SURVEILLANCE AND TRANSPARENCY

by
Valerie Caproni[*]

In this Article, the General Counsel for the Federal Bureau of Investigation provides a practical perspective on issues of national security surveillance and the use of national security letters. The author begins by setting forth a primer on national security surveillance. Next, she contrasts the procedural standards and execution methods of FISA surveillance with Title III surveillance. The author then discusses the changes in the FBI's national security electronic surveillance practices since 9/11.

In the final part of the Article, the author describes the FBI's use of national security letters (NSLs), a somewhat controversial non-surveillance national security tool, and addresses recent critiques of the Bureau's use of NSLs. While acknowledging that more work can be done, the author notes how the FBI has already improved its use of NSLs through increased training and education of its agents. The author concludes the article by stressing the importance of NSLs, and cautioning that future restrictions on the FBI's capacity to obtain documents though NSLs could significantly harm the Bureau's ability to fulfill its mission of keeping the nation safe.

Well, it is getting late and we have heard a lot today.[1] We started out with Kelly Moore,[2] who presented a very practical approach to how we deal with the threat of terrorism: criminal law versus other alternatives. And now at the end of the day we are going to come back to practicalities, because I am not an academician.

What I will do is follow on what Bill Funk[3] has said and discuss the practicalities of all of this. How does this work in reality, in what the FBI does on a day in and day out basis? In that regard, the name of this panel is interesting: "Surveillance and Transparency." In the national security arena, that is an odd title because most of the surveillance work we do is

[*] General Counsel, Federal Bureau of Investigation (2003 to present).

[1] This Article began as a transcription of the author's presentation at Lewis & Clark Law School's spring symposium on "Crimes, War Crimes, and the War on Terror." Comments of Valerie Caproni, FBI Chief Counsel, Lewis & Clark Law School Symposium on "Crimes, War Crimes, and the War on Terror" (Apr. 20, 2007), *available at* http://lawlib.lclark.edu/podcast/?p=203.

[2] Kelly Moore, *The Role of Federal Criminal Prosecutions in the War on Terrorism*, 11 LEWIS & CLARK L. REV. 837 (2007).

[3] William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma—A History*, 11 LEWIS & CLARK L. REV. 1099 (2007).

not transparent at all. It is, in fact, classified. And so talking about specifics is not possible; in fact, it would be unlawful. We will start one step earlier than where we are now, with a short primer on the national security tools that FBI agents have in their toolbox.

The first tool is old-fashioned physical surveillance: we can direct agents or surveillance teams to follow somebody. Maybe that somebody is an intelligence officer (IO) who is in the United States from Pakistan or Israel or wherever. The agents are directed to simply follow the IO around and see who the IO meets with, to see where the IO goes. We could even install a camera so long as it is only "looking" in public areas. That sort of surveillance does not require a court order because it does not intrude into areas as to which there is a reasonable expectation of privacy. It might feel a little creepy to have somebody following you around all the time, but it does not violate the Fourth Amendment, and no court authorization is required (so long as our camera stays focused in public areas). But that does not mean there are no restraints on the Bureau. As a matter of policy, there are restraints, because it is creepy to have someone following you around. For that reason, there has to be some level of predication before an agent is authorized to engage in physical surveillance for any sort of extended period.

So now I will talk about electronic surveillance. In the national security area, the Foreign Intelligence Surveillance Act (FISA)[4] is the way to go. FISA actually authorizes a number of different types of electronic surveillance. First, it authorizes pen registers and trap and trace devices.[5] Remember this from criminal procedure: a pen register/trap and trace device is a device that tells you both the incoming and outgoing numbers dialed or pulsed from a telephone. Back in the old days, this was a big deal. Now everybody has caller ID on their phones, so it does not seem so magical. There was a time when it was practically magical that you could get trap and trace information. Although such a device does not collect the content of the call, as a matter of statute, we are required to have an order. So we can get a FISA order for a pen register and trap and trace device, although the standard is a little lower than it is to get full content.

