THE INTERSECTION OF WHITE COLLAR CRIMINAL PROSECUTIONS AND NATIONAL COUNTERINTELLIGENCE: A NEW LEGAL CHALLENGE

I. THE PROBLEM

a. The NSA (or National Security Agency) engages in extensive electronic surveillance, collection and retention of many millions of electronic communications, including that of Americans. The purpose is counterintelligence to ensure national security against foreign powers and their agents here.

b. But the principle federal law enforcement agency – the FBI – has broad access to such communications, and they are free to use that information for purposes of enforcing domestic federal crimes. They are doing so with increased frequency.

c. Foreign nationals or foreign companies doing business here are particularly at risk of such prosecutions because of counterintelligence activity aimed at the governmental strategies of their home nations. China and Iran in particular are a focus.

d. Any defendant charged with a federal crime based on information learned from the counterintelligence intercepts will confront a black box. S/he will not be able to discover what communications were intercepted, why or how. S/he will have virtually no ability to challenge the interception in defense.

e. Civil rights and privacy interests are implicated by this trend, especially for Chinese Americans and Chinese nationals who all too often have been targeted for misguided prosecutions. More broadly, the trend has implications for the ability of defense counsel to mount an adequate defense. On the other side, FBI agents and prosecutors face unique challenges of respecting the fine line between their discovery obligations and national security secrecy requirements.

II. “BIG BROTHER” IN A WORLD FRAUGHT WITH DANGER?

a. FBI Director Christopher Wray recently made a speech to the American College of Trial Lawyers describing the FBI’s priorities. (Tab 1)

   i. “National security remains our top priority as it has to be, and counterterrorism is still a paramount concern.”
“On the counterintelligence front, we still face traditional espionage – spies seeking our state secrets, working under diplomatic cover, or posing as every day citizens. Think of dead drops and tunnels, clandestine meetings in cafes, the kind of stuff you would see in a John le Carré novel. Today’s spies also seek our trade secrets, our economic ideas or innovation. They are often businessmen, researchers, scientists or students acting on behalf of state governments. Nation states like China are attempting to infiltrate our companies, your clients, by any means necessary to get control of cutting edge technology. Not just by stealing propriety information, but also by extra-legal means, like acquiring the company, or exploiting business partnerships.”

 “[We have] dramatically stronger integration of intelligence, and our continued need to focus on it, in everything that we do. Under Director Mueller’s leadership in the aftermath of 9/11, the FBI made a paradigm shift from a law enforcement agency that investigated crime after the fact to a national security service, working to prevent crime and terrorism. . . . we have developed a sophisticated and complex intelligence program.”

“We talk a lot about the term ‘intelligence’ in a national security world, but what it really boils down to is information. Information that we use to make decisions and to drive operations.”

b. The principle information-gathering technique for counterintelligence is through FISA. What is FISA and how does it work?

i. Foreign Intelligence Surveillance Act of 1978. (Excerpts in Tab 2)

ii. FISA section 702 permits the Attorney General and Director of National Intelligence to authorize the targeting of persons reasonably believed to be outside the United States to acquire foreign intelligence information.

iii. FISA, established the Foreign Intelligence Surveillance Court (FISC), which reviews and (largely) approves the government’s ex parte applications to conduct electronic surveillance and physical search for foreign intelligence purposes.

iv. FISA was reauthorized in early 2018 and amended.
v. Virtually all FISA applications are approved by the FISA court, and the court approves more than a thousand such applications each year.

1. DOJ annually submits to Congress bare statistical data about FISA applications. (See example at Tab 3)
   a. In 2017, gov’t filed 1,321 final applications to FISC (FISA Court) seeking authority to conduct electronic surveillance. FISC did not deny any of them. DOJ Report at 1 -2.
   b. In 2017, somewhere between 1000 and 1499 persons were targeted for electronic surveillance somewhere between 0 and 499 of them were United States’ citizens. DOJ Report at 2.

2. As Americans (and especially American lawyers), what should we be concerned about?
   a. Elizabeth Goiten’s 2016 testimony before the U.S. Senate Committee on the Judiciary describes the dangers we face. (Tab 4)
      1. Goiten is co-director of the Liberty and National Security Program at the Brennan Center for Justice at NYU Law School.
   b. She describes some key concerns about the ways in which FISA has developed in real life.
      1. “Domestic surveillance of communications between foreign targets and Americans now takes place through massive collection programs that involve no case-by-case judicial review.”
      2. “the government may target for foreign intelligence purposes any person or group reasonably believed to be foreign and located overseas. The person or group need not pose any threat to the United States, have any information about such threats, or be suspected of any wrongdoing.”
      3. “the government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, or about the target.”
a. In theory, it could be applied even more broadly to collect any communications that even mention ISIS or a wide array of foreign leaders and public figures who are common topics of conversation.

b. It includes information “that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States.” This could encompass everyday conversations about current events.

i. [Note that while NSA halted its “about” collections in 2017, the FISA Amendment earlier this year permits the government to resume “about” collections if they recommend it, the FISA court approves, and the procedure for “about” collections will be reviewed by the congressional intelligence and judiciary committees.

ii. We should expect such “about” collections to resume.]

4. The government collected more than 250 million Internet transactions a year as of 2011.

5. According to a leaked certification, listing the foreign nations and factions about which foreign intelligence could be sought: “most of the countries in the world, ranging from U.S. allies to small countries that play little role on the world stage” were included.

6. “Section 702 establishes the boundaries of permissible surveillance, and it clearly allows collection of communications between Americans and foreigners who pose no threat to the U.S. or its interests.”

a. the FISA Court has held that the right to conduct warrantless surveillance of the foreign target entails the right to “incidentally” collect the communications of those in contact with the target.
7. **Untested by adversarial process, risk of abuse is high.** Since inception, the FISC has identified numerous instances of outright abuse by the intelligence community:

   a. “Since January 15, 2009, it has finally come to light that the FISC’s authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata.”

   b. “The Court is troubled that the government’s revelations regarding NSA’s acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.”

   c. “Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted]. . . . This overcollection . . . had occurred continuously since the initial authorization…”

   d. “The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection.”

8. **What are some consequences of this expansive collection authority?**

   a. Chilling Effect

   b. Risk of Data Theft

   c. Economic Consequences
      i. In a survey of 300 British and Canadian businesses, 25 percent of respondents indicated they were moving their data outside of the U.S.

   d. Massive quantity obscures relevant information
NAPABA Panel Presentation – November 2018
Panelists:
Christine Chung
Joon Kim
Tai H. Park
Brian A. Sun

i. Investigation of the shootings by U.S. Army Major Nidal Hasan at Fort Hood concluded that the “crushing volume” of information was one of the factors that hampered accurate analysis prior to the attack.

III. FISA USAGE FOR DOMESTIC CRIMINAL PROSECUTIONS

a. Information Sharing: the NSA may and does share raw data with the FBI and CIA.

i. All three agencies generally may keep unreviewed raw data – including data about U.S. persons – for five years after the certification expires;

ii. The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.

iii. Statute has minimization requirements “that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.”

1. Language is broad but it also has a caveat: the procedures must “allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.”

2. If the NSA discovers U.S. person data that has no foreign intelligence value and contains no evidence of a crime, the agency is supposed to purge the data.

   a. But “in practice, this requirement rarely results in actual purging of data.”

3. If any of the three agencies – all of which have access to raw data – disseminate information to other agencies, they must first obscure the identity of the U.S. person.
a. “but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person’s identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.”

b. “Back door” and “Reverse Targeting” U.S. Persons

i. Minimization procedures do not prohibit any agency from querying collected data using U.S. person identifiers, with the express goal of retrieving and analyzing Americans’ communications.

ii. The statute contains a prohibition on “reverse targeting” – i.e., targeting a foreigner overseas when the government’s intent is to target “a particular, known person reasonably believed to be in the United States.”

1. Before conducting Section 702 surveillance, the government must certify that it does not intend to target specific, known Americans.

iii. But, “immediately upon obtaining the data, all three agencies may sort through it looking for the communications of ‘particular, known’ Americans – the very people in whom the government just disclaimed any interest.”

iv. Moreover, the FBI may search the Section 702 data for Americans’ communications to use in criminal proceedings having no foreign intelligence dimensions whatsoever.

1. There are statutory and constitutional obligations to notify criminal defendants when the government intends to use evidence “obtained or derived from” Section 702 surveillance.

2. But as of the Brennan report in 2016, the government had notified only seven defendants, even though the Privacy and Civil Liberties Oversight Board (PCLOB) reports that the FBI searches Section 702 every time it conducts a national security investigation and there have been several hundred terrorism and national security convictions during this time.
3. “There is reason for concern that the government is avoiding its notification requirements by engaging in “parallel construction” – i.e., recreating the Section 702 evidence using less controversial means.”

v. We don’t know:

1. how many times the FBI uses U.S. person identifiers to query databases containing Section 702 data;

2. The list of crimes for which Section 702 data has been used to find evidence;

3. The FBI’s policies, if any, governing when evidence used in legal proceedings is considered to be “derived from” Section 702 surveillance; or

4. The length of time that the FBI may retain data that has been reviewed but whose value has not yet been determined.

IV. FAILED ESPIONAGE CASES

a. The government’s mixed results in espionage cases (that is, those that relate directly to national security) raise questions about the efficacy and reliability of national counterintelligence methods.

b. As the U.S. government targets suspected agents of the Chinese government, the record is mixed at best.

i. Some have led to successful prosecutions:

1. Greg Chung was convicted after a three-week bench trial of conspiracy to commit economic espionage, six counts of economic espionage to benefit a foreign country, one count of acting as an agent of the People’s Republic of China.

2. Chi Mak was convicted for similar conduct after a six-week jury trial.

ii. But some of the most high-profile cases have shown deep flaws in counterintelligence efforts.

c. Wen Ho Lee was perhaps the most notorious case.

i. A Taiwanese American scientist, he was indicted in 1999 for alleged theft of information relating to U.S. nuclear capabilities so that he could pass them on to the Chinese government. He was locked up in solitary confinement pending trial for many months.

ii. The government’s case deteriorated in the face of defense efforts and they dropped all but one count: mishandling of restricted data.

iii. He agreed to plead guilty to that count and was released. He received apologies from both the district court judge that jailed him and later from President Clinton.

d. Guoqing Cao and Shuyu Li, Chinese-American scientists at Eli Lilly, were arrested in October 2013 for passing alleged drug-related proprietary secrets to a Chinese drug company.

i. The defense argued throughout that the information was publicly available exploratory data.

ii. The government subsequently changed the charges to wire fraud and then dropped all charges in December 2014.

e. Xiafen “Sherry” Chen, a Chinese-American hydrologist at the National Ocean Atmospheric Administration (a federal agency), was arrested and charged with espionage in 2014 for allegedly stealing a password to download government information relating to dams. She had shared such info with an old classmate in China.

i. The charges were dropped in March 2015.
f. Xiaoxing Xi, then chair of the Temple University physics department, was arrested in May 2015 for sending plans to a device used in semiconductor research, known as a “pocket heater,” to China.

i. The plans were not of a pocket heater, and the federal investigators without the proper scientific background had confused the data.

ii. The charges were later dropped.

g. The nature and role of counterintelligence activity pursuant to FISA in these cases are not known. Given the espionage allegations at issue, and the FBI’s ready access to FISA surveillance materials in aid of a criminal prosecution, one has to presume that the government used its investigative resources under FISA to obtain communications relating to their targets before bringing charges.

i. The outcome of these prosecutions may suggest that such efforts yield unreliable data even for those offenses that directly relate to national security issues.

ii. One also questions whether such investigative materials may have yielded exculpatory information, namely, that their search resulted in no evidence of contacts with foreign governments or agents.

V. THE BLACK BOX -- CONFLICT WITH FEDERAL CRIMINAL PROCEDURE

a. The Supreme Court’s Fourth Amendment jurisprudence has long required judicial oversight of searches and wiretaps and an opportunity by the defendant to challenge violations of privacy.

i. Searches require a warrant authorized by an independent judicial officer, absent exigent circumstances.

ii. Similarly, at least since Katz v. United States, 389 U.S. 347 (1967), the government has been required to obtain a warrant to wiretap Americans’ communications.

1. The subsequent Wiretap Act provides elaborate and highly prescriptive rules about the circumstances and manner in which the government may listen in on private communications.
iii. *Franks v. Delaware*, 438 U.S. 154 (1978), provides for a mechanism by which any defendant may challenge the government’s search of his or her private property or interception of his or her private communications.

