GEORGETOWN LAW

Laura K. Donohue
Professor of Law

March 14, 2014

Privacy and Civil Liberties Oversight Board
2100 K Street, NW
Washington, DC 20427

Dear Privacy and Civil Liberties Oversight Board,

Thank you kindly for the opportunity to meet with you on March 19, 2014 to discuss Section 702. I will address the statutory and constitutional concerns related to the program at that point.

I am writing in advance, however, to raise a deeper concern: namely, the piece-meal nature of inquiries into Sections 215 and 702 and, consequently, the bifurcated conversation about potential reforms to FISA.

The legislation is built on an understanding of technology that is nearly four decades old. The threat environment has changed. New surveillance techniques carry with them different implications for privacy and civil liberties. Responding on an individual basis to specific concerns, moreover, risks ignoring the potential effects of alterations in the law, as well as opportunities that now present themselves to create a sustainable structure for the future.

A more comprehensive approach should be adopted, and I would be interested in PCLOB's view of this following the hearings. I recognize that it is not realistic to undertake thorough reform by the deadline that the President set in his January 17, 2014 speech. Nevertheless, it is in all parties' best interests to ensure that the framework adopted addresses the related interests of national security, foreign intelligence gathering, and constitutional protections for individual rights.

I am thus writing to propose a taxonomy that may be helpful to you in your effort to move beyond the current framework. I do not take a position on the categories proposed. Instead, the aim is to deepen the conversation about abeyant approaches to foreign intelligence gathering, to allow sufficient discussion of what a comprehensive package could contain, and to place the initiatives that are currently under consideration within a broader framework.

The taxonomy divides foreign intelligence gathering into two categories: front-end collection and back-end analysis and use. Each category contains a counterpoise structured to ensure the appropriate exercise of Congressionally-mandated authorities. For the front-end, this means balancing the manner of collection with requirements for approval. For the back-end, this means offsetting implementation with transparency and oversight. Further delineations mark each category.

600 New Jersey Avenue, NW Washington, DC 20001-2075
PHONE 202-662-9455 FAX 202-662-9454
lkdonohue@law.georgetown.edu

A. Front-End Framework to Collect Foreign Intelligence Information

Front-end considerations relate to the acquisition of information. They divide into (1) the manner of collection, and (2) requirements for approval of the authorities thereby created. (See *Fig. 1*) The structure thus reflects in (1) a positive grant of authority under certain conditions, and, in (2), ways to ensure that the appropriate processes are followed prior to entities acting on those powers. While (2) thus acts primarily as a limitation on (1), it would be too simplistic to say that each category only performs these functions. There are a number of ways the sub-divisions in (1) could be constructed to provide checks on the system. Nevertheless, approaching the question in this manner allows for attention to be drawn to the different functions of the relevant entities.

FRONT-END FRAMEWORK TO COLLECT FOREIGN INTELLIGENCE INFORMATION

Manner of Collection	Requirements for Approval
1. **Type of information** a. Content b. Locational c. Relational d. Transactional e. Personal 2. **Method of access/transmission/storage** a. A/V (immediate observation) b. Communications Technologies c. Paper/tangible goods d. HD/Device e. Server/Cloud Technologies f. Social media 3. **Form in which information is transferred** a. Anonymization and re-identification b. Prior screening by third party 4. **Agency obtaining information** a. Broad institutional design (e.g., NSA/Cybercom division) b. Primary authorization (e.g., FBI, CIA, NSA) c. Concurrences required (e.g., AG, NSD) 5. **Target** a. US v. non-US persons b. Foreign powers/agents thereof c. Terrorists (KSTs/Int'l) 6. **Source of information** a. Private industry - data retention requirements and costs - voluntary v. compulsory compliance - data security - litigation risks b. Third party data holders - relationship to gov't, private entities - division of information between entities - data security. - encryption key holders (internal/external) c. Government agencies d. Non-governmental entities e. International partners (including verification) 7. **Location of information** a. International v. domestic b. Mixed (e.g., cyber) c. Border	1. **Entity Approving Collection** a. Executive - agency-internal - agency-external b. Judicial - special court (e.g., FISC) - ordinary Art. III court - Art. I court c. Other (e.g., private industry) 2. **Construction of entity** a. Selection of decision-makers - originating entity (e.g., Circuit division, regional division, etc.) - manner of selection (e.g., President, Chief Justice, SCOTUS, Congress) b. Length/progression of terms (period of years, staggered terms, term limits) c. Adversarial processes - Rights of challenge - Rights of appeal - Third party rights - Constitutional advocate d. Technological expertise 3. **Scope of approval** a. Application format b. Standards (e.g., particularized, RAS) c. Duration d. Renewal requirements 4. **Verification** a. Third party data holder requirements b. Encryption key holder requirements 5. **Emergency exceptions** a. Substantive requirements b. Timeline for subsequent approval c. Use of information

Fig. 1

1. Manner of Collection

The first two considerations in the manner of collection center on the type of information in question and the method of access thereto, as well as the way in which such information is transmitted and stored. A brief discussion of how both of these categories have changed since the adoption of FISA helps to underscore why the current statute is inadequate as a way to address the contemporary environment.

a. Shift in Type of Information Available

At the most general level, over the past four decades, the law has recognized three principal types of information: content, personally-identifiable information (PII), and business records (including, *inter alia*, banking and financial records). These categories have been provided with different levels of protection.[1] In the current context, however, not only have the contours of these types of information altered, but at least five categories of information relevant to electronic foreign intelligence gathering have emerged: personal, transactional, relational, geolocational, and content-based. (See *Fig. 2*)

The first category, personal information, relates to a single individual whose identity can be obtained from the information itself, or from that information and other information that is in the possession of, or is likely to come into the possession of, the person controlling the information. Traditionally this category has included information such as one's social security number, home address, credit card number, health or medical records, insurance information, and educational records. New technologies, however, have extended this category to include areas like biometric identification markers (e.g., facial recognition, DNA, and iris patterns), habit identification, and pattern matching.

