 XKeyscore and the Mass Collection of Data

XKeyscore allows the NSA to efficiently utilize the information that it collects. XKeyscore manages data obtained through methods such as tapping fiber-optic cables and confiscating data from the servers of U.S. technology companies via PRISM through a distributed database. All data fed into XKeyscore is stored for approximately three days, and all metadata is stored for about thirty days before a determination is made to keep the data for longer.

There are two key questions to consider when examining a program like XKeyscore: First, does the NSA violate the Fourth Amendment if it collects data in bulk, knowing that it will incidentally capture data on U.S. persons in the process, and, second, what should the oversight process be for controlling access to the massive distributed database underlying XKeyscore?

To answer the question of whether it is constitutional for the NSA to intentionally collect data on a U.S. person, one could apply the Katz test and ask if the U.S. person has a reasonable expectation of privacy in data transmitted over the internet. In the case of email messages, the Sixth Circuit Court of Appeals in *U.S. v. Warshak* ruled that email messages stored on an ISP server are protected by the Fourth Amendment and thus require a warrant to be searched by law enforcement.\(^{31}\) The court’s verdict read, “Over the last decade email has become ‘so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument for self-expression, even self-identification.’” As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise.”\(^{31}\) In keeping with the spirit of the Fourth Amendment, it certainly seems that email messages and other forms of transmitted data should receive the same protection as, for example, letters sent through the U.S. post office.

While it would be a violation of the Fourth Amendment to intentionally collect data transmitted over the internet by specific Americans, it is worth considering whether incidental collection of data associated with U.S. persons is unconstitutional.

In 2011 the FISA court determined that the collection of tens of thousands of email messages through PRISM between Americans was unconstitutional.\(^{12}\) The NSA defended its actions by claiming that the situation amounted to a “complex technical problem,” instead of an intentional violation of American civil liberties.\(^{12}\) The ruling declared that a technical inability to be able to separate domestic email messages from foreign email messages was still a violation of the Fourth Amendment. Such a stance, while directed towards the collection of email messages through PRISM, has interesting implications for the incidental collection of data on U.S. persons through programs like the tapping of fiber-optic cables with the intention of gaining foreign intelligence.

Even if it would be unconstitutional to permanently store massive amounts of indiscriminately collected data from the internet because data from U.S. persons could not be reliably parsed out, one interesting question concerns whether or not the temporary storage of data until it can be processed is constitutional. One could apply similar logic as was used in *Sony Corp. of America v. Universal City Studios, Inc*, which found that VCR’s could be considered time-shifting devices and thus their recording capabilities did not infringe upon copyrights.\(^{32}\) In a similar manner, storing data for three days and metadata for thirty days could be considered buffering the data until it could be reliably processed.

In order to examine the collected data on a particular U.S. person a warrant granted upon probable cause should be required on a per situation basis. This point is pretty straightforward, but claims have surfaced that analysts need no prior authorization to search through the vast database underlying XKeyscore. Clearly, with such sensitive
information stored in the database, oversight needs to be very rigorous.

3.4 Parallel Construction

XKeyscore provides the NSA with a massive database of information. Current data collection procedures, which focus on the bulk collection of data with minimal filtering, ultimately result in the NSA storing, without a warrant or probable cause, a lot of information on Americans. The NSA claims that it keeps this data only until it can determine whether or not the data constitutes foreign intelligence. This justification requires an enormous amount of trust from U.S. persons that intelligence agencies will not misuse such a vast collection of data.

Alarmingly, reports have surfaced that the U.S. Drug Enforcement Administration’s Special Operations Division (SOD), which is comprised of agents from the NSA, FBI, CIA, the Department of Homeland Security, and a number of other partner agencies, has been leaking intelligence information on U.S. persons to local law enforcement agencies. Internal SOD documents state that local law enforcement agencies are instructed to conceal SOD tips from defense lawyers and even prosecutors and judges in some cases. Local law enforcement is instructed to use these tips as a basis for parallel construction – using knowledge gained from an initial tip to catch a criminal in the act. The initial tip is concealed, and law enforcement manipulates the investigative trail to cover everything up.

Parallel construction performed in this manner violates a defendant’s right to a fair trial. The concealment of evidence violates certain pretrial evidence discovery rules. During the discovery process, the judge examines whether certain evidence, like classified information or the identities of informants, must be shared with the defense in order to ensure a fair trial. To not even submit initial leads to the judge to examine in this pretrial discovery phase is very alarming. Nancy Gertner, a professor at Harvard Law School, echoed similar sentiments: “I have never heard of anything like this at all...It is one thing to create special rules for national security. Ordinary crime is entirely different. It sounds like they are phonying up investigations.” Transitioning from indiscriminate data collection in order to gather foreign intelligence to similar methods of data collection to catch U.S. drug distributors sets a dangerous precedent: it sets in motion the beginning of a mission creep of NSA projects. If such a mission creep isn’t shut down from the start, gathering foreign intelligence could turn into simply gathering intelligence, which could be used to incriminate a U.S. person in any crime.