1. The defendant is entitled to question whether the government had probable cause to support the search application, as well as whether the government complied with the terms of the warrant.

iv. The government’s violation of a defendant’s Fourth Amendment rights generally requires the exclusion of evidence obtained from the unlawful search or wiretap, as well as “fruit of the poisonous tree,” that is, any evidence derived from that unlawfully acquired information.

b. But use of FISA processes enables the FBI to mine massive amounts of electronic surveillance data obtained without a warrant for use in ordinary criminal cases against Americans.

i. The FISA amendment requires that the government create query procedures that “are consistent with the Fourth Amendment.”

ii. The FISA Amendment also requires the FBI to obtain a FISC order to review certain query results in connection with a predicated criminal investigation that does not relate to national security or foreign intelligence.

iii. “Predicated” investigations are those that have passed a certain point of factfinding. Perversely, the FBI remains free to conduct warrantless searches during the earlier stages of an investigation—when there is much less evidence to justify them. The “predicated investigation” language thus makes it more likely that the bill’s warrant requirement will not apply.

iv. The government interprets the “national security” and “foreign intelligence” broadly, and under the FISA amendment, no one can challenge the government’s designation. When investigating an immigrant, for instance, a mere desire to rule out foreign ties could be cited to justify dispensing with the warrant.

v. It is too early to tell whether the FISA amendment has limited the types of cases the government will bring using FISA data, but privacy and other
advocacy groups are skeptical that the amendment will have any meaningful impact.

c. And, contrary to well-established Fourth Amendment jurisprudence, the defendant has extraordinarily limited ability to test the constitutionality of the government’s investigative activity.

d. In theory, there are statutory remedies and procedures for access to FISA and other national security protected materials. But in cases where the government does not propose to use such materials as evidence at trial, the defense almost never gets to see them.

   i. Defendants can move to suppress FISA derived information. 50 U.S.C. §§ 1806(e) and 1825(f).

      1. However, defendant will not have access to the FISA warrant or the basis for its issue as it attempts to argue that the information was unlawfully acquired or the surveillance was not made in conformity with the order authorizing it.

      2. While defendants can seek disclosure of the FISA information, 50 U.S.C. §§ 1806(g), it is rarely granted.

   ii. The Classified Information Procedures Act (“CIPA”) provides another, theoretical avenue for gaining access to classified material. (Tab 5)

      1. It was enacted in 1980 as a way to prevent “graymailing” – threats by criminal defendants to disclose classified information during trial – leaving prosecutors with the choice between exposing classified information or dismissing the indictment.

      2. CIPA contains a set of procedures by which federal district courts rule on pretrial matters concerning the discovery, admissibility and use of classified information in criminal cases.

         a. The 7th Circuit has described CIPA’s purpose as to “protect and restrict the discovery of classified information in a way that does not impair the defendant’s right to a fair trial.” United States v. Dumeisi, 424 F.3d 566 (7th Cir. 2005).
3. A criminal defendant may learn for the first time that there is classified information related to the charges against him when the government files a letter seeking an ex parte conference with the court to discuss classified information under CIPA.

4. Typically, the government files an *ex parte* motion under CIPA section 4 seeking to withhold classified information from discovery. Such motions are filed under seal.
   a. The court can review the materials to determine if they should be turned over to the defense.

5. Without the advocacy of defense counsel, the court most frequently agrees with the government that they are not relevant to the defense and grants the government motion not to disclose.
   a. CIPA Section 4 also permits a court to delete specific classified information from documents, or to substitute an unclassified summary in place of a document.

6. If the court determines that classified material should be disclosed, the defense counsel must undergo security clearance process before being given access to the materials.
   a. And even if granted, after several months of scrutiny, counsel may review the material only within the confines of a specific room designated in a federal building - the SCIF (Sensitive Compartmented Information Facility).

7. CIPA materials at trial
   a. Defense counsel must submit notice (pretrial) of each classified item it may use at trial.
   b. If the prosecution requests, the court will hold a pretrial hearing under CIPA section 6(a) determining the “use, relevance, and admissibility” of classified information in the CIPA section 5 notice.
Because each item on the section 5 notice is discussed at the hearing, the government gets insight into defense strategy and theories prior to trial.

c. If the court finds that a piece of evidence is relevant and admissible the government may move to substitute the information with a summary.

VI. THREE CASE STUDIES OF DOMESTIC PROSECUTIONS INVOLVING NO APPARENT NATIONAL SECURITY ISSUES

a. United States v. Ng Lap Seng

i. Macau-based Chinese national charged in the Southern District of New York with bribing ambassadors to the United Nations in an effort to facilitate building of a UN conference center in Macau, China.

ii. Several indicia of counterintelligence interest leading to prosecution on bribery charges having nothing to do with national security:

1. Likely international importance for China to have a UN center in China, especially in light of tensions over South China Sea;

2. Electronic intercept of an associate of defendant;

3. Arrest of another associate in EDNY on charges of smuggling documents to Chinese officials.

   a. The charges against the associate, Ying Lin, were subsequently reduced to a violation of FARA (Foreign Agent Registration Act);

4. Govt. provided notice of CIPA documents without disclosing materials to defense.

   iii. Motions to compel made on grounds of improper government motive for prosecution. Denied.
iv. On eve of trial, Govt. made ex parte communication with Judge to seek adjournment of trial to obtain approval to not disclose additional CIPA materials by submitting materials to Court for ex parte review.

1. Defense ex parte conference to try to inform Court of what may be relevant.
   a. Arguing in the blind.

2. Files reviewed by Court and nothing turned over.

v. Trial proceeds, defendant convicted. On appeal for traditional issues.

1. Black box materials never seen by defense.

b. United States v. Reza Zarrab

i. Turkish banker and gold trader accused of violating Iran Trade sanctions via $100 million in wire transfers from one foreign country to another, while outside the U.S., on basis that wires were made in U.S. dollars.

ii. While U.S. government never revealed any indication that the investigation or prosecution was the product of counterintelligence activity, the impact of case on international relations with Turkey was extraordinary:

1. Zarrab was a confidant of Turkish President Recip Tayyip Erdogan, and his decision later to cooperate was viewed as a “turn” against the Turkish government.

2. Case contributed significantly to the souring of U.S.-Turkish relations. Erdogan tried repeatedly and directly with Obama and Trump administrations to have Zarrab freed (or swapped), including via intermediaries like Rudy Giuliani and Michael Mukasey.

3. Michael Flynn’s meeting with Turkish officials re potential swap, while Flynn was on Trump transition team, has fallen within scope
of Mueller’s inquiry. Public speculation about whether Zarrab is cooperating in that inquiry.

iii. According to U.S. govt., FBI interest in Zarrab was triggered by their review of a leaked Turkish police dossier.

1. Implausible to believe extensive FISA intercepts would not have been tapped for information to support this international investigation involving Iran sanctions.

c. United States v. Keith Preston Gartenlaub

i. Defendant was a Boeing employee initially suspected of spying on behalf of the Chinese government, among other reasons because he is married to a Chinese-American woman, who has relatives and property in China.

ii. He was never charged with espionage, however, because the FBI’s FISA-based investigation did not support such a theory. Instead, in a FISC-authorized secret search of his home, the government found a hard drive containing child pornography. He was charged in the Northern District of California, tried and convicted of a single count of possession of child pornography.

1. He was sentenced to 41 months in prison. (Bail pending appeal was denied in part because of his wife’s ties to China.)

iii. Pre-trial, defense counsel made a number of arguments related to FISA, all of which failed.

1. Defense argued that the government's secret search of Gartenlaub’s computers violated his Fourth Amendment rights because:

   a. The government's application to the FISC could not have established probable cause to believe that he was an "agent of a foreign power [China]."

   b. Second, the application to the FISC likely contained intentional or reckless material falsehoods or omissions, requiring a Franks hearing.
c. Third, under FISA the FISC order could only authorize a search for "foreign intelligence information." By seizing and then examining files containing child pornography, the government exceeded the order.

2. The defense had to argue all of this based in part on suppositions because they were not given access to the FISA application for the search or the FISC order.

a. The defense argued, again, unsuccessfully, that they should be given access to the FISC materials.

i. Disclosure was both "necessary to make an accurate determination of the legality of the physical search," 50 U.S.C. § 1825(g), and required as a matter of due process.

iv. These issues are now all on appeal.
Tab 1
FBI DIRECTOR REFLECTS ON PRESENT AND FUTURE STATE OF THE BUREAU

CHRISTOPHER A. WRAY IS THE EIGHTH AND CURRENT DIRECTOR OF THE FBI, HAVING ASSUMED OFFICE ON AUGUST 2, 2017, AND HE HAS DEEP ROOTS IN THE COLLEGE.

“His grandfather, Samuel Gates, a name partner in the firm then known as Debevoise, Plimpton, Lyons and Gates, was one of the preeminent trial lawyers of his time. He was not only a Fellow of the College, but in the spring of 1979, he was President-Elect, scheduled to become President in the fall. On the way to the Spring Meeting, he unfortunately had a heart attack and suddenly died. In his memory, the College created the Samuel Gates Award, for significant contribution to the improvement of the litigation process,” said Past President Robert B. Fiske, Jr. in his introduction of Wray at the 2018 Spring Meeting in Phoenix, Arizona. “Sam’s wife, Chris’s grandmother, Philomene, better known as Phil, was a powerful force in her own right. Growing up in the South, she was one of three women to graduate from George Washington Law School in 1941. She went on to have an extremely distinguished career practicing law in New York City and serving the community in a wide variety of ways…. She was a regular attendee, and an important presence, at every College meeting for many years after Sam passed on.”

His other major connection to the College was his good fortune in being able to work with three of its former presidents, Griffin B. Bell, Frank C. Jones and Chilton Davis Varner, after graduating from Yale and Yale Law School. Another King & Spalding partner who played an extremely important role in Wray’s career was Larry Thompson. When Thompson became the deputy attorney general of the United States in May 2001, he asked Wray to be his principal associate deputy attorney general.

In 2003, President Bush nominated Wray to be the Assistant Attorney General in charge of the criminal division, a position previously held by one of his predecessors at the FBI, Robert Mueller. He served there until 2005, and then left to return to King & Spalding.
On June 7, 2017, President Trump announced that Wray was his choice to replace James B. Comey as director of the FBI, describing him as, “an impeccably qualified individual.” He went on to say in words that would resonate with all of us that know him, “I know that he will again serve his country as a fierce guardian of the law and a model of integrity,” Fiske said. “I speak for all who know and have worked with Director Wray, to say that it is extremely reassuring and comforting to know that we have someone with his professional skills, integrity and courage, to lead the FBI at this critical time in our nation’s history.”

Wray spoke to the audience on the threats faced by the FBI, where the Bureau needs to be moving forward and the meaning and impact of the work and the people of the FBI.

**A SIMPLE, PROFOUNDED MISSION**

“First, I feel compelled to say a couple of things about what’s been going on at the Bureau over the past few months. I have been lucky to work with the men and women of the FBI through a big chunk of my professional career, both originally as a line assistant out in the field working on all manner of cases, from bank robberies to public corruption, kidnapping, to financial fraud. Then at main justice, I got to see a different side of the Bureau on the day of 9/11, and in the years afterwards, watching the way agents, analysts and staff tackled the national security mission. I could not

---

**QUIPS & QUOTES**

I’m getting used to being introduced a lot, and that was a much warmer introduction than some of the ones I receive. I am really glad to be here because as you heard a little bit from Bob, I can confidently say that there’s no organization that meant more to my grandfather than this one.

Director Wray, on his introduction by Past President Fiske, which mentioned his grandfather Samuel Gates, a College Fellow and namesake of the Samuel E. Gates Litigation Award
be more fired up to be back and part of the Bureau’s next chapter.

“It took me about five seconds after walking back in the door at headquarters to remember how much I had missed the mission, protecting the American people, and upholding the Constitution. Those are fairly simple words to say, but they are very profound to actually execute. I come back to them a lot because I think staying laser-focused on that mission has never been more important than right now. This has been, by any measure, a chaotic and uncertain time for the men and women of the Bureau on a number of different levels. In the midst of all the choppy water, my immediate priority has been to try to bring calm and stability back to the Bureau.

“I am hoping to steady the ship by keeping our eyes focused on the mission and the work, day in, day out, just grinding away. In a society that is impatiently fixated on a fault on the results, I am somebody that happens to be a big believer in process. Following our rules, following the law, following our guidelines. Trying to make sure we’re not just doing the right thing, but doing it in the right way. Treating everybody with respect and pursuing the facts independently and objectively no matter who likes it. Those are not glamorous concepts. But I am firmly convinced that that is the approach that represents the Bureau at its best.

“National security remains our top priority as it has to be, and counterterrorism is still a paramount concern. The counterterrorism threat has morphed significantly since the last time I was in government. We are no longer just worried about large structured terrorist organizations like Al Qaeda planning large scale attacks in big cities like New York, Chicago and Los Angeles. That threat, to be clear, is still very much there. We now also face groups like ISIS, which can use social media to lure people in and inspire them much more remotely and indirectly to attack wherever and whenever they can. We face home-grown violent extremists who self-radicalize at home and are prone to attack with little warning. That new breed of terrorist is particularly troubling and challenging because unlike Al Qaeda, these folks use crude but agile methods of attack, from guns to knives to cars to primitive IEDs that they can figure out how to build just off the internet.