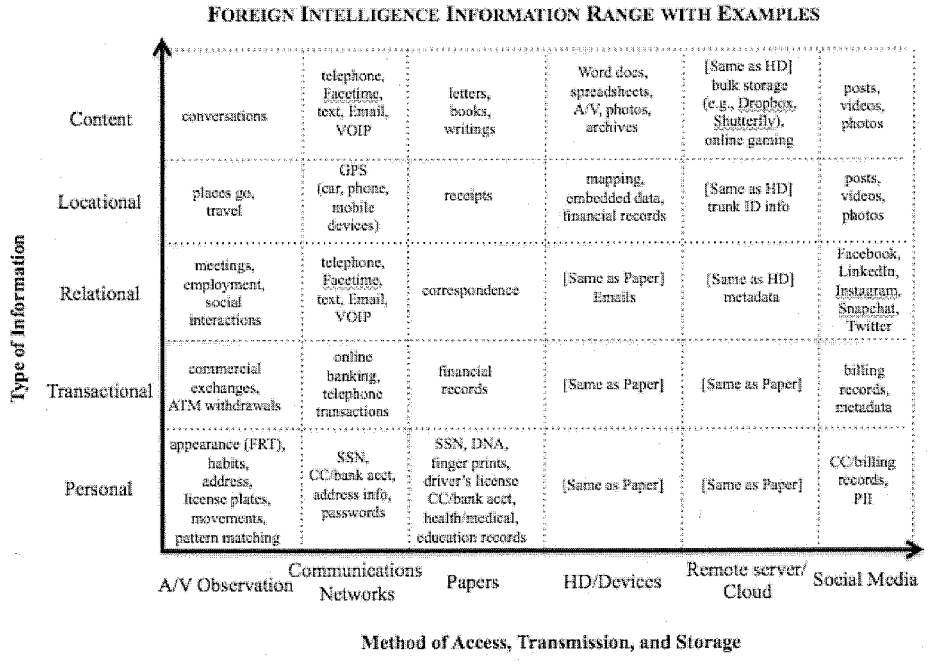

Fig. 2

[1] The Supreme Court, for example, has traditionally applied a higher level of protection to content and, in the context of third party doctrine, a lower level of protection to customer records held by companies. Accordingly, traditional FISA created a more stringent regime for electronic communications or physical searches, wherein content would be obtained, and a lower level of protection for the use of pen registers and trap and trace devices.

The second category, transactional information, incorporates commercial transactions—i.e., the process of buying or selling something. It suggests a contractual relationship between two or more entities in which goods, services, or money are transferred. Historically, this category was limited to banking or financial records or the purchase of property—and, again, differing levels of protection were provided, particularly as it was extended to areas like billing records. But transactional information also includes other contractual agreements between entities and records pertaining thereto.

The third category, relational information, has emerged as an independent area as technology related to social network analysis has evolved. Using both visual and mathematical tools, new technologies allow individuals to map and to analyze various types of flows between people, groups, organizations, geographic regions, computers, URLs, and other connected entities. Relational information gives insight into not just the existence of connections between individuals, but their roles and groupings within a network—i.e., who are the key connectors, leaders, bridges, and isolates, where the key clusters are and who comprises them, who is in the core of the network, and who is on the periphery. Social network analysis yields insight into the distribution of resources (both material and nonmaterial), and potential constraints on individual actions.[2]

The fourth category, locational information, identifies the specific physical location of an object or an individual. It thus relates to the terrain of the real world. Geolocational data in particular has come to be associated with technologically-enhanced methods of ascertaining physical placement (e.g., radar, GPS devices in automobiles or mobile phones, or internet connections). This category also incorporates the more traditional mode of ascertaining individuals' locations—i.e., the simple observation of individuals in public space.[3]

The fifth category, content, is perhaps the most traditional category in its close association with both the First and Fourth Amendments. Technology, however, has expanded the range of materials that may provide content—a category that includes the *substance* of communications, writings, and other materials. As a form of communication, content conveys information through the exchange of ideas, thoughts, or other information, such as through speech, writing, or symbolic representations. It incorporates media as well, such as pictures, videos, auditory files, and writing. It thus relates to the nature of individual experience.

Each of these categories has privacy interests associated with it that are particular to that type of information. This suggests that consideration of each category, *sui generis*, may be necessary to construct the most appropriate structures to protect such privacy interests. An added layer of complexity here is that the manner in which such information presents in each category—i.e., the way it is accessed, transmitted, or stored—differs.

b. Method of Access, Transmission, and Storage

Each of the forms of information (personal, transactional, relational, locational, and content) may be accessed, transmitted, and stored in different ways. Some of these may be non-digital, such as simply observing another's actions or reading a hand-written letter. Others, such as accessing information held on a server, may be technology-dependent. Simply extending the existing rules from hard copy to hard drives, though, misses the enhanced privacy implications of greater amounts of information and advanced

[2] For further discussion *see* S. WASSERMAN AND K. FAUST, SOCIAL NETWORK ANALYSIS (1994).