The SOD contends that the information relayed to local law enforcement agencies is all legally obtained: Information sources include foreign governments, court-sanctioned wiretappings, and U.S. intelligence agencies. The information from intelligence agencies is screened to ensure that the people implicated are not U.S. persons, the SOD claims. However, in this case, it’s not the source of the information that is objectionable. It is the concealment of the information entirely at trial that is very concerning. Such a practice opens up the door for illegally obtained data to be utilized to initiate investigations.

3.5 Backdoors

Over the last few decades, U.S. intelligence agencies have attempted to dismantle and undermine encryption and security on the internet. For example, in the 1990’s the NSA advocated for the Clipper chip, an encryption device whose cryptographic key would be shared with the government upon creation, providing the government with the ability to decrypt anyone’s messages. More recently, it was revealed that the NSA engineered a backdoor in RSA’s Bsafe by promoting a random number generating algorithm, the dual elliptic curve method, that the NSA knew had vulnerabilities. The NSA even lobbied for the National Institutes of Standards and Technology to approve the method, which is required for the government to be able to purchase such products.

While trying to undermine encryption is not unconstitutional in and of itself, it is a very dangerous and concerning practice. When the NSA engineers a backdoor in a commercial encryption technology, any individual who discovers the backdoor can exploit it as well, and security is significantly diminished as a result. Bruce Schneier of Harvard’s Berkman Center for Internet and Society purports that “the NSA is undermining the very fabric of the internet.” Even a White House review panel admitted that “encryption is an
essential basis for trust on the Internet” and urged
the NSA to stop its efforts to subvert it. While
subverting encryption isn’t unconstitutional, it is
definitely in opposition to the best interests of U.S.
citizens.

4. Conclusion

The first step towards reaching a solution for
gathering foreign intelligence that balances privacy
and national security is getting a conversation
started among U.S. citizens. Certainly there are
ways to increase security without sacrificing
privacy: more precise data filtering and data mining
algorithms, alleviation of the root issues that breed
terrorism and extremism, improvements in
diplomatic channels, and countless other ways.
However, in general privacy and national security
are at odds with each other. Increasing national
security generally necessitates concessions in
certain forms of privacy, and increasing privacy by
limiting government surveillance reduces the
resources at the government’s disposal to protect
national security. This is not to say that restricting
privacy completely implies perfect national security
but rather that there are implicit tradeoffs between
security and privacy that U.S. citizens must
acknowledge when proposing a framework for the
collection of foreign intelligence.

Currently, there is a disconnect between
government actions and the desires of U.S. citizens.
For the first time since the September 11th terrorist
attacks, U.S. citizens are more afraid of the
infringement on their civil liberties by the U.S.
government than of international terrorism. They
are doing so through PRISM, the collection of data
from fiber-optic cables, backdoors in commercial
encryption technology, the confiscation of
telephone metadata, and a handful of other national
intelligence endeavors. The means through which
U.S. national intelligence agencies have chosen to
combat terrorism have actually become more
alarming to U.S. citizens than terrorism itself. In a
recent poll, 62% of American were opposed to the
government reading any domestic email without a
warrant, and 71% of Americans were opposed to
the government listening to any domestic phone call
without a warrant. There certainly seems to be
incongruity between government opinion and
popular opinion in the United States as a result of
the Edward Snowden leaks.

Since the Edward Snowden leaks, many
organizations have tried to challenge NSA actions
that threaten civil liberties. The Electronic Frontier
Foundation has sued the Department of Justice over
secret interpretations by the FISA court of Section
215 of the Patriot Act. Major U.S. technology
corporations, including Google, Microsoft, and
Yahoo, fought to release coarse statistics on PRISM
compliance and are still urging the Senate
Intelligence Committee to let them release more
precise statistics, as well as the nature of the PRISM
requests that they have received.

The significant disconnect between the U.S.
government and U.S. citizens became clear after the
initial NSA leaks concerning the bulk collection of
telephone metadata from Verizon. While U.S.
citizens were outraged, members of Congress failed
to pass an amendment to withdraw funding for the
NSA project associated with the bulk collection of
telephone records on Americans.

A number of different pieces of legislation of
varying radicalness have been proposed to reform
NSA practices. On the more conservative end of the
spectrum is a bill backed by Senator Dianne
Feinstein. The bill would preserve the metadata
collection program under the NSA but would
increase the transparency of the program. The NSA
would be required to publish an annual report on
metadata collection and to set a lower time limit for
how long telephone metadata could be stored. The
bill also clearly articulates the standards that must
be met for the NSA to monitor the phone
conversation associated with a particular phone
number and requires the NSA to report each phone
number that it is monitoring to the FISA court.
Supporters of the bill backed by Senator Feinstein
have also expressed openness to appointing a public
advocate to be an adversary in front of the FISA
court.