“Our attacks can be planned much more leanly and executed in a matter of days, or even hours, instead of weeks or months. They are perfectly happy to strike at so-called soft targets, which is an intelligence term that I have always despised, because soft targets basically means everyday people, living their everyday lives. People at concerts, people at cafes and clubs, people at their jobs, people walk-

**Quips & Quotes**

With all the voices out there trying to speak for us or about us, we focused more on letting our actions do the talking. Our work is what is going to endure over time, as all the chatter fades.

Director Wray

“We have 37,000 men and women at the Bureau who understand that we prove our mettle, not through the chatter of cable TV pundits or social media, but through the actual work we do. One case at a time, one search warrant at a time, one interview at a time, one intelligence product at a time, one decision at a time. We intend to keep grinding away, doing every-
ing down the street. These terrorists can strike anywhere from big cities to small towns. Right now we have about 1,000 open investigations into just that category of terrorists in all fifty states. We’re talking about homegrown violent extremists, individuals inspired by the global jihadist movement. That is the new normal that we have to contend with. It has created a whole new set of challenges, a much greater number of potential threats, even though each one of them might be more compact and lean.

“On the counterintelligence front, we still face traditional espionage—spies seeking our state secrets, working under diplomatic cover, or posing as every day citizens. Think of dead drops and tunnels, clandestine meetings in cafes, the kind of stuff you would see in a John le Carré novel. Today’s spies also seek our trade secrets, our economic ideas or innovation. They are often businessmen, researchers, scientists or students acting on behalf of state governments. Nation states like China are attempting to infiltrate our companies, your clients, by any means necessary to get control of cutting edge technology. Not just by stealing propriety information, but also by extra-legal means, like acquiring the company, or exploiting business partnerships.”

“That brings me to the third national security threat, the cyber threat. When I was last at DOJ as the head of the criminal division, we oversaw all cyber investigations. No area has evolved more dramatically since then, given the blistering pace of technological change.

“In 2005, when I left DOJ, social media did not really exist as it exists today. Tweeting was something that birds did. Today we live most of our lives online, and just about everything that is important to everybody in this room and our families, lives on the internet. That is a pretty scary thought. What was once a comparatively minor threat, people hacking for fun or bragging rights, has turned into full-blown economic espionage and breathtakingly lucrative cybercrime. This threat comes at us now from all sides. We have to worry not just about a range of threat actors, from multinational cyber syndicates, insider threats and activists. We are also seeing an increase in nation state sponsored computer intrusions. We are also seeing increasingly what we are calling a blended threat, which is the nation state actor in effect hiring criminal hackers, or mercenaries, to help execute their efforts. We are also concerned about a wider gamut of methods, from botnets to ransomware.

“As if that trifecta, counterterrorism, counterintelligence, and cyber of national security threats were not enough, we are also responsible at the Bureau for a laundry list of criminal threats—everything from gangs to crimes against kids to public corruption to hate crimes to health care fraud and just about everything in between.

“Violent crime has been on the rise in a lot of areas in this country for the last several years. It is the top concern for our state and local partners. Our crime data for 2015 and 2016 showed increases in violent crime of roughly 4% a year. Four percent might not sound like a big number, but when you consider the sheer number of victims 4% represents in a country our size, you realize the human toll that is reflected in that increase. While preliminary statistics for the first half of last year, 2017, show that overall violent crime finally fell just a little bit, murders, and non-negligent manslaughters were up 1.5%.

“At the Bureau we are focused on doing everything we can to help our partners fight it. We now have 168 safe-street task forces, and forty-seven violent crimes task forces. We are also providing our state and local partners with intelligence related to gun crime and crime trend analysis. We are developing targeting packages, which help them prioritize neighborhoods, and prioritize their own resources in a way that makes their impact maximized.

“Closely connected to the violent crime problem is the country’s opioid epidemic. We are trying to do our part, working not just with our partners in state and local law enforcement, and in federal agencies, but also in other
disciplines. We have launched a prescription drug initiative, targeting criminal enterprises that engage in prescription drugs schemes. We are focused on medical professionals who distribute opioids with no legitimate purpose. We have established a high-tech organized crime unit, which focuses on the trafficking of opioids over the internet, especially the dark net. We have more than doubled our number of transnational organized crime task forces.”

**PARTNERSHIPS AND INNOVATION**

“Now a few hectic months into the job, I am still listening. I am trying to get to all fifty-six of our field offices by the end of this year. I am formulating my own long-term priorities about where the Bureau needs to be over the next ten years. There are a few, very positive, enterprise-wide things that have jumped out at me already that I thought I would flag. First, the FBI’s commitment to partnerships has evolved, almost breathtakingly, since the last time I was at DOJ. I am talking about partnerships with the rest of the intelligence community, our federal, state and local law enforcement colleagues, our foreign counterparts, our partners in the private sector in the communities that we serve. Partnerships are much more part of the DNA of the Bureau, and it is a real point of pride in every office that I visit. It is clearly a change that happened gradually over a period of time, but because I went into the private sector for a while, I am able to see the before and after in a way that jumps out at me. The FBI has always been proud, passionate, persistent, perfectionist, and that has definitely not changed. What has changed is what our folks are proud, passionate, persistent and perfectionist about. That is their partnerships.

“It is a mindset of what can we bring to the table, what can they bring to the table. How can we match strengths, so that we can put the FBI’s two together with their two, and somehow have it equal more than four. Equal five, or six, or seven. That kind of sea change has made me realize more than ever, how important it is that we continue to nurture and build on those relationships as we move forward.

“The second thing that has really jumped out at me is our dramatically stronger integration of intelligence, and our continued need to focus on it, in everything that we do. Under Director Mueller’s leadership in the aftermath of 9/11, the FBI made a paradigm shift from a law enforcement agency that investigated crime after the fact to a national security service, working to prevent crime and terrorism. That transformation continued under Director Comey and today we have developed a sophisticated and complex intelligence program.

“We talk a lot about the term ‘intelligence’ in a national security world, but what it really boils down to is information. Information that we use to make decisions and to drive operations. Information that we share with the people who need
it, whether state, local, federal law enforcement, to the community and civic leaders, to business leaders in the private sector. On one of my first visits to the FBI Academy at Quantico I spotted this little stone plaque, tucked away on a corner in one of the courtyards. It was only about the size of an 8 1/2 by 11 piece of paper. It had a picture of the Twin Towers. Underneath the Twin Towers it just had two words, “Intelligence Matters.” That is as true today as it was on 9/11, maybe even more so. We know we are going to be really great at intelligence. We have to get better at collecting it, at analyzing it, and sharing it, in everything we do.

“"We have to make the best and highest use of the information we have. We have to be able to connect the dots and see the bigger picture. A lot of that is easier to say than it is to do. What I see is a radically more sophisticated and integrated effort to do that in the bureau. We are determined to keep pushing ourselves so that we can see not just those threats, but the threats that are coming around the pike. The FBI has come a long way in the years since I left DOJ, but I am continually asking myself, what’s next? Where do we need to be down the road? As grateful as I am for the progress that Director Mueller and others launched fifteen or so years ago, that put us in the position we are in 2018, I am trying to focus on where do we need to be ten years from now? What kind of transformation do we need to have over the next ten years? To remain the premier law enforcement and national security organization in the world, not just in 2018, but in 2028, and beyond? We need to get smarter and more agile than we have ever been. To do that, we are going to have to be more innovative.”

“The word innovation is not something you normally associate with the federal government. When I talk about innovation, what I mean is not just technological innovation. I mean innovation even more broadly in terms of best practices, strategies, threat indicators, processes, partnerships, really anything that we can do to be smarter, better, more agile, more creative. As I make my way around the 37,000 people in the Bureau, I am trying to encourage everyone to think more, not just about what is directly in front of them, but more to think long term, ten, fifteen, twenty years. Where do we need to be then? What kind of innovation do we need? What is the threat that we are underestimating now, but that is going to be the biggest threat then? What will our workforce need to look like then? What will our technologies need to look like then?

“We are trying to drive that innovation in a variety of ways across the enterprise. Trying to rethink the way we work with our partners, the way we use technology, the way we conduct operations. For example, we now have a program called The Technology Accelerator, which provides a platform for employees to easily share and work on innovative ideas and solutions. One idea is a mobile app on FBI smartphones to collect crime scene and evidence data quickly and accurately. The goal is to cut down on the time spent at crime scenes, improve data accuracy and simplify the record keeping process. Frankly, it makes so much sense, you wonder, why didn’t we think of it before? We are also encouraging all of the heads of our field offices to tell their employees to spend 10 percent of their time innovating. That is what they do at places like Google. Then, when they come up with brilliant ideas, they can submit them to the technology accelerator for development.

“This spring, we are holding our first innovation challenge to examine some of the top
technical problems reported over the past year from the field. Employees from across the Bureau will have two months to come up with solutions to those problems, and the winners will present their ideas at the Big Idea Summit, which we are holding at headquarters this summer. By fostering more of that culture of innovation, we hope to ensure that the Bureau will continue to always be leading the way, years and years from now.”

**WORK THAT A FOUR-YEAR-OLD UNDERSTANDS AS MEANINGFUL**

“I want to close with a few thoughts about the FBI’s work, the people and the challenging environment that we are in. It seems that there is no shortage of opinions about the Bureau these days, but an awful lot of that is rhetoric, without much to back it up. The old saying is true, talk is cheap. What is valuable are the views of those who actually know, who actually experience our work. Those are informed opinions. The judges who hear our hardworking agents on the stand, the magistrate judges who have to sign our warrants, the victims and their families - [they are the ones] that our folks get up every morning determined to protect, our year round partners in federal, state, local law enforcement in the intelligence community, overseas and in the private sector.

“Like me, those folks get to see the men and women of the Bureau for who they really are. People of integrity, people of compassion, and kindness, people fiercely focused on doing the right thing, in the right way. With all the voices out there trying to speak for us or about us, we are focused more on letting our actions do the talking. Our work is what is going to endure over time, as all the chatter fades away. I am doing my best to remind our folks of that. I am doing my best to try and reintroduce the country to the work that we do every day to protect Americans from national security threats coming from all sides to a mind boggling array of criminal threats. For example, this past December, our agents in Sacramento arrested Everit Jameson who had pledged allegiance to ISIS, and was plotting an attack on Pier 39, in San Francisco on Christmas Day, combining the deadly tactics used in San Bernardino and at the Tribecca attack in New York. He planned to use explosives to funnel people into the area, so he could cause even greater casualties. Quite a number of lives were saved that day.

“In October, through something we call Operation Cross Country, which we conducted in forty-four states and the District of Columbia, we arrested 120 sex traffickers and recovered eighty-four sexually exploited juveniles. Those included a three-month-old girl and her five-year-old sister, who were recovered after a family friend, and I use that term about as loosely as I can, offered to sell them for sex for $600.

“We also have our top ten most wanted fugitives program. Through that program we have been able to apprehend some of the most dangerous violent offenders over the past two years. One captures what I think is the character of the Bureau. Robert Van Wees turned himself in to FBI agents in January, a few weeks after being added to the top ten list. This is a guy who was wanted in Texas for the 1983 murder of a young woman who at the time had a one-year-old daughter. For thirty-three years, that woman’s daughter had hoped and prayed for his capture. He was finally arrested on her birthday, no less. Cold comfort. We hope it brought her some measure of peace and justice. To me, it illustrates the persistence, the relentless pursuit of justice that is so typical of the people I get to work with.

“That kind of work is what keeps us going when times get tough. The FBI’s work matters because with our investigations, people’s lives hang in the balance. That is why our actions have
to be based at all times on the guiding principles of adherence to the Constitution, the rule of law, integrity and fairness. The same in many ways could be said for your work. In different ways, lives, certainly livelihoods often hang in the balance when you take a case to trial. Like the men and women of the FBI, I think each of you understands that the rule of law is our country’s bedrock. Every day at the Bureau we have to weigh our need to protect the citizens we serve with our duty to the Constitution and the rule of law. We have to weigh national security on the one hand, and privacy and civil liberties on the other. Director Mueller used to tell agents at Quantico graduations that it is not a question of conflict; it is a question of balance. That the rule of law, civil rights and civil liberties are not the FBI’s burdens, they are the very things that make us all safer and stronger.

“As long as I am at the Bureau, we are going to make sure that we never forget that. As long as I am there, we are going to stay committed to doing things independently and by the book. If we start getting too worried about who is going to be happy, or unhappy, about the results of one of our investigations, or who is going to criticize us or praise us for one of our investigations, we are going to lose our way, and I am determined not to let that happen. We cannot let the ends justify the means. We have to have our means justify our ends. We are going to get through this current tumult by keeping our nose to the grindstone and doing great work, case by case, day by day, no matter what else happens.

“Every day I pass people on the street, who come up to me, and say, ‘I just want you to know, we’re all praying for you.’ I believe strongly in the power of prayer, so my first reaction is, ‘Thank you.’ My second reaction is, ‘I have not been in front of a television in the last two hours. Is this a new thing, or is this the other stuff?’ I have tried to make that point to a lot of our folks because I think our 37,000 people have the same experience. One of the things I try to do is remind them about why they went into this work in the first place, and that is the mission.