[3] Efforts to address the collection of this information have been introduced into Congress, but no laws have yet been passed. *See, e.g.,* Geolocational Privacy and Surveillance Act, S. 639, Mar. 21, 2013 and H.R. 1312, as well as the Geolocation Privacy and Surveillance Act, June 2011 (co-sponsored by Sen. Ron Wyden and Rep. Jason Chaffetz). Online Communications and Geolocation Protection Act, Mar. 6, 2013, introduced by Reps Zoe Lofgren (D-CA), Ted Poe (R-TX), and Suzan DelBene (D-WA), H.R. 983. Location Privacy Protection Act of 2012, Introduced by Sen. Al Franken (D-MN); passed Senate Judiciary Cte in Dec. 2012. S. 1223.

back-end analysis.[4] Six categories here deserve notice: audio/visual (AV) observation; communications networks; papers; hard drives (HD) and device-specific storage; remote server/cloud technologies; and social media. (See *Fig. 2*)

The first category, A/V observation, is one of the most traditional ways in which information is accessed. Under this approach, information is obtained by observing a particular target or entity's actions. Traditional modes of information collection in this area still exist—this is the realm of placing a tail on a suspect in the law enforcement world, or of HUMINT in the intelligence community. The key point here is that technology has expanded the ways in which one may be able to observe such actions. Electronic bugs represented one of the early expansions. Placed in an individual's office or home, such devices allow investigators or analysts to hear conversations that are occurring within, thus giving them access to the content of communications. *Katz* dealt with such an "amplifying device," attached to the outside of a phone booth. The Court recognized at the time that new technologies applied to traditional areas could have a deeper impact on the right to privacy.

Other types of technologies are similarly relevant to enhanced A/V observation, and they cross informational categories. CCTV, for instance, may allow for remote surveillance even where the information obtained is not recorded. This extends beyond content information to include locational data: individuals may be followed in public space via traffic cameras, surveillance equipment on drones, satellite cameras, or other technologies. Such tracking may similarly reveal meetings, actions in the workplace, and social interactions—all forms of relational information. Observations of commercial exchanges, such as individuals shopping or withdrawing money from the ATM, represent transactional information. And in the realm of personal information, A/V observation may track individuals by appearance (e.g., using facial recognition), or by license plate [e.g., via automatic license-plate recognition (ALPR) or car plate recognition (CPR) systems]. Such tracking through public space may identify individuals' habits, their home address, their movements, and common patterns in which they engage.[5]

The second category, communications networks, incorporates wire, cable, and satellite communication systems. This is the realm of electronic surveillance—which was one of the central areas addressed by FISA in 1978. The purpose was to provide a heightened level of protection for the content of individuals' communications. But technology has progressed significantly beyond the telephone and wire communications originally considered. Communications networks may be accessed via telephones, computers, or other devices that link up to the Internet. Content information may be conveyed through telephone conversations, Face Time, texts, emails, or voice over Internet protocol (VOIP).

Much more than content information is now involved in information carried through communications networks. Locational data, such as GPS transmissions, may be transferred. Relational data based on telephone and Internet content may yield insight into social networks. Transactional information also may be conducted via automated telephone systems: post-cut-through dialed digits (PCTDD) (numbers dialed on a phone once a call has been put through) allow customers to buy airline tickets, transfer money between accounts, and sell stock. In the criminal law realm, efforts have been made to apply PRTT to this area. The problem is that PCTDD also reveals content—suggesting a deeper privacy interest than

[4] For purposes of this discussion, I understand data in a manner consistent with the Data Protection Act, that is, information which: "(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or (e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d)."

[5] *See* Laura K. Donohue, *Remote Biometric Identification*, MINNESOTA L. REV., 2012.

mere envelope information.[6] To the extent that automated systems reveal personal data, such as social security numbers (SSN), credit card or bank account numbers, address information, and passwords (such as mother's maiden name, place of birth, name of first pet), personal information is similarly implicated.

Neither of the first two categories (A/V observation and communications networks) records what has historically been considered content. Instead, they record process and movement. Individual A goes to Place 1, then Place 2, and then Place 3. Or number X dials number Y. Or person A uses Credit Card Z. The recording of process and movement itself is what generates information.

Critics of the Section 215 bulk collection program point to the generation of information premised on structural connections, and the ability of the government to amass this information in large quantities, at reduced cost, and over extensive periods, to note the significant privacy implication. It may also be prospective, which shifts the question from how to access stored information or already-existing data, to how to control access to information generated in this manner in the future.

The third category, papers, is the one most closely associated with Fourth Amendment jurisprudence—not least because of the wording of the provision itself.[7] Content information located in papers has thus traditionally been afforded the highest level of protection. Since obtaining one's letters, books, and writings, has generally required entry into one's domicile, a warrant, or something approaching a warrant in the realm of foreign intelligence, has typically been required. FISA, accordingly, includes within its auspices special provisions for physical search that, along with electronic communications (also content-based), are afforded the highest level of protection.

Lines between categories may, of course, be somewhat permeable. The substance of one's papers may demonstrate an individual's location at a particular time, such as via receipts. Relational information may be ascertained from correspondence, and transactional information from financial records. Simultaneously, papers may provide personal information, such as one's health/medical, or educational records.

Notably, scientific advances have deepened the type of information that may be found in one's personal papers. DNA technologies, for instance, may reveal a host of information about individuals that was not previously knowable. But minimization procedures have failed to account for the qualitative differences in types of personal information obtained. Instead, they are rather crudely based on merely whether an individual is a U.S. person or a non-U.S. person.

The digitization of this information has not lessened the privacy interests involved. If anything, its presentation in an analyzable format has deepened the privacy implications. Simultaneously, the increased volume of information means that much more about an individual and his or her movements can be ascertained. Whereas before an individual's prior location could be determined by a receipt, mobile devices now include maps that can be queried for directions and that archive all of the places one has travelled. Pictures taken on an iPhone may include embedded data with the precise location at which the image was snapped. To the extent that mobile devices reflect their owner's actions (and not those of others who use or borrow the device), they create a digital map of an individual's movements. Yet the statute has failed to acknowledge this equal, or deeper, privacy intrusion.