Taking a more reform-oriented approach, the
chairman of the Senate Judiciary Committee,
Patrick Leahy, and congresswoman and co-author of
the Patriot Act, Jim Sensenbrenner, have proposed
sweeping changes across U.S. intelligence
agencies. Senator Leahy and congressman
Sensenbrenner emphasize that transparency alone is
insufficient; significant reform is needed. In perhaps the most telling sign that the FISA court has breached the scope of the Patriot Act, Jim Sensenbrenner expressed his dissatisfaction with the current state of affairs: “Following 9/11, the Patriot Act passed the judiciary committees with overwhelming bipartisan support. But somewhere along the way, the balance between security and privacy was lost. It’s now time for the judiciary committees to again come together in a bipartisan fashion to ensure the law is properly interpreted, past abuses are not repeated and American liberties are protected.”

Senator Leahy and congressman Sensenbrenner through their bill seek to eliminate ambiguities in the Patriot Act and the Foreign Intelligence Surveillance Act that allow U.S. intelligence programs to target the communications of U.S. persons. Similar to Senator Feinstein’s bill, Senator Leahy and congressman Sensenbrenner’s bill would increase the transparency of NSA court orders and would appoint an independent public advocate to serve as an adversary before the FISA court with the duty or protecting U.S. civil liberties. Senator Leahy and congressman Sensenbrenner’s bill has been well received by members of Congress and legal experts. Elizabeth Goitein, who works for the Brannan Center for Justice at New York University law school, expressed her support for the bill: “This bill would go a long way toward restoring the presumption of privacy for the communications and personal information of law-abiding Americans. The NSA and the Foreign Intelligence Surveillance Court have secretly interpreted the law to allow the broad collection of Americans’ information, even where the law expressly prohibits the targeting of Americans or requires a showing of relevance to an international terrorism investigation. The bill is designed to put an end to this perversion of the law.” When a co-author of the Patriot Act comes forward with a bill that proposes sweeping reform to counteract current interpretations of the Patriot Act, a combination of reform and transparency seems vital.

Another bill, backed by Senators Ron Wyden, Mark Udall, Richard Blumenthal, and Rand Paul, promises sweeping reform of U.S. intelligence agencies. The first major overhaul in the bill would eliminate the bulk collection of telephone metadata. In addition to the bulk collection of telephone metadata being an invasion into the civil liberties of U.S. citizens, Senator Udall states, “It has never been proven to Senator Wyden or me that any of the bulk collection has provided uniquely valuable intelligence that had led to the disruption of any plots.” The bill would also impose stricter regulations on PRISM. The bill contains provisions that seek to prevent reverse targeting of Americans – obtaining data on Americans through PRISM by issuing a query that is supposedly targeting a foreigner. The bill also contains provisions requiring the NSA to take a more active stance in filtering out information accidentally obtained on Americans through PRISM.

The bill backed by Senators Wyden, Udall, Blumenthal, and Paul would also require a constitutional advocate to be appointed when important constitutional and legal issues are being raised before the FISA court. In addition, many previous verdicts in the FISA court would be declassified. Finally, the bill would require U.S. intelligence agencies to be more transparent with their activities and allow private companies to be more transparent about their compliance with U.S. intelligence agencies.

The bills proposed by Senator Feinstein; Senator Leahy and congressman Sesenbrenner; and Senators Wyden, Udall, Blumenthal, and Paul all have their respective merits. When changing circumstances – in this case technological innovation and the September 11th terrorist attacks – lead to the infringement on civil liberties by the government, it is important to not overreact and to not take too aggressive of a stance against the collection of foreign intelligence, which would ultimately be unsustainable. All of the proposed reforms across the three bills are relatively moderate. All of the reforms revolve around clarifying what the NSA can and cannot do with data on U.S. persons, but none of the bills seeks to radically change the rules for how the NSA could only tap fiber-optic cables at the borders of the United States or outside of it. The most judicial approach to reform would involve transparency and incremental change to U.S. intelligence agencies, but there is an argument to be made for instituting massive reform while public sentiment is strong.
On the other end of the spectrum, the bill backed by Senator Feinstein does not seem to propose sufficient reform for the situation. When one of the co-authors of the Patriot Act suggests that the Patriot Act has been grossly misinterpreted, a bill that focuses on transparency without eliminating the bulk collection of telephone metadata on U.S. persons seems insufficient. Ultimately, a combination of the bill proposed by Senator Leahy and congressman Sensenbrenner and the bill proposed by Senators Udall, Wyden, Blumenthal, and Paul -- both with an emphasis on increased transparency, an end to the targeting of American communications, and reform for the FISA court -- seems to be the best solution to the difficult problem of balancing national security with privacy, civil liberties, and the Fourth Amendment, at least at the present moment.

References
5. 50 U.S.C. § 1801(b) 