“For me, I often think back to a time when I was an AUSA, working in Atlanta. My daughter was four. It was Dad’s Day at the nursery school. One of the questions, of course, was what does your dad do for a living? This guy is standing next to me, and he keeps looking at me, so I start looking over at him. He says, ‘Do you mind if I ask you what you do for a living?’ I looked back at the bulletin board, and my daughter had put, ‘My daddy and his friends put bad guys in jail and help keep us all safe.’ Then I looked over at his daughter’s answer. It said, ‘My daddy talks on the phone all day, so mommy and I can buy nice stuff.’

“What I try to say to our 37,000 people when they start to drag is if you want to do something that a four-year-old little girl gets as meaningful and impactful and valuable, you are in the right place. We know that the mission comes first. We know the American people come first. That has not changed, and it is not going to change. Thank you for inviting me here, and for taking the time to listen.”

David N. Kitner
Dallas, Texas

Samuel E. Gates Litigation Award

To honor a lawyer or judge, whether or not a Fellow of the College, who has made a significant, exceptional and lasting contribution to the improvement of the litigation process.

Chair: Robert C. Riter, Jr.
rriter@riterlaw.com
Tab 2
Chapter 36—Foreign Intelligence Surveillance
50 USCA Ch. 36, Refs & Annos

Subchapter I—Electronic Surveillance
50 USCA Ch. 36, Subch. I, Refs & Annos

§ 1801. Definitions
§ 1802. Electronic Surveillance Authorization Without Court Order; Certification by
Attorney General; Reports to Congressional Committees; Transmittal Under Seal; Duties
and Compensation of Communication Common Carrier; Applications; Jurisdiction of
Court
§ 1803. Designation of Judges
§ 1804. Applications for Court Orders
§ 1805. Issuance of Order
2473
2473
2473
§ 1806. Use of Information
§ 1807. Report of Electronic Surveillance
§ 1808. Report of Attorney General to Congressional Committees; Limitation on
Authority or Responsibility of Information Gathering Activities of Congressional
Committees; Report of Congressional Committees to Congress
§ 1809. Criminal Sanctions
§ 1810. Civil Liability
§ 1811. Authorization During Time of War
§ 1812. Statement of Exclusive Means by Which Electronic Surveillance and Interception
of Certain Communications May be Conducted
§ 1813. Procedures for the Retention of Incidentally Acquired Communications

Subchapter II—Physical Searches

§ 1821. Definitions
§ 1822. Authorization of Physical Searches for Foreign Intelligence Purposes
§ 1823. Application for Order
§ 1824. Issuance of Order
§ 1825. Use of Information
§ 1826. Congressional Oversight
§ 1827. Penalties
§ 1828. Civil Liability
§ 1829. Authorization During Time of War

Subchapter III—Pen Registers and Trap and TRACE Devices for Foreign Intelligence
Purposes

§ 1841. Definitions
§ 1842. Pen Registers and Trap and TRACE Devices for Foreign Intelligence and
International Terrorism Investigations
§ 1843. Authorization During Emergencies
§ 1844. Authorization During Time of War
§ 1845. Use of Information
§ 1846. Congressional Oversight
Subchapter IV—Access to Certain Business Records for Foreign Intelligence Purposes
§ 1861. Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations
§ 1862. Congressional Oversight
§ 1864. Notification of Changes to Retention of Call Detail Record Policies
Subchapter V—Oversight
50 USCA Ch. 36, Subch. V, Refs & Annos
§ 1871. Semiannual Report of the Attorney General
§ 1872. Declassification of Significant Decisions, Orders, and Opinions
§ 1873. Annual Reports
§ 1874. Public Reporting by Persons Subject to Orders
Subchapter VI—Additional Procedures Regarding Certain Persons Outside the United States
§ 1881. Definitions
§ 1881a. Procedures for Targeting Certain Persons Outside the United States Other than United States Persons
§ 1881b. Certain Acquisitions Inside the United States Targeting United States Persons Outside the United States
§ 1881c. Other Acquisitions Targeting United States Persons Outside the United States
§ 1881d. Joint Applications and Concurrent Authorizations
§ 1881e. Use of Information Acquired Under this Subchapter
§ 1881f. Congressional Oversight
§ 1881g. Savings Provision
Subchapter VII—Protection of Persons Assisting the Government
§ 1885. Definitions
§ 1885a. Procedures for Implementing Statutory Defenses
§ 1885b. Preemption
§ 1885c. Reporting
United States Code Annotated
Title 50. War and National Defense (Refs & Annos)
Chapter 36. Foreign Intelligence Surveillance (Refs & Annos)
Subchapter I. Electronic Surveillance (Refs & Annos)

50 U.S.C.A. § 1806

§ 1806. Use of information

Effective: June 2, 2015

(a) Compliance with minimization procedures; privileged communications; lawful purposes

Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification by United States

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.
(e) Motion to suppress

Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that--

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or
granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under subsection (e) or (f) of section 1805 of this title and a subsequent order approving the surveillance is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Coordination with law enforcement on national security matters

(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this subchapter may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1804(a)(7)(B) of this title or the entry of an order under section 1805 of this title.

CREDIT(S)


Notes of Decisions (52)

50 U.S.C.A. § 1806, 50 USCA § 1806
§ 1825. Use of information, 50 USCA § 1825

50 U.S.C.A. § 1825

§ 1825. Use of information

Effective: July 10, 2008

Currentness

(a) Compliance with minimization procedures; lawful purposes

Information acquired from a physical search conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No information acquired from a physical search pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Notice of search and identification of property seized, altered, or reproduced

Where a physical search authorized and conducted pursuant to section 1824 of this title involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this chapter and shall identify any property of such person seized, altered, or reproduced during such search.

(c) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(d) Notification by United States

Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from a physical search pursuant to the authority of this subchapter, the United States shall, prior to the trial, hearing, or the other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(e) Notification by States or political subdivisions
Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof against an aggrieved person any information obtained or derived from a physical search pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(f) Motion to suppress

(1) Any person against whom evidence obtained or derived from a physical search to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such search on the grounds that--

(A) the information was unlawfully acquired; or

(B) the physical search was not made in conformity with an order of authorization or approval.

(2) Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(g) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (d) or (e) of this section, or whenever a motion is made pursuant to subsection (f) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to a physical search authorized by this subchapter or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this subchapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

(h) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (g) of this section determines that the physical search was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the
aggrieved person. If the court determines that the physical search was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(i) Finality of orders

Orders granting motions or requests under subsection (h) of this section, decisions under this section that a physical search was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the physical search shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

(j) Notification of emergency execution of physical search; contents; postponement, suspension, or elimination

(1) If an emergency execution of a physical search is authorized under section 1824(d) of this title and a subsequent order approving the search is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to the search as the judge may determine in his discretion it is in the interests of justice to serve, notice of--

(A) the fact of the application;

(B) the period of the search; and

(C) the fact that during the period information was or was not obtained.

(2) On an ex parte showing of good cause to the judge, the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed 90 days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Coordination with law enforcement on national security matters

(1) Federal officers who conduct physical searches to acquire foreign intelligence information under this subchapter may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1823(a)(6) of this title or the entry of an order under section 1824 of this title.

CREDIT(S)


Notes of Decisions (4)

50 U.S.C.A. § 1825, 50 USCA § 1825
Tab 3
The Honorable Michael R. Pence  
President  
United States Senate  
Washington, DC 20510

This report is submitted in accordance with sections 107 and 502 of the Foreign Intelligence Surveillance Act of 1978 (the “Act”), as amended, 50 U.S.C. § 1801 et seq., and section 118 of USA PATRIOT Improvement and Reauthorization Act of 2005, as amended. This report provides information regarding: (1) all final, filed applications made by the Government during calendar year 2017 for authority to conduct electronic surveillance and/or physical search for foreign intelligence purposes under the Act; (2) all final, filed applications made by the Government during calendar year 2017 for access to certain business records (including the production of tangible things) for foreign intelligence purposes; and (3) certain requests made by the Federal Bureau of Investigation (FBI) pursuant to national security letter authorities.

In addition to reporting statistics based on the number of final filed applications this report also includes statistics published by the Director of the Administrative Office of the United States Courts (AOUSC). The AOUSC reports the number of proposed applications rather than the number of final, filed applications. Rule 9(a) of the Foreign Intelligence Surveillance Court Rules of Procedure requires the Government to submit proposed applications at least seven days before the Government seeks to have a matter entertained by the Foreign Intelligence Surveillance Court (FISC). Modifications or withdrawals of applications may occur between the filing of a proposed application and the filing of a final application for a variety of reasons, including the Government modifying a proposed application in response to questions or concerns raised by the Court. The statistics prepared by the AOUSC, which use the number of proposed applications rather than final, filed applications as their baseline, reflect this robust interaction between the Government and the Court, and thus are included herein to provide important additional context. The AOUSC Director’s full report is available on the AOUSC website.

**Applications Made to the Foreign Intelligence Surveillance Court During Calendar Year 2017** (section 107 of the Act, 50 U.S.C. § 1807)

During calendar year 2017, the Government filed 1,349 final applications to the Foreign Intelligence Surveillance Court (hereinafter “FISC”) for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The 1,349 applications include applications made solely for electronic surveillance, applications made solely for
physical search, and combined applications requesting authority for electronic surveillance and physical search. Of these, 1,321 applications included requests for authority to conduct electronic surveillance.

Two of these applications were withdrawn by the Government. The FISC did not deny any final, filed applications in whole, or in part. The FISC made modifications to the proposed orders in 154 final, filed applications. Thus, the FISC approved collection activity in a total of 1,319 of the applications that included requests for authority to conduct electronic surveillance.

The AOUSC, applying the methodology outlined above, has reported that the FISC received 1,372 proposed applications in 2017 for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes. The AOUSC reported that 948 proposed orders were granted, 353 proposed orders were modified, 47 proposed applications were denied in part, and 24 proposed applications were denied in full. As noted above, the AOUSC statistics include modifications made to proposed orders between the filing of the proposed application and the final application, as well as proposed applications withdrawn by the Government in full or in part after being advised that the Court would not grant the proposed application as initially submitted by the Government.

During calendar year 2017, the total number of persons targeted for orders for electronic surveillance was between 1,000 and 1,499. The aggregate number of United States persons targeted for orders for electronic surveillance was between zero and 499.

**Applications for Access to Certain Business Records (Including the Production of Tangible Things) Made During Calendar Year 2017** (section 502 of the Act, 50 U.S.C. § 1862(c)(1))

During calendar year 2017, the Government filed 117 final applications to the FISC for access to certain business records (including the production of tangible things) for foreign intelligence purposes. The FISC did not deny, in whole or in part, any such final, filed application by the Government during calendar year 2017. The FISC did not modify any of the proposed orders in a final application for access to business records.

The AOUSC, applying the methodology outlined above, has reported that the FISC received 118 proposed applications in 2017 for access to certain business records (including the production of tangible things) for foreign intelligence purposes. In these matters, the AOUSC reported that 92 proposed orders were granted, 23 proposed orders were modified, two proposed applications were denied in part, and one proposed application was denied in full.

Twenty-five final, filed applications did not specifically identify an individual, account, or personal device as the specific selection term. The FISC did not modify the proposed orders.

---

1 Notably, the definition of “specific selection term” for obtaining an order for the production of tangible things is “a term that specifically identifies a person, account, address, or personal device, or any other specific identifier,” 50 U.S.C. § 1861(k), whereas the definition of “specific selection term” for the reporting requirement encompasses a smaller group of terms, to include only “an individual, account, or personal device,” 50 U.S.C. § 1862(c)(1)(C). Thus, the reporting requirement mandates inclusion in this report of certain requests that otherwise meet the definition of specific selection term in 50 U.S.C. § 1861(k). For example, the reporting requirement mandates inclusion of requests in which the specific selection term was an “address.”
in these 25 applications for access to business records. Separately, the FISC did not direct additional, particularized minimization procedures beyond those adopted pursuant to section 1861(g) to the proposed orders in applications made by the Government.


The FBI reports it made 9,006 NSL requests (excluding requests for subscriber information only) in 2017 for information concerning United States persons. These sought information pertaining to 2,983 different United States persons.²

The FBI reports it made 14,861 NSL requests (excluding requests for subscriber information only) in 2017 for information concerning non-United States persons. These sought information pertaining to 3,084 different non-United States persons.³

The FBI reports it made 17,712 NSL requests in 2017 for information concerning only subscriber information for United States persons and non-United States persons. These sought information pertaining to 4,598 persons.⁴

---

² In the course of compiling its NSL statistics, the FBI may over-report the number of United States persons about whom it obtained information using NSLS. For example, NSLS that are issued concerning the same U.S. person and that include different spellings of the U.S. person's name would be counted as separate U.S. persons, and NSLS issued under two different types of NSL authorities concerning the same U.S. person would be counted as two U.S. persons.