As a result, in the fourth category, hard drives and electronic devices, we find varied application of the existing rules. This category encompasses information held in electronic format on individual electronic

---

[6] In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information, 515 F.Supp. 2d 325 (E.D.N.Y. 2007).

[7] To wit, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures..." U.S. CONST., 4th Amend.

devices, as well as other forms of local storage, such as memory sticks and stand-alone external hard drives. Content may take a number of forms—e.g., documents, spreadsheets, audio/visual files, and new code.[8]

Recent court decisions suggest that there is confusion about what level of protection to give to electronic devices in the face of steadily expanding government capabilities. Confronted by requests by the FBI to place malware on a suspect's computer and to access a wide range of information held by the device in the course of an investigation, for instance, district court judges have come out on different sides of the issue.[9] Network investigative techniques (NIT) allow the FBI to covertly download files, photographs, and stored emails, or even to activate cameras located on computers, allowing the government to obtain real-time images.[10] The privacy interests involved in NIT are substantial. As the Ninth Circuit sitting en banc recognized in *U.S. v. Cotterman* in the context of a border search of a laptop:

> The amount of private information carried by international travelers was traditionally circumscribed by the size of the traveler's luggage or automobile. That is no longer the case. Electronic devices are capable of storing warehouses full of information. The average 400-gigabyte laptop hard drive can store over 200 million pages—the equivalent of five floors of a typical academic library. . . . Even a car full of packed suitcases with sensitive documents cannot hold a candle to the sheer, and ever-increasing, capacity of digital storage.[11]

Pari passu, the amount of information that can be obtained from any individual's laptop carried within domestic bounds is staggering. Recent media reports suggest that the NSA has inserted malware into computer networks, as well as, like the FBI, into individual computers, to collect information.[12] Simultaneously, the agency has compromised encryption technologies by arranging for secret "back doors" to be built into software, by making secret agreements with private companies, and by using supercomputers to overcome barriers using brute force.[13] The location of the devices in question, which is one of the traditional ways to think about procuring foreign intelligence, seems to be a minor matter, when compared to the privacy implications of access to such broad swathes of data.

The fifth category, centered on server and cloud technologies, recognizes that the same type of information that may be held on individual devices may be stored on a remote server, such as IBM Cloud, iCloud, Kindle Cloud, or Amazon Cloud. Some companies, such as Dropbox, ZipCloud, SugarSync, and Google Gdrive, offer the ability to store all data remotely, so that the information can be shared and accessed at any time. Other companies, such as Livedrive, Mozy, and BackupGenie, operate primarily as

---

[8] Early reports about law enforcement use of malware emerged in 2001 with discussion of Magic Lantern, MSNBC. The programs have since become increasingly sophisticated.

[9] *Compare* Third Amended Search and Seizure Warrant, US District court for the District of Colorado, Case No. 12-sw-05685-KMT, Dec. 11, 2012; and In Re Warrant to Search a Target Computer at Premises Unknown, Memorandum and Order, United States District Court Southern District of Texas, Houston Division, Case 4:13-mj-00234, Apr. 22, 2013.

[10] Craig Timberg and Ellen Nakashima, FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance, Wash. Post, Dec. 6, 2013, available at http://www.washingtonpost.com/business/technology/fbis-search-for-mo-suspect-in-bomb-threats-highlights-use-of-malware-for-surveillance/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html.

[11] U.S. v. Cotterman, 4:07-cr-01207, En banc, Mar. 8, 2013, pp. 20-21.

[12] *See, e.g.,* Violet Blue, NSA malware infected over 50,000 computer networks worldwide, ZD Net, Nov. 23, 2013, available at http://www.zdnet.com/nsa-malware-infected-over-50000-computer-networks-worldwide-7000023537/; Andrea Peterson, The NSA has its own team of elite hackers, Wash. Post, Aug. 29, 2013, available at http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/; Floor Boon, Steven Derix, and Huib Modderkolk, NSA infected 50,000 computer networks with malicious software, nrc.nl, Nov. 23, 2013, available at http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/; Raphael Satter, Associated Press, Report: NSA intercepts computer deliveries, USA Today, Dec. 29, 2013, available at http://www.usatoday.com/story/news/world/2013/12/29/report-nsa-intercepts-computer-deliveries/4244181/.

[13] James Ball, Julian Borger, and Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security*, THE GUARDIAN, Sept. 5, 2013, available at http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Jeff Larson, Pro Publica, Nicole Perlroth, The New York Times, and Scott Shane, The New York Times, Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security, Pro Publica, Sept. 5, 2013, available at http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

an online backup to individual devices. Yet others, such as MyPCBackup and JustCloud offer both services.

The cloud, though, does more than just offer ways to store information. Cloud computing uses a network of remote servers hosted on the Internet to manage and process data, extending these functions beyond individual hard drives or personal devices. Because of the sophistication of analytical techniques, the amount of storage available, and the potential multi-sourcing of data involved, cloud computing changes what individuals and companies can actually do. It provides an opportunity for users to increase their capacity and to add capabilities without extensive, new investments in infrastructure, software, and personnel. And the market is exploding. As of July 2013, for instance, approximately 30 public companies represented more than $100 billion in market capitalization and $12.5 billion in estimated 2013 revenue.[14]

The same techniques that may be used to exploit hard drives and individual, stand-alone electronic devices may be employed to obtain content, as well as locational, relational, transactional, and personal information, from remote servers. The amount of information available—and insight into—the thoughts and actions of the target may be significantly enhanced—not least because more information can be uploaded and more powerful analytical software may be marshaled in relation to the cloud. In addition, there are some functions, such as online gaming, that are unique to the world of servers in that they take place (in part) on servers located outside the immediate electronic device. Efforts to communicate with others inside the gaming world may be subject to interception with (under traditional foreign intelligence provisions) little or no structure, oversight, or control. Yet this, too, is a form of access to the content of one's communications—an area traditionally afforded the highest, not the lowest, level of protection to ensure that foreign intelligence gathering comports with the Fourth Amendment.

The sixth category, social media, is a form of electronic communication where users can create virtual communities to share information, ideas, personal messages, photographs, videos, and other data. Web sites like Facebook, Twitter, Google+, Instagram, and Snapchat have become a critical form of networking and microblogging. They cross different types of information categories, simultaneously generating content, locational information, and relational information. The companies hosting the sites, in turn, maintain billing records, metadata, and other forms of transactional information, even as they have access to a host of personally-identifiable information about their account holders.

Each of these six categories, as it intersects with the five types of information, present opportunities for agencies looking to learn information about potential targets. Yet not all information is equal: the substance and techniques employed may yield different levels of value as well as different levels of insight into individuals' private actions, thoughts, and beliefs. At one extreme, programs that fail to provide meaningful intelligence in the manner anticipated may be voluntarily ended by the IC. According to James Clapper, for instance, "[i]n December 2011, the Government decided not to seek reauthorization of the bulk collection of Internet metadata."[15] ODNI explained, "[T]he program was no longer meeting the operational expectations that NSA had for it."[16]

Reliance, however, on the value of a program to the intelligence agency involved for whether it will or will not operate would be misplaced. Individuals who have insight into the program's extent may

---

[14] The top 15 cloud computing companies include Jife Software, Demandware, Fleetmatics, RealPage, Dealertrack Technologies, Cornerstone OnDemand, Medidata Solutions, The Ultimate Software Group, Athenahealth, Concur Technologies, ServiceNow, NetSuite, Workday, LinkedIn, and Salesforce.com.

[15] Press Release, *DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly after the Attacks of September 11, 2011*, Dec. 21, 2013, available at http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the.

[16] Additional Information on the Discontinued PR/TT Program, Dec. 21, 2013, available at http://icontherecord.tumblr.com/tagged/declassified.

disagree about its worth. The bulk collection of telephony metadata, for example, has been challenged by individuals on the Senate Intelligence Committee, who have substantial access to the inner workings of the program, on the grounds that it does not yield significant benefits.[17] But not all members of the committee—much less officials in the agencies themselves—agree with that position.[18]

Regardless of how useful a program may be, underlying social, political, and constitutional concerns remain. To the extent that the different categories of information and related access, transmission, and storage yield differing levels of confidential information, different privacy interests come into play. Traditional models, based on, for instance, geography (i.e., whether the object, device, or target is located within US bounds or outside the country), rather miss the point. It is thus crucial to build an expanded understanding of the types of information in question into the statutory framework.

c. Technology Shifts in the Context of the Taxonomy

A short discussion will help to illustrate how using these demarcations would significantly depart from the current orientation of FISA, which relies on the target and the location of the information, and help to construct a new approach to foreign intelligence.

Consider first the type of information. It may be that personal and/or transactional information (e.g., the association of particular credit card numbers or billing records in relation to specific individuals) should be considered in a category apart from relational information, which in turn could be distinguished from locational or content-based information. In other words, the associated structures may depend upon the type of information being sought. The number and types of entities from whom personal and/or transactional information may be obtained, the process for obtaining the information, what information may be retained, the manner and length of time of retention, and the use of such provisions would then revolve around the information itself, thus allowing the provisions to be tailored to the specific privacy interest involved.

This approach allows more careful consideration of the information categories themselves. For relational information, for instance, in addition to the threshold issue, perhaps the most important question is how to treat different levels of social connectedness—e.g., it may be a lesser privacy intrusion to obtain information *that* an individual is a member of an organization, than to look at relationships within organizations to consider the role one plays within the entity. Similarly, it may be that there are greater (or fewer) privacy interests in building social networks of geographic regions versus looking at individuals with similar political, economic, or religious subject-matter-interests. The mere observation of individuals' involvement, moreover, may be less intrusive than the digitization of such information and the combination of such data with other information—suggesting heightened privacy protections as one moves outward along the digitization axis (see *Fig. 2*).

To the extent that locational information reveals substantive data, perhaps it should be placed within a framework similar to content-based approaches. Again, the outward movement along the digitization axis may trigger further protections as the data changes form or is incorporated into recombinant systems (i.e., systems that combine data with other information that allows the user a greater level of insight into individuals' private lives).

---

[17] Senator Ron Wyden (D-OR), Senator Mark Udall (D-Co), for instance, both of whom sit on the U.S. Senate Intelligence Committee, filed an amicus brief in November 2013 in First Unitarian Church v. NSA, asserting that they had "reviewed this surveillance extensively and have seen no evidence that the bulk collection of Americans' phone records has provided any intelligence of value that could not have been gathered through less intrusive means."

[18] *See, e.g.,* Dianne Feinstein, *The NSA's Watchfulness Protects America*, WALL STREET J., Oct. 13, 2013, available at http://online.wsj.com/news/articles/SB10001424052702304520704579125950862794052.

d. Remaining Demarcations in the Manner of Collection

Beyond the first two categories, the manner of collection may be constructed with reference to five areas. First, the form in which information is transferred, may be considered as part of the front-end collection. The data, for instance, may be anonymized before it is provided to the government agency, with only certain data points meeting a pre-set selection criteria then subjected to re-identification.[19] Alternatively, a third party data-holder may pre-screen the results of any searches. Thus, for instance, if a search returns 400 numbers, those relating to non-concerning entities could be screened out.