³ In the course of compiling its NSL statistics, the FBI may over-report the number of non-United States persons about whom it obtained information using NSLS. For example, NSLS that are issued concerning the same non-U.S. person and that include different spellings of the non-U.S. person's name would be counted as separate non-U.S. persons, and NSLS issued under two different types of NSL authorities concerning the same non-U.S. person would be counted as two non-U.S. persons.

⁴ Because Congress has recognized that the FBI typically knows little about the user of a facility when requests for only subscriber information are made, Section 118(c)(2)(B) does not require the number of requests for NSLS seeking only subscriber information to be broken down to identify the number of requests related to United States persons and non-United States persons. See Section 118(c)(2)(B), USA Patriot Act Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 217 (2006), as amended.
We hope that this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Stephen E. Boyd
Assistant Attorney General
Tab 4
STATEMENT OF

ELIZABETH GOITEIN
CO-DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

HEARING ON

OVERSIGHT AND REAUTHORIZATION OF THE FISA AMENDMENTS ACT:
THE BALANCE BETWEEN NATIONAL SECURITY, PRIVACY AND CIVIL LIBERTIES

MAY 10, 2016
Chairman Grassley, Ranking Member Leahy, and members of the committee, thank you for this opportunity to testify on behalf of the Brennan Center for Justice at New York University School of Law. The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. I co-direct the Center’s Liberty and National Security Program, which works to advance effective counterterrorism policies that respect constitutional values and the rule of law.

Our nation faces real threats from international terrorism. The challenge and the responsibility you face as members of Congress is to ensure that these threats are addressed, not only effectively, but in a way that is consistent with the Constitution, the privacy interests of law-abiding individuals, and our nation’s economic interests. Section 702 surveillance in its current form does not accomplish these aims.

I. A Massive Expansion in Government Surveillance

Technological advances have revolutionized communications. People are communicating at a scale unimaginable just a few years ago. International phone calls, once difficult and expensive, are now as simple as flipping a light switch, and the Internet provides countless additional means of international communication. Globalization makes such exchanges as necessary as they are easy. As a result of these changes, the amount of information about Americans that the NSA intercepts, even when targeting foreigners overseas, has exploded.

But instead of increasing safeguards for Americans’ privacy as technology advances, the law has evolved in the opposite direction since 9/11, increasingly leaving Americans’ information outside its protective shield. Section 702 is perhaps the most striking example.

Before 2007, if the NSA, operating domestically, sought to collect a foreign target’s communications with an American inside the U.S., it had to show probable cause to the Foreign Intelligence Surveillance Court (FISA Court) that the target was a foreign power – such as a foreign government or terrorist group – or its agent. The Protect America Act of 2007 and the FISA Amendments Act of 2008 (which created Section 702 of FISA) eliminated the requirement of an individualized court order. Domestic surveillance of communications between foreign targets and Americans now takes place through massive collection programs that involve no case-by-case judicial review.

In addition, the pool of permissible targets is no longer limited to foreign powers or their agents. Under Section 702, the government may target for foreign intelligence purposes any person or group reasonably believed to be foreign and located overseas. The person or group need not pose any threat to the United States, have any information about such threats, or be

---

1 This testimony is submitted on behalf of a Center affiliated with New York University School of Law but does not purport to represent the school’s institutional views on this topic. More information about the Brennan Center’s work can be found at [http://www.brennancenter.org](http://www.brennancenter.org).


4 50 U.S.C. § 1881a(b).
suspected of any wrongdoing. This change not only renders innocent private citizens of other nations vulnerable to NSA surveillance; it also greatly increases the number of communications involving Americans that are subject to acquisition – as well as the likelihood that those Americans are ordinary, law-abiding individuals.

Further expanding the available universe of communications, the government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, or about the target. The inclusion of “about” in this formulation is a dangerous leap that finds no basis in the statutory text and little support in the legislative history. In practice, it has been applied to collect communications between non-targets that include the “selectors” associated with the target (e.g., the target’s e-mail address or phone number). In theory, it could be applied even more broadly to collect any communications that even mention ISIS or a wide array of foreign leaders and public figures who are common topics of conversation. Although the NSA is prohibited from intentionally acquiring purely domestic communications, such acquisition is an inevitable result of “about” collection.

Other than the foreignness and location criteria (and certain requirements designed to reinforce them), the only limitation on collection imposed by the statute is that the government must certify that acquiring foreign intelligence is a significant purpose of the collection. FISA’s definition of foreign intelligence, however, is not limited to information about potential threats to the U.S. or its interests. Instead, it includes information “that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States.” This could encompass everyday conversations about current events. A conversation between friends or colleagues about the merits of the Trans-Pacific Partnership Agreement, for instance, “relates to the conduct of foreign affairs.” Moreover, while a significant purpose of the program must be the acquisition of foreign intelligence, the primary purpose may be something else altogether. Finally, the statute requires the FISA Court to accept the government’s certifications under Section 702 as long as they contain the required elements.

The government uses Section 702 to engage in two types of surveillance. The first is “upstream collection,” whereby a huge proportion of communications flowing into and out of the United States is scanned for selectors associated with designated foreigners. Although the data are first filtered in an attempt to weed out purely domestic communications, the process is imperfect and domestic communications are inevitably acquired. The second type of Section 702 surveillance is “PRISM collection,” under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communications service providers, who must turn

---

7 50 U.S.C. § 1801(e)(2).
8 In re Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002).
10 PCLOB 702 REPORT, supra note 5, at 36-41.
over any communications to or from the selector.\footnote{Id. at 33-34.} Using both approaches, the government collected more than 250 million Internet transactions a year as of 2011.\footnote{[Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).}

Due to the changes wrought by Section 702, it can no longer be said that FISA is targeted at foreign threats. To describe surveillance that acquires 250 million Internet communications a year as “targeted” is to elevate form over substance. And on its face, the statute does not require that the targets of surveillance pose any threat, or that the purpose of the program be the collection of threat information.

It is certainly possible that the government is choosing to focus its surveillance more narrowly than Section 702 requires. The certifications that the government provides to the FISA Court – which include the foreign intelligence categories at which surveillance is aimed, and could therefore shed some light on this question – have not been publicly disclosed by the government. Even if actual practices stop short of what the law allows, however, the available statistics suggest a scope of surveillance that is difficult to reconcile with claims of narrow targeting. Moreover, one certification, listing the foreign nations and factions about which foreign intelligence could be sought, was leaked; it included most of the countries in the world, ranging from U.S. allies to small countries that play little role on the world stage.

More important, Americans’ privacy should never depend on any given administration’s voluntary self-restraint. Nor should it depend on additional requirements layered on by the FISA Court, given that the court’s membership changes regularly and its judges generally are not bound by others’ decisions. Section 702 establishes the boundaries of permissible surveillance, and it clearly allows collection of communications between Americans and foreigners who pose no threat to the U.S. or its interests. That creates an enormous opening for unjustified surveillance.

\section{II. Constitutional Concerns}

The warrantless acquisition of millions of Americans’ communications presents deep Fourth Amendment concerns. The communications being obtained under Section 702, like any e-mails or phone calls, include not only mundane conversations, but the most private and personal confidences, as well as confidential business information and other kinds of privileged exchanges. Since the Supreme Court decided \textit{Katz v. United States} in 1967, the government has been required to obtain a warrant to wiretap Americans’ communications.\footnote{389 U.S. 347 (1967).} Moreover, in a subsequent case, the Court made clear that this requirement applied in domestic national security cases as well as criminal cases.\footnote{United States v. U.S. Dist. Court for the E. Dist. Of Mich. (\textit{Keith}), 407 U.S. 297 (1972).}

\subsection{A. “Incidental” Collection}

The government nonetheless justifies the warrantless collection of international communications under Section 702 on the ground that the targets themselves are foreigners
overseas, and the Supreme Court has held (in a different context) that the government does not need a warrant to search the property of a non-U.S. person abroad. Although the communications obtained under Section 702 sometimes involves both foreigners and Americans, the FISA Court has held that the right to conduct warrantless surveillance of the foreign target entails the right to “incidentally” collect the communications of those in contact with the target.

But there is nothing “incidental” about the collection of Americans’ communications under Section 702. Indeed, with one exception, Section 702 wrought no change to the government’s authority to collect foreign-to-foreign communications. The primary change brought about by Section 702 was to eliminate the requirement of an individual court order when a foreign target communicates with an American. The legislative history makes clear that facilitating the capture of communications to, from, or about Americans was a primary purpose, if not the primary purpose, of the statute.

In any event, outside of Section 702, the case law does not support the existence of a right to warrantless “incidental” collection. In criminal cases, courts have held that the government need not obtain separate warrants for everyone in contact with the target. But they have emphasized the existence of a warrant for the target (which affords some vicarious protection to those in contact with him) and the application of strict minimization procedures.

In the Section 702 context, there is no warrant to help mitigate “incidental” collection, and the minimization procedures are significantly weaker than those that apply in the domestic criminal context.

B. The Foreign Intelligence Exception

Alternatively, the FISA Court (and, more recently, a district court following its lead) has relied on the “foreign intelligence exception” to the Fourth Amendment’s warrant requirement. The Supreme Court has never recognized this exception, and there is significant controversy over its scope. The Supreme Court has never recognized this exception, and there is significant controversy over its scope. The FISA Court has construed the exception extremely broadly, 

15 See infra Part VII(A).
16 See, e.g., FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary, 109th Cong. 9 (2006), available at http://www.gpo.gov/fdsys/pkg/CHRG-109shrg43453/pdf/CHRG-109shrg43453.pdf (statement of Michael Hayden, Director, Nat’l Sec. Agency) (“[W]hy should our laws make it more difficult to target the al Qaeda communications that are most important to us—those entering or leaving this country.”); see also Transcript of Privacy and Civil Liberties Oversight Board Public Workshop, Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act 109 (July 9, 2013), available at http://www.pclob.gov/library/20130709-Transcript.pdf (statement of Steven G. Bradbury, Former Principal Deputy Ass’t Att’y Gen., Dep’t of Justice Office) (“But it is particularly focused on communications in and out of the United States because . . . those are the most important communications you want to know about if you’re talking about a foreign terrorist suspect communicating to somebody you don’t know inside the United States.”).
18 See Brief for Appellant at Argument I, In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) (noting that “FISA’s minimization standards are more generous than those in Title III”).
stating that it applies even if the target is an American and even if the primary purpose of collection has no relation to foreign intelligence.\textsuperscript{20}

In the era before FISA, however, several federal courts of appeal had the opportunity to review foreign intelligence surveillance, and they articulated a much narrower version of the exception.\textsuperscript{21} They held that it applies only if the target is a foreign power or agent thereof, and only if the acquisition of foreign intelligence is the primary purpose of the surveillance. They also emphasized the importance of close judicial scrutiny (albeit after-the-fact) in cases where the target challenges the surveillance. While these cases addressed surveillance activities that differed in many respects from Section 702, it is clear that Section 702 surveillance would not pass constitutional muster under the standards they articulated.

A detailed analysis of the case law is beyond the scope of this testimony, but the Brennan Center’s report, \textit{What Went Wrong With the FISA Court}, engages in such an analysis and explains why the foreign intelligence exception does not justify Section 702 surveillance.\textsuperscript{22}

\textbf{C. The Reasonableness Test}

Even if a foreign intelligence exception applies, the surveillance still must be “reasonable” under the Fourth Amendment. The “reasonableness” inquiry entails weighing the government’s interests against the intrusion on privacy.\textsuperscript{23}

In undertaking this analysis, courts generally accept that the government’s interest in protecting national security is of the highest order – as it certainly is. But to determine the reasonableness of a surveillance scheme, one must also ask whether it goes further than necessary to accomplish the desired end. For instance, how does it further national security to allow the targeting of foreigners who have no known or suspected affiliation with foreign governments, factions, or terrorist groups? How does it further national security to permit the FBI to search for Americans’ communications to use in prosecutions having nothing to do with national security?\textsuperscript{24}

Moreover, in assessing the impact on privacy rights, the FISA Court has focused on the protections offered to Americans by minimization procedures.\textsuperscript{25} As discussed below, however, these protections fall short in a number of significant respects. On their face, they allow Americans’ communications to be retained, disseminated, and used in a wide range of circumstances.

\textsuperscript{20} \textit{See, e.g., In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act}, 551 F.3d 1004 (FISA Ct. Rev. 2008); \textit{In re DNI/AG Certification [REDACTED]}, No. 702(i)-08-01 (FISA Ct. Sept. 4, 2008).


\textsuperscript{22} \textit{Goitein & Patel, supra} note 2, at 11-12, 35-43.


\textsuperscript{24} \textit{See infra} Part V.

\textsuperscript{25} \textit{In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act}, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008).
III. Risks and Harms of Mass Data Collection

Constitutional concerns aside, the mass collection and storage of communications that include sensitive information about Americans carries with it significant risks and harms, which must be considered in evaluating what the appropriate scope of surveillance should be.

A. Risk of Abuse or Mishandling of Data

The substantive legal restrictions on collecting information about Americans are looser than they have been since before 1978. At the same time, the amount of data available to the government and the capacity to store and analyze that data are orders of magnitude greater than they were during the period of J. Edgar Hoover’s worst excesses. History teaches us that this combination is an extraordinarily dangerous one.