Second, contours may be built around access to information based on the agency obtaining the information. This, in turn, has three components: (a) broad institutional design [e.g., deciding to separate NSA/Cybercom or requiring civilian personnel to head particular agencies); (b) primary authorization [e.g., authorizing the FBI but preventing the CIA (as in Exec. Order 12333) from engaging in certain activities], and (c) concurrences required (e.g., requiring the Attorney General or the Assistant Attorney General of the National Security Division to sign off on applications to obtain information).

The third consideration is the target about whom information is sought. Traditionally, FISA has focused on U.S. versus non-U.S. persons, presenting higher barriers to collection of information on the former, versus the latter. It has overlaid this with two additional categories—namely, whether individuals are foreign powers or agents thereof, or involved in international terrorism. These categories are decidedly individual, requiring a nexus between the target of the information and the category. Discussion thus may turn on the level of suspicion required to collect information related to a target, for instance requiring a statement of facts supporting reasonable, articulable suspicion. (Note that one would then expect parity between this an the scope of approval, addressed, below).

A fourth associated area may be the source of the information itself. FISA has only tangentially considered this in relation to business records and, subsequently, tangible goods. But there are numerous sources that could be considered. Private industry may generate and/or store information. Different approaches that could be taken here include possibly introducing data retention requirements, which gives rise to considerations of cost. Data security prior to government access could be statutorily addressed. Attention also could be drawn to voluntary versus compulsory compliance and associated risks of litigation borne by the companies. Alternatively, reform efforts may want to focus on constructing new, third-party data holders, which may be linked in some way either to government or to industry—or to neither. Under this approach, further thought may be given to dividing information between entities for additional protection of data. In this case, the security of the data would also be relevant, as would the potential for introducing yet another third party in the form of encryption key holders—the purpose of which is to divide the process via which the information is accessed.[20] Encryption key holders may also be built into the independent entity holding the data, much like an IG office is part of the institutional framework of a government entity.

Information may also be obtained from other government agencies, in which case interim MOUs, standards, and procedures will have to be taken into consideration. Or it may be derived from non-governmental entities. If obtained from international partners, further verification of the information may be required. If this is the favored approach, the type of framing used alters. For example, lower levels of reliance may be assumed when information comes from foreign entities, in relation to which the U.S. has limited control, suggesting greater minimization procedures until information is verified. Alternatively, to protect other agencies' missions, it may suggest limiting intra-governmental transfer of information.

---

[19] *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV., 1701 (2010).

[20] *But see* Scott D. Sagan, *The Problem of the Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security*, RISK ANALYSIS, Vol. 24, No. 4, 2004.

Or, in the interests of privacy, it may mean creating higher barriers to obtaining information from a target's employer, requiring a higher showing before a neutral arbiter before obtaining certain records.

The fifth additional area associated with the manner of collection is location. Traditionally, FISA has considered international versus domestic. But the possibility of having a mixed category (e.g., where information flows across borders), or one focused on the border itself may sharpen the analysis.

2. Requirements for Approval

Having considered the manner of collection, attention then turns to checks on these authorities in the form of what is required for approval for the collection of the information—essentially, the process that must be followed in order for the collection to commence. Here, there are four principal considerations: the entity(ies) approving the collection, how that entity is constructed, what the scope of the approval is, and emergency exceptions. Underlying this demarcation is the deep time-honored understanding that having a neutral arbiter provides an important check on the exercise of authority.

The entity approving collection may be one of three types. Within the executive branch, it may be internal or external to the intelligence agency that has been authorized to collect the data. In the judicial realm, there are three types of arbiters that may be constructed: a special court (like FISC), an ordinary Article III court, or an Article I court. There may, in addition, be a way to construct a board or independent arbiter from other sources, such as private industry or quasi-governmental organizations.

The construction of the entity itself also offers numerous options. The manner in which decision makers are selected may include requirements with regard to the originating entity (for instance requiring a division among certain circuits, regions, or types of industry), as well as the manner of selection (e.g., by the President with the advice and consent of the Senate, by the Chief Justice of the Supreme Court, by members of the Supreme Court, by the Appellate Courts, or by Congress). The length of the terms, or their progression (e.g., the period of years, staggered terms, and term limits) may also be considered. Adversarial processes, in turn, may involve rights of challenge to the orders, rights of appeal, third party rights, or the creation of a constitutional advocate, while technological expertise similarly may be built into the statutory design.

The scope of approval contributes further to the potential requirements that must be met prior to acquisition of information. This category highlights the form that the application or request must take, standards that the entity must follow in approving or disapproving of the applications, the duration for which applications may be granted, and the contours of any requirements for renewal.

Although not currently required under the statute, depending upon the final form of data storage and access, it may be desirable to include an additional verification stage—i.e., requirements that must be met by certain actors in verifying that the requesting agency has gone through the appropriate steps. These may apply to third party data holders, such as telecommunications companies, or independent entities established for the purpose of holding the data for intelligence purposes. It may be equally relevant for encryption key holders, prior to allowing access to the information.

A final area to highlight relates to emergency exceptions that could be constructed to take account of national security crises. Three principal areas (substantive requirements, the timeline for subsequent approval, and the subsequent use of information obtained during the exercise of the emergency provisions) provide the focus. Taken together, these various approaches suggest a more comprehensive view of ways to provide access to new types of information.