To date, there is only limited evidence of intentional abuse of Section 702 authorities.26 There have, however, been multiple significant instances of non-compliance by the NSA with FISA Court orders. Notably, these include cases in which the NSA did not detect the non-compliance for years, and the agency’s overseers had no way to uncover the incidents in the meantime. Given that these incidents went unreported for years even when the agency was not trying to conceal them, it is not clear how overseers would learn about intentional abuses that agency officials were making every effort to hide. In other words, regardless of whether intentional abuse is happening today, the potential for abuse to take place – and to go undiscovered for long periods of time – is clearly present.

Inadvertent failures to adhere to privacy protections are a concern in their own right. On multiple occasions in the past decade, the FISA Court has had occasion to rebuke the NSA for repeated, significant, and sometimes systemic failures to comply with court orders. These failures took place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, dissemination, and retention. It is instructive to review some of the Court’s comments in these cases. The following statements are excerpted from four opinions:

- “In summary, since January 15, 2009, it has finally come to light that the FISC’s authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata. This misperception by the FISC existed from the inception its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government’s submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently

---

and systemically violated that it can fairly be said that this critical element of the overall [bulk collection] regime has never functioned effectively.”27

• “The government has compounded its non-compliance with the Court’s orders by repeatedly submitting inaccurate descriptions . . . to the FISC.”28

• “[T]he NSA continues to uncover examples of systematic noncompliance.”29

• “Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures.”30

• “[U]ntil this end-to-end review is completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation . . . will be the last.”31

• “The Court is troubled that the government’s revelations regarding NSA’s acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.”32

• “The current application [for pen register/trap and trace data] . . . raises issues that are closely related to serious compliance problems that have characterized the government’s implementation of prior FISA orders.”33

• “As far as can be ascertained, the requirement was simply ignored.”34

• “Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted] . . . This overcollection . . . had occurred continuously since the initial authorization . . . .”35

• “The government has provided no comprehensive explanation of how so substantial an overcollection occurred.”36

• “[G]iven the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary fact that the NSA’s end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively.”37

• “The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government’s poor track record with bulk PR/TT acquisition . . . presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve.”38

• “As noted above, NSA’s record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States

27 In re Production of Tangible Things from [Redacted], No. BR 08-13, at 10-11 (FISA Ct. Mar. 2, 2009).
28 Id. at 6.
29 Id. at 10.
30 Id. at 15.
31 Id. at 16.
34 Id. at 19.
35 Id. at 20.
36 Id. at 21.
37 Id. at 22.
38 Id. at 77.
person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained… The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor.”39

- “Given NSA’s longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information.”40

- “[The] cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance.”41

- “The Court was extremely concerned about these additional instances of non-compliance.”42

- “Perhaps more disturbing and disappointing than the NSA’s failure to purge this information for more than four years, was the government’s failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information . . . .”43

It is unclear whether these failures occurred because the NSA was not putting sufficient effort into compliance, because the NSA lacked the technical capability to ensure consistent compliance, or some other reason. Whatever the explanation, the fact that the agency’s many failures to honor privacy protections were inadvertent is of limited comfort when the NSA is asking Congress and the American public to entrust it with extensive amounts of private data.

B. Chilling Effect

When Americans are aware that intelligence agencies are collecting large amounts of their data (and not just the data of suspected criminals and terrorists), it creates a measurable chilling effect on free expression and communication. After Edward Snowden’s revelations in June 2013, an analysis of Google Trends data showed a significant five percent drop in U.S.-based searches for government-sensitive terms (e.g., “dirty bomb” or “CIA”). A control list of popular search terms or other types of sensitive terms (such as “abortion”) did not show the same change.44 In 2013, PEN America surveyed 528 American writers to learn how the disclosures affected their behavior. Twenty-eight percent reported curtailing social media activities; 24 percent avoided certain topics by phone or email; 16 percent chose not to write or speak on a certain topic; and 16 percent avoided Internet searches or website visits on controversial or suspicious topics.45 These kinds of self-censorship are inimical to the robust exchange of ideas necessary for a healthy democracy.

39 Id. at 95.
40 Id. at 115.
41 [Redacted], at 48-49 (FISA Ct. Nov. 6, 2015), available at www.dni.gov%2Ffiles%2Fdocuments%2F20151106-702Mem_Opinion_Order_for_Public_Release.pdf&t=MDM3MGZmYiY1ZWQ5YjUvMTQ5ZiQ1ZTA0ZDExNjY2NWU0ZTE1ZWNJNxaRjRYlRaQg%3D%3D.
42 Id. at 50.
43 Id. at 58.
C. Risk of Data Theft

Any massive government database containing sensitive information about Americans also raises concerns about data theft. The disastrous attack on the Office of Personnel Management’s database, in which personal data concerning more than 21 million current and former federal employees was stolen (ostensibly by the Chinese government), illustrated how vulnerable government databases are.46 More recently, hackers published contact information for 20,000 FBI employees and 10,000 Department of Homeland Security employees that they may have obtained by hacking into a Department of Justice database.47 The broad scope of Section 702 data makes it an attractive target for hacking, and its inclusion of large amounts of information about presumptively innocent Americans increases the harm that would be caused by such an event.

D. Economic Consequences

Another important concern is the negative impact of Section 702 collection on the U.S. technology industry. After Snowden’s disclosures revealed the extent of NSA collection, American technology companies reported declining sales overseas and lost business opportunities. In a survey of 300 British and Canadian businesses, 25 percent of respondents indicated they were moving their data outside of the U.S.48 An August 2013 study by the Information Technology and Innovation Foundation estimated that the revelations could cost the American cloud computing industry $22 to $35 billion over the coming years, representing a 10-20% loss of the foreign market share to European or Asian competitors.49 Another analyst found this estimate to be low, and predicted a loss to U.S. companies as high as $180 billion.50

The economic news went from bad to worse in late 2015, when the Court of Justice of the European Union (CJEU) invalidated the “Safe Harbor” agreement – an agreement between the United States and the European Union (EU), in place since 2000, governing how U.S. companies must handle information transferred from Europe. The court held that EU law requires U.S. companies to give the data a level of protection that is essentially equivalent to the protections under EU law. Citing U.S. authorities’ broad access to data held by U.S. companies under Section 702, the CJEU found that the data was insufficiently protected. Although the U.S. and

---

the European Commission have devised a new agreement, known as the “Privacy Shield,” a group of European Data Protection Commissioners have expressed concern over its adequacy.51

In the absence of Section 702 reform, it appears likely that the Privacy Shield will ultimately be invalidated by the CJEU or potentially even by the European Commission itself (which can suspend the agreement unilaterally). Experts believe this would deal a massive economic blow to U.S. companies and could undermine the very structure of the Internet, which requires free data flow across borders. In the meantime, the legal limbo in which U.S. companies find themselves constrains their ability to pursue business opportunities in Europe.

E. Potential National Security Harms

Last but clearly not least, there is a risk to national security in acquiring too much data. While computers can glean relationships and flag anomalies, they cannot replace human analysis, and human beings have limited capacity. When they are presented with an excess of data, real threats can get lost in the noise. This is not merely a theoretical concern. After the intelligence community failed to intercept the so-called “underwear bomber” (the suicide bomber who nearly brought down a plane to Detroit on Christmas Day 2009), an official White House review observed that a significant amount of critical information was available to the intelligence agencies but was “embedded in a large volume of other data.”52 Similarly, the independent investigation of the FBI’s role in the shootings by U.S. Army Major Nidal Hasan at Fort Hood concluded that the “crushing volume” of information was one of the factors that hampered accurate analysis prior to the attack.53

Whatever threat information may exist amidst the 250 million Internet communications acquired yearly under Section 702, there is surely a large amount of chaff. Because this may make it more difficult to find the threats, it is important for lawmakers to examine whether the current scope of Section 702 collection may be too broad from a security standpoint as well as a privacy one.

IV. Minimization and Its Loopholes

Legal and policy defenses of Section 702 surveillance rely heavily on the existence of minimization procedures to mitigate the effects of “incidental” collection. The concept behind minimization is fairly simple: The interception of Americans’ communications when targeting


foreigners is inevitable, but because such interception ordinarily would require a warrant or individual FISA order, incidentally collected U.S. person information generally should not be kept, shared, or used, subject to narrow exceptions.

The statutory language, however, is much more complex. It requires the government to adopt minimization procedures, which it defines as procedures “that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” The statute also prohibits disseminating non-foreign intelligence information in a way that identifies U.S. persons unless their identity is necessary to understand foreign intelligence information or assess its importance. The one caveat is that the procedures must “allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.”

The lack of specificity in this definition, and the tension between its general rule and its caveat, has allowed the government to craft rules that are permissive and contain multiple exceptions. To begin with, the NSA may share raw data with the FBI and CIA. All three agencies generally may keep unreviewed raw data – including data about U.S. persons – for five years after the certification expires; they also can seek extensions from a high-level official, and the 5-year limit does not apply to encrypted communications (which are becoming increasingly common among ordinary users of mobile devices) or communications “reasonably believed to contain secret meaning.” The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.

54 50 U.S.C. § 1801(h).
57 PCLOB 702 REPORT, supra note 5, at 60.
58 NSA 702 MINIMIZATION PROCEDURES, supra note 55, at § 6(a)(1)(a); CIA 702 MINIMIZATION PROCEDURES, supra note 56, at § 3.c.
59 NSA 702 MINIMIZATION PROCEDURES, supra note 55, at § 6(a); FBI 702 MINIMIZATION PROCEDURES, supra note 56, at § III.G; CIA 702 MINIMIZATION PROCEDURES, supra note 56, at §§ 3.a, 7.d.
If the NSA discovers U.S. person data that has no foreign intelligence value and contains no evidence of a crime, the agency is supposed to purge the data. The NSA, however, interprets this requirement to apply only if the NSA analyst determines “not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need.” This is an impossibly high bar, and so, “in practice, this requirement rarely results in actual purging of data.”

The FBI and the CIA have no affirmative requirement to purge irrelevant U.S. person data on detection, relying instead on age-off requirements. Moreover, if the FBI reviews information containing U.S. person information and makes no determination regarding whether it is foreign intelligence information or evidence of a crime, the 5-year limit evaporates, and the FBI may keep the data for a longer period of time that remains classified.

If any of the three agencies – all of which have access to raw data – disseminate information to other agencies, they must first obscure the identity of the U.S. person; but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person’s identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.

In short, the NSA routinely shares raw Section 702 data with the FBI and CIA; and the agencies’ minimization procedures suggest that U.S. person information is almost always kept for at least five years and, in many circumstances, much longer. The sharing and retention of U.S. person information are not unrestricted, but it is a stretch to say that they are “minimized” under any common sense understanding of the term.

V. Back Door Searches

Perhaps the most problematic aspect of the minimization procedures is that they allow all three agencies to query Section 702 data using U.S. person identifiers, with the express goal of retrieving and analyzing Americans’ communications.

If the government wishes to obtain an American’s communications for foreign intelligence purposes, it must secure an individual court order from the FISA Court after demonstrating that the target is an agent of a foreign power. If the government wishes to obtain an American’s communications for law enforcement purposes, it must get a warrant from a neutral magistrate. To ensure that Section 702 is not used to avoid these requirements, the statute contains a prohibition on “reverse targeting” – i.e., targeting a foreigner overseas when the government’s intent is to target “a particular, known person reasonably believed to be in the

---

60 NSA 702 MINIMIZATION PROCEDURES, supra note 55, at §§ 3(b)(1), 3(c).
61 PCLOB 702 REPORT, supra note 5, at 62.
62 Id.
63 FBI 702 MINIMIZATION PROCEDURES, supra note 56, at § III.G.1.b.
64 Id. at § 5.A-B; NSA 702 MINIMIZATION PROCEDURES, supra note 55, at § 6(b); CIA 702 MINIMIZATION PROCEDURES, supra note 56, at §§ 5, 7.d.
65 NSA 702 MINIMIZATION PROCEDURES, supra note 55, at § 3(b)(5); FBI 702 MINIMIZATION PROCEDURES, supra note 56, at § III.L; CIA 702 MINIMIZATION PROCEDURES, supra note 56, at § 4.
United States.” Before conducting Section 702 surveillance, the government must certify that it does not intend to target specific, known Americans.

And yet, immediately upon obtaining the data, all three agencies may sort through it looking for the communications of “particular, known” Americans – the very people in whom the government just disclaimed any interest. Worse, even though the FBI would be required to obtain a warrant in order to access Americans’ communications absent a significant foreign intelligence purpose, the FBI may search the Section 702 data for Americans’ communications to use in criminal proceedings having no foreign intelligence dimensions whatsoever.66 This is a bait and switch that is utterly inconsistent with the spirit, if not the letter, of the prohibition on reverse targeting. It also creates a massive end run around the Fourth Amendment’s warrant requirement.

Some have defended these “back door searches,” claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose. Whatever truth that may have in other contexts, it is manifestly not correct in the case of Section 702. Congress required agencies to “minimize” information about U.S. persons; the very meaning of “minimization” is that agencies may not use the information for any purpose they wish.

Moreover, as a constitutional matter, Judge Bates of the FISA Court has made clear that “the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information.”67 In cases involving the foreign intelligence exception to the warrant requirement, the reasonableness of a surveillance scheme turns on weighing the government’s national security interest against the privacy intrusion. While the surveillance scheme should be evaluated as a whole, it is difficult to see how any scheme could pass the reasonableness test if a significant component of the scheme were not justified by any national security interest.68

Compounding the constitutional harm, the government has not fully and consistently complied with its statutory and constitutional obligation to notify criminal defendants when it uses evidence “obtained or derived from” Section 702 surveillance. Before 2013, the government interpreted “obtained or derived from” so narrowly that it notified no one. In the three years since the government’s approach reportedly changed,69 the government has notified only seven defendants, even though the Privacy and Civil Liberties Oversight Board (PCLOB) reports that the FBI searches Section 702 every time it conducts a national security investigation70 and there

---

68 This is one of several errors, in my view, in the recent FISA Court decision upholding the constitutionality of back door searches. See Elizabeth Goitein, The FBI’s Warrantless Surveillance Back Door Just Opened a Little Wider, JUST SEC. (Apr. 21, 2016), https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/.
70 PCLOB 702 REPORT, supra note 5, at 59.
have several hundred terrorism and national security convictions during this time.\textsuperscript{71} There is reason for concern that the government is avoiding its notification requirements by engaging in “parallel construction” – i.e., recreating the Section 702 evidence using less controversial means.\textsuperscript{72} Attorneys have asked the Department of Justice to share its policies for determining when information is considered to be “derived from” Section 702, but the Department refuses to provide them.

Importantly, opposition to warrantless searches for U.S. person information is not a call to re-build the barriers to cooperation among agencies often attributed to “the wall.” Threat information, including threat information that focuses on U.S. persons, can and should be shared among agencies when identified, and the agencies should work together as necessary in addressing the threat. What the Fourth Amendment cannot tolerate is the government collecting information without a warrant with the intent of mining it for use in ordinary criminal cases against Americans. That is why President Obama’s Review Group on Intelligence and Communications Technologies – a five-person panel including a former acting director of the CIA (Michael J. Morell) and chief counterterrorism advisor to President George W. Bush (Richard A. Clarke) – unanimously recommended closing the “back door search” loophole by prohibiting searches for Americans’ communications without a warrant.\textsuperscript{73}

VI. Foreign Nationals and Human Rights Risks

Section 702 surveillance also raises concerns about the privacy and human rights of foreign nationals who are not foreign powers, agents of foreign powers, or affiliated with terrorism. While the Fourth Amendment may not extend rights to these individuals, the right to privacy is a fundamental human right recognized under international law – including treaties, such as the International Covenant on Civil and Political Rights, that the U.S. has signed. In Presidential Policy Directive 28 (PPD-28), President Obama acknowledged that “all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and . . . all persons have legitimate privacy interests in the handling of their personal information.”\textsuperscript{74}

PPD-28 requires agencies to extend certain privacy protections to foreign nationals when conducting electronic surveillance. Most notably, personal information of non-U.S. persons may be retained or disseminated only if retention and sharing would be permitted for “comparable information concerning U.S. persons.”\textsuperscript{75} This is a significant change. However, it does not

\textsuperscript{71} DEPT OF JUSTICE, UNITED STATES ATTORNEYS’ ANNUAL STATISTICAL REPORT FISCAL YEAR 2015 at 14; DEPT OF JUSTICE, UNITED STATES ATTORNEYS’ ANNUAL STATISTICAL REPORT FISCAL YEAR 2014 at 12; DEPT OF JUSTICE, UNITED STATES ATTORNEYS’ ANNUAL STATISTICAL REPORT FISCAL YEAR 2013 at 60.
\textsuperscript{75} Id. at § 4(a)(i).
prevent the acquisition of information about foreign nationals who pose no threat to the United States. Moreover, as noted above, the limits on retention and sharing of U.S. person information are not particularly strict, and it remains to be seen whether and how the agencies incorporated PPD-28’s requirement of “comparability” in their 2015 minimization procedures (which have not been declassified).

A particular concern relates to the sharing of Section 702 information with foreign governments. Agencies have significant leeway to share foreign intelligence information, as long as the sharing is consistent with U.S. law, clearly in the national interest, and “intended for a specific purpose and generally limited in duration.”\(^76\) Although the agency should have “confidence” that the information “is not likely to be used by the recipient in an unlawful manner or in a manner harmful to U.S. interests,”\(^77\) there is no express requirement or mechanism to ensure that governments with poor or spotty human rights records will not use the information to facilitate human rights violations – for instance, to harass or persecute journalists, political dissidents, human rights activists, and other vulnerable groups whose communications may have been caught up in the Section 702 collection.\(^78\)

VII. Must We Leave Section 702 in Its Current Form?

Having discussed the concerns surrounding Section 702 surveillance, it is important to address the arguments that have been put forward for its necessity. These arguments have varying degrees of merit, but none of them forecloses the possibility of reforms.

A. Restoring FISA’s Original Intent?

Executive branch officials have argued that Section 702 was necessary to restore the original intent behind FISA, which was being subverted by changes in communications technology. These officials note that FISA in 1978 required the government to obtain an individual court order when collecting any communications involving Americans that traveled by wire, but required an individual court order to obtain satellite communications only when all of the communicants were inside the U.S. Asserting that “‘wire’ technology was the norm for domestic calls,”\(^79\) while “almost all transoceanic communications into and out of the United States were carried by satellite, which qualified as ‘radio’ (vs. ‘wire’) communications,”\(^80\) they infer that Congress intended to require the government to obtain an order when acquiring purely


\(^{80}\) Statement of Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Department of Justice, before the House Permanent Select Committee on Intelligence at 4 (Sept. 6, 2007).
domestic communications, but not when obtaining communications between foreign targets and Americans. This intent was undermined when fiber-optic cables later became the standard method of transmission for international calls.

The problem with this theory is two-fold. First, it would have been quite simple for Congress to state that FISA orders were required for purely domestic communications and not for international ones. Instead, Congress produced an elaborate, multi-part definition of “electronic surveillance” that relied on particular technologies rather than the domestic versus international nature of the communication. Second, it is not correct that “almost all” international communications were carried by satellite; the available evidence indicates that one third to one half of international communications were carried by wire.81

A more plausible explanation for the original FISA’s complex scheme – one with much stronger support in the legislative history – was put forward by David Kris, a former head of the Justice Department’s National Security Division. Mr. Kris concluded that Congress intended to require a court order for international wire communications obtained in the U.S., and that the purpose behind its definitional acrobatics was to leave legislation covering surveillance conducted outside the U.S. and NSA satellite surveillance for another day.82 Although Congress never followed up, the legislative history of FISA made clear that the gaps in the statute’s coverage of NSA’s operations “should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans.”83

A related argument in support of Section 702 is that certain purely foreign-to-foreign communications, which Congress never intended to regulate, now travel through the United States in ways that bring them within FISA’s scope. In practice, this appears to be a fairly discrete (albeit thorny) problem that applies to one category of communication: e-mails between foreigners that are stored on U.S. servers.84 Section 702, however, goes far beyond what would be necessary to solve that problem. Moreover, there is a flip side to this issue: changes in technology have also caused certain purely domestic communications to travel outside the U.S. in ways that remove them from FISA’s scope. Purely domestic communications once traveled on copper wires inside the U.S., and FISA thus required a court order to obtain them. Today, digital data may be routed anywhere in the world – and U.S. Internet Service Providers may store domestic communications on overseas servers – rendering these communications vulnerable to...
surveillance under Executive Order 12333, which has far fewer safeguards. Any legislation that attempts to solve the former problem should address the latter one as well.

B. Thwarting Terrorist Plots

Executive officials have stated, and the PCLOB and the president’s Review Group on Intelligence and Communications Technologies have found, that Section 702 surveillance played a role in detecting and thwarting a number of terrorist plots. That is, after all, the most important function the statute is intended to serve; if it did not accomplish this goal, it presumably should go the way of the now-discontinued Section 215 bulk collection program, which, by most reliable reports, added little counterterrorism value.

Whether Section 702 is useful is thus a question of critical importance. It is not, however, the only question that must be answered. There is also the question of whether effective surveillance could be conducted in a manner that entails less intrusion on the privacy of law-abiding Americans and foreigners. Indeed, in the few cases that have been made public – including those of Najibullah Zazi, Khalid Ouazzani, David Headley, Agron Hasbajrami, and Jamshid Muhtorov – it appears that the targets of the Section 702 surveillance were known or suspected to have terrorist affiliations. These cases therefore do not support, for example, the idea that the NSA needs the ability to target any foreigner overseas.

We must also ask whether the costs to our liberties are too high. It is commonly said that if terrorists succeed in undermining our values, they win. But while this notion is often invoked, it is also often forgotten. The United States was founded on a set of core principles, and none of these was more important than the right of the citizens to be free from undue intrusions by the government on their privacy. Our Constitution promises us that law-abiding citizens will be left alone. It is incumbent upon us as a nation to find ways of addressing the terrorist threat that do not betray this promise.

VIII. Who Decides? – The Need for Transparency

Within constitutional bounds set by our nation’s courts, it is up to the American people – speaking through their representatives in Congress – to decide how much surveillance is too much. But they cannot do this without sufficient information.

While a significant amount of information about Section 702 has been declassified in recent years, critical information remains unavailable. For instance, the certifications setting forth the categories of foreign intelligence the government seeks to collect – but not the

85 Goitein & Patel, supra note 2, at 19-20; Toh et al., supra note 78, at 8-10.
individual targets – have not been released, even in redacted form. Unlike the NSA and the CIA, the FBI does not track or report how many times it uses U.S. person identifiers to query databases containing Section 702 data. The list of crimes for which Section 702 data may be used as evidence has not been disclosed. Nor have the policies governing when evidence used in legal proceedings is considered to be “derived from” Section 702 surveillance. The length of time that the FBI may retain data that has been reviewed but whose value has not been determined remains secret.

Perhaps most strikingly, despite multiple requests from lawmakers dating back several years, the NSA has yet to disclose an estimate of how many Americans’ communications are collected under Section 702. The NSA has previously stated that generating an estimate would itself violate Americans’ privacy, ostensibly because it might involve reviewing communications that would otherwise not be reviewed. In October of last year, a coalition of more than thirty advocacy groups – including many of the nation’s most prominent privacy organizations – sent a letter to the Director of National Intelligence urging that the NSA go forward with producing an estimate.88 The letter noted that, as long as proper safeguards were in place, the result would be a net gain for privacy. Recently, a bipartisan group of fourteen House Judiciary Committee members sent the DNI a letter making the same request.89

This basic information is necessary for Americans to evaluate the impact of Section 702 on their privacy. It is also necessary because most Americans are not lawyers, and when they hear that a surveillance program is “targeted” only at foreigners overseas and that any acquisition of Americans’ communications is “incidental,” they may reasonably assume that there is very little collection of their own calls and e-mails. An estimate of how many communications involving Americans are collected would help to pierce the legalese and give Americans a truer sense of what the program entails.

In short, Section 702 is a public statute that is subject to the democratic process, and the democratic process cannot work when Americans and lawmakers lack critical information. More transparency is urgently needed so that the country can begin an informed public debate about the future of foreign intelligence surveillance.

Thank you again for this opportunity to testify.

---

Tab 5
§ 1. Definitions

(a) “Classified information”, as used in this Act, means any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)).

(b) “National security”, as used in this Act, means the national defense and foreign relations of the United States.

CREDIT(S)

§ 2. Pretrial conference

Currentness

At any time after the filing of the indictment or information, any party may move for a pretrial conference to consider matters relating to classified information that may arise in connection with the prosecution. Following such motion, or on its own motion, the court shall promptly hold a pretrial conference to establish the timing of requests for discovery, the provision of notice required by section 5 of this Act, and the initiation of the procedure established by section 6 of this Act. In addition, at the pretrial conference the court may consider any matters which relate to classified information or which may promote a fair and expeditious trial. No admission made by the defendant or by any attorney for the defendant at such a conference may be used against the defendant unless the admission is in writing and is signed by the defendant and by the attorney for the defendant.

CREDIT(S)


Notes of Decisions (1)

Classified Information Procedures Act, § 2, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 2
Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States.

CREDIT(S)

§ 4. Discovery of classified information by defendants

The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.