B. Back-End Framework to Analyze and Use Foreign Intelligence Information

Like front-end considerations, a range of categories could be used to explore the construction of a back-end framework centered on implementation of the authorities thereby granted. This framework also divides into two parts, reflective of the positive grant of authority and subsequent checks on the same powers, even as considerations within each category may consider both aspects as well. These realms relate to implementation, on the one hand, and transparency and oversight, on the other. (See *Fig. 3*)

BACK-END FRAMEWORK TO ANALYZE AND USE FOREIGN INTELLIGENCE INFORMATION

Implementation	Transparency and Oversight
1. **Analysis** a. Raw data - type of analysis (e.g., data mining, social network analyses) - levels of analysis (e.g., primary, secondary, tertiary) - requisite standards and processes to be followed b. Recombinant information - substantive (e.g., biometric v. biographic) - programmatic (e.g., Sec. 215/Sec. 702) - source (e.g., intra-agency and inter-agency; government and private databases) c. Verification 2. **Use** a. Minimization b. Judicial processes (e.g., prosecution, use of information as evidence in trial, etc.) c. Consequential actions (e.g., further targeting, watch listing, etc.) 3. **Retention** a. Length of time b. Who holds the information (e.g., NSA, FBI, DNI, CIA) c. How is the information held (e.g., digital v. hard copy, combined with PII or other data v. isolated) d. Access (e.g., which individuals within agency, which agencies, under what conditions) 4. **Transfer** a. To whom b. Restrictions on use, access, and sharing c. Verification	1. **Who reports** a. Agency executing foreign intelligence authorities b. IC entity's Inspector General - Administrative (e.g., NSA, NGA, NRO IGs) - Statutory (e.g., CIA IG, DOJ IG) c. IC entity's privacy officer d. Concurrence entity (e.g., NSD) e. Approval entity (e.g., FISC) f. External Agencies (e.g., ODNI, OMB) g. Entities providing the information to the IC (e.g., private sector, NGOs) h. Independent oversight body (e.g., PCLOB) 2. **What is reported** a. Execution of authorities (e.g., #/range of orders, programs, benefits/rates of success) b. Application under the law (e.g., novel or significant legal interpretations, application to new technologies) c. Noncompliance (willful and non-willful) d. Non-standard (specifically requested) information 3. **To whom report** a. Head of agency executing foreign intelligence authorities b. IC entity's IG or privacy officer c. Concurrence entity d. Approval entity e. External agencies f. Independent bodies (e.g., PCLOB) g. Congressional committees h. Public 4. **Penalties for violations** a. Administrative (e.g., reprimand, loss of security clearance, suspension, termination) b. Civil (e.g., fines) c. Criminal (e.g., prison) 5. **Alternative reporting channels** a. fraud, waste, abuse (programmatic) - path (agency, supervisor, ODNI, Congress) - protections against recrimination b. Public interest (systemic) - external body - criminal defense (*ex post* v. *ex ante*)

Fig. 3

1. Implementation

Implementation centers on how the authorities granted to the intelligence community are actually used. There are four categories to consider: analysis, use, retention, and transfer. Traditionally, emphasis has only been placed on the second and third areas and, even within these, on only a few components (e.g., minimization procedures and the length of time data is retained). The taxonomy thus allows more careful scrutiny of different aspects of the implementation phase and expands the ways in which Congress could approach each area.

Under analysis, for instance, a framework could focus on how raw data is treated. Focus on the type of analysis, such as what sorts of data mining or social network analyses can be performed can here be considered, as well as levels of analysis (e.g., primary, secondary, and tertiary "hops"). Attention may be drawn to the requisite standards and processes to be adopted prior to progressing from one stage (i.e., hop) to the next stage (i.e., hop).

Consideration could also focus on what I consider to be "recombinant information"—namely, the combining of information from different sources in a way that generates new knowledge. Attention can be paid to combining substantively distinct information, such as biometric and biographic data. It may center on programmatic combinations. For instance, agencies may want to combine information from different programs run under the same legal authorities (e.g., Section 215), or from programs run under different legal authorities (e.g., Section 215 and Section 702). Alternatively, agencies may want to combine databases held in different areas of the agency with databases held outside the agency, or government databases with publicly-available databases. Another consideration in looking at the analysis of the data centers on information verification. This becomes particularly important when subsequent intrusions into civil liberties and individual privacy may flow from the initial analyses. This type of an approach would help to bring to the surface new and emerging ways in which data analysis is progressing.

The use of such information also presents an opportunity for statutory construction. Minimization procedures have historically been considered and still offer an opportunity for further inspection. But prosecution limits, the use of such evidence in trial, and other judicial process-related concerns may be taken on board, as well as the extent to which consequences that follow from initial analyses, such as further targeting or watch listing, occur.

Retention has historically been limited to considerations about time, but there are other questions that could also be statutorily addressed. Once *obtained* (and not just at the outset), who should hold the information? Should it be held by the NSA? The FBI? The CIA? Different government entities have different missions, and so the placement of the data may be of consequence. Beyond the entity responsible for the data, how is the information being held? It may be in digital form or hard copy. It may be combined with other data or personal identifiers, or it may be isolated. Additionally, access may be considered—not just who has access within the intelligence agency in question (e.g., on a need to know basis, by level of clearance, or by programmatic assignment), but which other agencies have access to the information as well.

The final consideration relates to transferring the data. This incorporates the recipient of the information, further restrictions on use, access, and sharing, and ways in which the information may be verified in the future.

2. Transparency and Reporting

The flip side of the design for implementing the authorities granted to the intelligence community is considering how such use is to be monitored. As with requirements for approval at the front end, this area acts as a counterpoise, balancing the power to collect foreign intelligence with protections to prevent

improper use of the same. It sub-divides into five primary considerations: who reports, what is reported, to whom the report is made, penalties for violations, and alternative reporting channels.

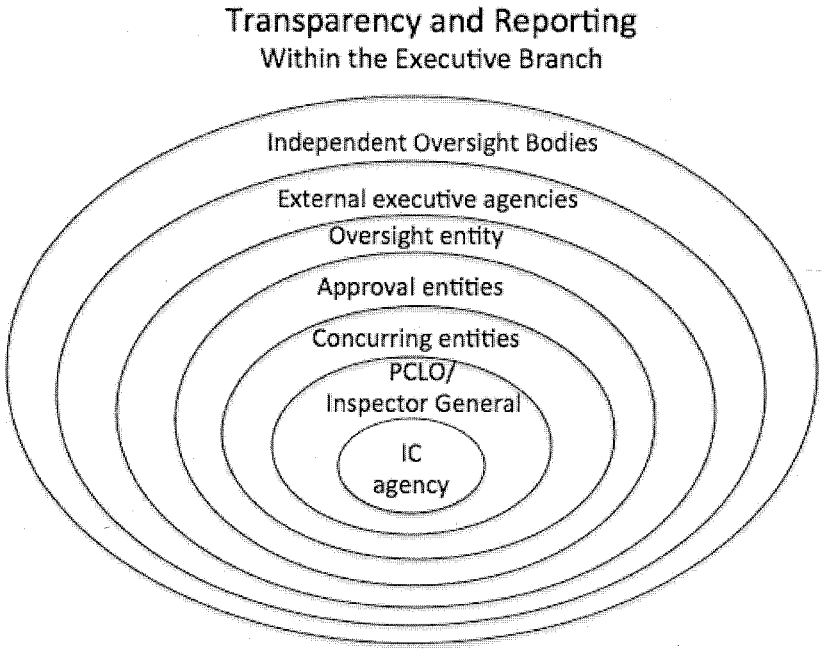

Fig. 4

The first area, who reports, incorporates entities internal and external to the entity exercising the authorities. A good way to think about this area is in terms of concentric circles. (See *Fig. 4*) In the core, the specific agency engaged in foreign intelligence collection may be required to report. One level out, the IC entity's inspector general may be brought on board. Of relevance is the underlying structure of this position—i.e., either administrative (e.g., the current IGs of the NSA, NGIA, and NRO), or statutorily required (e.g., the current IGs of the CIA and DOJ). Additional consideration can be given to reporting requirements to the IC entity's privacy officer. The next ring includes any entities required for concurrence at the front-end application or initiation, such as DOJ's National Security Division. The adjoining circle incorporates any entity required for approval of the intelligence gathering. This may be FISC, or some other entity created for the purpose of addressing the counterpoise to the front-end considerations. The following band includes external agencies, which perform oversight within the executive branch, such as ODNI, or OMB. The abutting loop focuses on entities that provide information to the IC—such as the private sector or NGOs. On the outermost ring we then find independent oversight bodies, such as the Privacy and Civil Liberties Oversight Board (PCLOB).

The question of who reports folds then into the second area, which is what is reported. Entities may be required to report on the execution of authorities (e.g., the number and range of orders, programs underway, and benefits or rates of success). They may address how the programs have been applied under the law, detailing novel or significant legal interpretations, or the extension of prior legal analysis to new technologies. Noncompliance requirements (either willful or non-willful) are included here. Finally, of importance will be the manner in which non-standard (specifically requested) information will be handled.

Having looked at who reports and what is reported, the third area to consider is to whom such information is made available. For logical reasons, the potential list of recipients is to some measure co-extent with the entities considered for who makes the report (to ensure access to information necessary for them to

fulfill their statutory duties). But there are some differences. Thus, reports may be required under certain circumstances to (a) the head of the agency executing the foreign intelligence authorities, (b) the entity's inspector general or privacy officer, (c) the concurring entity, (d) the approval entity, (e) other executive branch agencies, or (f) independent bodies. In addition, (g) Congress, and (h) the public may also be considered for receiving reports from the various reporting bodies. While the latter reports would necessarily be unclassified, the reports to the preceding areas [(a)-(g)] may be either classified or unclassified.

Crossing the first three categories are questions related to the burden such reporting may place on the agencies involved, in terms of time, personnel, and money. Special appropriations may be made, for instance, to account for the need to develop new technologies to allow for auditing programs, or to hire additional analysts to act in an internal capacity. Alternatively, consideration of reporting requirements as a whole may help to streamline the overall process.

The fourth consideration in transparency and oversight focuses on what to do about misuse of authorities. Penalties for violations may include administrative measures, such as reprimands, loss of security clearances, suspension, or termination. Civil remedies such as fines may be created, or criminal measures may be attached.

The fifth and final consideration focuses on what to do when the regular reporting channels are not working. How should one conceive of alternative reporting channels? There appear to be two divisions. The first, relating to fraud, waste, and abuse, tends to be programmatic in that it focuses on specific programs in place. Questions to address include (a) the path that individuals concerned about fraud, waste, and abuse should follow (e.g., within the agency, relating to supervisors, going to ODNI, or approaching congress), as well as (b) protections against recrimination. The second division emphasizes public interest—representing a systemic (not a programmatic) concern about the exercise of foreign intelligence gathering authorities. Here, attention may be paid to the role of external bodies as well as potential criminal defenses available in the event that the matter goes to trial (*ex post* v. *ex ante* considerations).

C. Concluding Remarks

While the above taxonomy does not represent a radical re-conception of intelligence collection, it does expand the scope of the current reform efforts to include the range of potential areas that could be brought on board. In doing so, it builds on our experience over the past 36 years even as it recognizes changed circumstances. Although it takes no normative position on the specific reforms to be given effect, it clarifies areas critical for discussion and, in so doing, their complex relationship with other elements in the framework.

The hope is that the taxonomy may thus serve as a way to move the conversation forward in developing an approach to foreign intelligence gathering that is cognizant of the need to obtain foreign intelligence even as it recognizes the changing privacy interests implicated by new and emerging technologies.

Thank you for your time. I look forward to discussing the specific issues related to Section 702 in more depth.

Yours sincerely,

Laura K. Donohue

Laura K. Donohue
Professor of Law