CREDIT(S)


Notes of Decisions (10)

Classified Information Procedures Act, § 4, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 4
§ 5. Notice of defendant's intention to disclose classified information, 18 USCA APP. 3 § 5

(a) Notice by defendant

If a defendant reasonably expects to disclose or to cause the disclosure of classified information in any manner in connection with any trial or pretrial proceeding involving the criminal prosecution of such defendant, the defendant shall, within the time specified by the court or, where no time is specified, within thirty days prior to trial, notify the attorney for the United States and the court in writing. Such notice shall include a brief description of the classified information. Whenever a defendant learns of additional classified information he reasonably expects to disclose at any such proceeding, he shall notify the attorney for the United States and the court in writing as soon as possible thereafter and shall include a brief description of the classified information. No defendant shall disclose any information known or believed to be classified in connection with a trial or pretrial proceeding until notice has been given under this subsection and until the United States has been afforded a reasonable opportunity to seek a determination pursuant to the procedure set forth in section 6 of this Act, and until the time for the United States to appeal such determination under section 7 has expired or any appeal under section 7 by the United States is decided.

(b) Failure to comply

If the defendant fails to comply with the requirements of subsection (a) the court may preclude disclosure of any classified information not made the subject of notification and may prohibit the examination by the defendant of any witness with respect to any such information.

CREDIT(S)


Notes of Decisions (14)

Classified Information Procedures Act, § 5, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 5
§ 6. Procedure for cases involving classified information, 18 USCA APP. 3 § 6

(a) Motion for hearing

Within the time specified by the court for the filing of a motion under this section, the United States may request the court to conduct a hearing to make all determinations concerning the use, relevance, or admissibility of classified information that would otherwise be made during the trial or pretrial proceeding. Upon such a request, the court shall conduct such a hearing. Any hearing held pursuant to this subsection (or any portion of such hearing specified in the request of the Attorney General) shall be held in camera if the Attorney General certifies to the court in such petition that a public proceeding may result in the disclosure of classified information. As to each item of classified information, the court shall set forth in writing the basis for its determination. Where the United States' motion under this subsection is filed prior to the trial or pretrial proceeding, the court shall rule prior to the commencement of the relevant proceeding.

(b) Notice

(1) Before any hearing is conducted pursuant to a request by the United States under subsection (a), the United States shall provide the defendant with notice of the classified information that is at issue. Such notice shall identify the specific classified information at issue whenever that information previously has been made available to the defendant by the United States. When the United States has not previously made the information available to the defendant in connection with the case, the information may be described by generic category, in such form as the court may approve, rather than by identification of the specific information of concern to the United States.

(2) Whenever the United States requests a hearing under subsection (a), the court, upon request of the defendant, may order the United States to provide the defendant, prior to trial, such details as to the portion of the indictment or information at issue in the hearing as are needed to give the defendant fair notice to prepare for the hearing.

(c) Alternative procedure for disclosure of classified information

(1) Upon any determination by the court authorizing the disclosure of specific classified information under the procedures established by this section, the United States may move that, in lieu of the disclosure of such specific classified information, the court order--

(A) the substitution for such classified information of a statement admitting relevant facts that the specific classified information would tend to prove; or
(B) the substitution for such classified information of a summary of the specific classified information.

The court shall grant such a motion of the United States if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information. The court shall hold a hearing on any motion under this section. Any such hearing shall be held in camera at the request of the Attorney General.

(2) The United States may, in connection with a motion under paragraph (1), submit to the court an affidavit of the Attorney General certifying that disclosure of classified information would cause identifiable damage to the national security of the United States and explaining the basis for the classification of such information. If so requested by the United States, the court shall examine such affidavit in camera and ex parte.

(d) Sealing of records of in camera hearings

If at the close of an in camera hearing under this Act (or any portion of a hearing under this Act that is held in camera) the court determines that the classified information at issue may not be disclosed or elicited at the trial or pretrial proceeding, the record of such in camera hearing shall be sealed and preserved by the court for use in the event of an appeal. The defendant may seek reconsideration of the court's determination prior to or during trial.

(e) Prohibition on disclosure of classified information by defendant, relief for defendant when United States opposes disclosure

(1) Whenever the court denies a motion by the United States that it issue an order under subsection (c) and the United States files with the court an affidavit of the Attorney General objecting to disclosure of the classified information at issue, the court shall order that the defendant not disclose or cause the disclosure of such information.

(2) Whenever a defendant is prevented by an order under paragraph (1) from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment or information; except that, when the court determines that the interests of justice would not be served by dismissal of the indictment or information, the court shall order such other action, in lieu of dismissing the indictment or information, as the court determines is appropriate. Such action may include, but need not be limited to--

(A) dismissing specified counts of the indictment or information;

(B) finding against the United States on any issue as to which the excluded classified information relates; or

(C) striking or precluding all or part of the testimony of a witness.

An order under this paragraph shall not take effect until the court has afforded the United States an opportunity to appeal such order under section 7, and thereafter to withdraw its objection to the disclosure of the classified information at issue.
(f) Reciprocity

Whenever the court determines pursuant to subsection (a) that classified information may be disclosed in connection with a trial or pretrial proceeding, the court shall, unless the interests of fairness do not so require, order the United States to provide the defendant with the information it expects to use to rebut the classified information. The court may place the United States under a continuing duty to disclose such rebuttal information. If the United States fails to comply with its obligation under this subsection, the court may exclude any evidence not made the subject of a required disclosure and may prohibit the examination by the United States of any witness with respect to such information.

CREDIT(S)


Notes of Decisions (42)

Classified Information Procedures Act, § 6, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 6

§ 7. Interlocutory appeal, 18 USCA APP. 3 § 7

United States Code Annotated
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Appendix 3. Classified Information Procedures Act (Refs & Annos)

Classified Information Procedures Act, § 7, 18 U.S.C.A. App. 3

§ 7. Interlocutory appeal

Effective: December 1, 2009

Currentness

(a) An interlocutory appeal by the United States taken before or after the defendant has been placed in jeopardy shall lie to a court of appeals from a decision or order of a district court in a criminal case authorizing the disclosure of classified information, imposing sanctions for nondisclosure of classified information, or refusing a protective order sought by the United States to prevent the disclosure of classified information.

(b) An appeal taken pursuant to this section either before or during trial shall be expedited by the court of appeals. Prior to trial, an appeal shall be taken within fourteen days after the decision or order appealed from and the trial shall not commence until the appeal is resolved. If an appeal is taken during trial, the trial court shall adjourn the trial until the appeal is resolved and the court of appeals (1) shall hear argument on such appeal within four days of the adjournment of the trial, excluding intermediate weekends and holidays, (2) may dispense with written briefs other than the supporting materials previously submitted to the trial court, (3) shall render its decision within four days of argument on appeal, excluding intermediate weekends and holidays, and (4) may dispense with the issuance of a written opinion in rendering its decision. Such appeal and decision shall not affect the right of the defendant, in a subsequent appeal from a judgment of conviction, to claim as error reversal by the trial court on remand of a ruling appealed from during trial.

CREDIT(S)


Notes of Decisions (3)

Classified Information Procedures Act, § 7, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 7
§ 8. Introduction of classified information, 18 USCA APP. 3 § 8

(a) Classification status

Writings, recordings, and photographs containing classified information may be admitted into evidence without change in their classification status.

(b) Precautions by court

The court, in order to prevent unnecessary disclosure of classified information involved in any criminal proceeding, may order admission into evidence of only part of a writing, recording, or photograph, or may order admission into evidence of the whole writing, recording, or photograph with excision of some or all of the classified information contained therein, unless the whole ought in fairness be considered.

(c) Taking of testimony

During the examination of a witness in any criminal proceeding, the United States may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible. Following such an objection, the court shall take such suitable action to determine whether the response is admissible as will safeguard against the compromise of any classified information. Such action may include requiring the United States to provide the court with a proffer of the witness’ response to the question or line of inquiry and requiring the defendant to provide the court with a proffer of the nature of the information he seeks to elicit.

CREDIT(S)

§ 9. Security procedures, 18 USCA APP. 3 § 9

Effective: April 21, 2005

Currentness

(a) Within one hundred and twenty days of the date of the enactment of this Act, the Chief Justice of the United States, in consultation with the Attorney General, the Director of National Intelligence, and the Secretary of Defense, shall prescribe rules establishing procedures for the protection against unauthorized disclosure of any classified information in the custody of the United States district courts, courts of appeal, or Supreme Court. Such rules, and any changes in such rules, shall be submitted to the appropriate committees of Congress and shall become effective forty-five days after such submission.

(b) Until such time as rules under subsection (a) first become effective, the Federal courts shall in each case involving classified information adopt procedures to protect against the unauthorized disclosure of such information.

CREDIT(S)


Notes of Decisions (5)

Classified Information Procedures Act, § 9, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 9

End of Document
§ 9A. Coordination requirements relating to the prosecution of cases involving classified information

Effective: March 9, 2006

(a) Briefings required.--The Assistant Attorney General for the Criminal Division or the Assistant Attorney General for National Security, as appropriate, and the appropriate United States attorney, or the designee of such officials, shall provide briefings to the senior agency official, or the designee of such official, with respect to any case involving classified information that originated in the agency of such senior agency official.

(b) Timing of briefings.--Briefings under subsection (a) with respect to a case shall occur--

(1) as soon as practicable after the Department of Justice and the United States attorney concerned determine that a prosecution or potential prosecution could result; and

(2) at such other times thereafter as are necessary to keep the senior agency official concerned fully and currently informed of the status of the prosecution.

(c) Senior agency official defined.--In this section, the term “senior agency official” has the meaning given that term in section 1.1 of Executive Order No. 12958.

CREDIT(S)


Classified Information Procedures Act, § 9a, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 9a
§ 10. Identification of information related to national defense, 18 USCA APP. 3 § 10

In any prosecution in which the United States must establish that material relates to the national defense or constitutes classified information, the United States shall notify the defendant, within the time before trial specified by the court, of the portions of the material that it reasonably expects to rely upon to establish the national defense or classified information element of the offense.

CREDIT(S)


Notes of Decisions (1)

Classified Information Procedures Act, § 10, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 10
Classified Information Procedures Act, § 11, 18 U.S.C.A. App. 3

§ 11. Amendments to Act

Currentness

Sections 1 through 10 of this Act may be amended as provided in section 2076, Title 28, United States Code.

CREDIT(S)


Classified Information Procedures Act, § 11, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 11
§ 12. Attorney General guidelines, 18 USCA APP. 3 § 12

United States Code Annotated
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Appendix 3. Classified Information Procedures Act (Refs & Annos)

Classified Information Procedures Act, § 12, 18 U.S.C.A. App. 3

§ 12. Attorney General guidelines

Currentness

(a) Within one hundred and eighty days of enactment of this Act, the Attorney General shall issue guidelines specifying the factors to be used by the Department of Justice in rendering a decision whether to prosecute a violation of Federal law in which, in the judgment of the Attorney General, there is a possibility that classified information will be revealed. Such guidelines shall be transmitted to the appropriate committees of Congress.

(b) When the Department of Justice decides not to prosecute a violation of Federal law pursuant to subsection (a), an appropriate official of the Department of Justice shall prepare written findings detailing the reasons for the decision not to prosecute. The findings shall include--

1. the intelligence information which the Department of Justice officials believe might be disclosed,

2. the purpose for which the information might be disclosed,

3. the probability that the information would be disclosed, and

4. the possible consequences such disclosure would have on the national security.

CREDIT(S)


Classified Information Procedures Act, § 12, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 12
§ 13. Reports to Congress, 18 USCA APP. 3 § 13

Effective: November 27, 2002

(a) Consistent with applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches, the Attorney General shall report orally or in writing semiannually to the Permanent Select Committee on Intelligence of the United States House of Representatives, the Select Committee on Intelligence of the United States Senate, and the chairman and ranking minority members of the Committees on the Judiciary of the Senate and House of Representatives on all cases where a decision not to prosecute a violation of Federal law pursuant to section 12(a) has been made.

(b) In the case of the semiannual reports (whether oral or written) required to be submitted under subsection (a) to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, the submittal dates for such reports shall be as provided in section 507 of the National Security Act of 1947.

(c) The Attorney General shall deliver to the appropriate committees of Congress a report concerning the operation and effectiveness of this Act and including suggested amendments to this Act. For the first three years this Act is in effect, there shall be a report each year. After three years, such reports shall be delivered as necessary.

CREDIT(S)


Classified Information Procedures Act, § 13, 18 U.S.C. App. 3
§ 14. Functions of Attorney General exercised by Deputy Attorney General, the Associate Attorney General, or designated Assistant Attorney General

Currentness

The functions and duties of the Attorney General under this Act may be exercised by the Deputy Attorney General, the Associate Attorney General, or by an Assistant Attorney General designated by the Attorney General for such purpose and may not be delegated to any other official.

CREDIT(S)


Classified Information Procedures Act, § 14, 18 U.S.C.A. App. 3, 18 USCA APP. 3 § 14
§ 15. Effective date

Currentness

The provisions of this Act shall become effective upon the date of the enactment of this Act, but shall not apply to any prosecution in which an indictment or information was filed before such date.

CREDIT(S)

§ 16. Short title, 18 USCA APP. 3 § 16

That this Act may be cited as the “Classified Information Procedures Act”.

CREDIT(S)