We can also get electronic surveillance of content. We can collect content on almost anything: it can be on a cell phone; it can be on a land line telephone; it can be on a fax machine; it can be on a computer. Anything that sends or receives electronic messages can be subject to a full content FISA order. And we can also do what are called physical searches.[6] A physical search can be both what you might think of as a physical search—meaning we go into a house and we take pictures of everything that is there—we can take pictures of every piece of paper that

[4] Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95- 511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–63 (2000)).

[5] 50 U.S.C. § 1842 (2000).

[6] 50 U.S.C. § 1822 (2000).

is on the desk, pictures of a Rolodex, etc. Or it can be an electronic physical search. So if there is a hard drive for a computer, that computer may get mirrored. That is, we will essentially take an electronic picture of the inside of the computer. That technique is viewed to be a physical search. It requires a court order because we are intruding into an area as to which there is a constitutionally protected expectation of privacy.

For each of those three techniques—pen registers, content collection, and physical search—the FBI needs a court order, assuming the collection is taking place in the United States. The CIA and the NSA may do things overseas with no court order, but they are subject to their own authorities. The FBI in the United States needs a court order to conduct that sort of surveillance. These orders are obtained from the FISA court, the so-called "secret court." I remember before I went to work for the FBI, I was fascinated by this notion of a secret court. How do you have a secret court? Where is it? What does it do? And sure enough, there is a secret court. The court has a little room; it has a big thick door on it. You go in, they close the door, and it's secret.

The Court is currently located within the Justice Department's building, which is a little quirky. And I remember when there was the appeal that Bill Funk mentioned, the ACLU wanted to file an amicus brief.[7] The question was, "Where do you file papers with a secret court?" But just so everybody understands, the secret court—as odd as that concept may seem—is drawn from regular old run-of-the-mill Article III judges who are selected to serve on the FISA court. During the period of time that they serve on the FISA court, they continue to do their normal Article III work, so these people actually have incredibly difficult jobs. It is a huge burden; and the judges on the FISA court work incredibly hard.

Now Bill Funk indicated that FISA has a "lower standard."[8] I have always quarreled with the notion that FISA has a lower standard. There is no question that it has a different standard. But as a practical matter, I would not say that FISA has a lower standard. To obtain a court order under FISA, we have to show that there is probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power.[9] An international terrorism group qualifies as a foreign power.[10] And we have to show that the target is using, has used, or is about to use the facility that is going to be tapped or searched.[11] That is the basic standard, which is a little different from a Title III standard, and we'll talk

[7] Comments of Bill Funk, Lewis & Clark Law School Symposium on "Crimes, War Crimes, and the War on Terror" (Apr. 20, 2007), *available at* http://lawlib.lclark.edu/
podcast/?p=203 (discussing *In re Sealed Case*, 310 F.3d 717, 719 (Foreign Int. Surv. Ct. Rev. 2002)).

[8] *Id.*

[9] 50 U.S.C. § 1805(a)(3)(A) (2000).

[10] 50 U.S.C. § 1801(a)(4) (2000).

[11] 50 U.S.C. § 1805(a)(3)(B).

about Title III surveillance in a second. But the notion that FISA is "easy peasy"—that we can throw up a FISA warrant on any kind of Tom, Dick, or Harry—is just not true. There actually has to be evidence or information sufficient so the court can make the required findings. Not evidence in the sense of firsthand information, because a lot of this is based on foreign intelligence. It could be information that we have obtained from many different sources, including human sources, foreign services, or signals intelligence (SIGINT) collection by the NSA. Whatever information we have goes in the application to make a factual showing that will permit the judge—again a regular old Article III judge that we trust to make these determinations day-in and day-out—to determine that there is probable cause to believe that the person is an agent of a foreign power.

But in addition to the different standards, there are differences in how this surveillance is conducted. FISA collection is different than collection that occurs under traditional criminal law wiretaps under Title III. And there is good cause for that, because the goal of FISA surveillance—the goal and a significant purpose of it—is to collect foreign intelligence.[12] Not to say that you cannot have in mind a subsequent criminal prosecution, but a significant purpose of the surveillance has to be to collect foreign intelligence.

So now let me talk a little bit about Title III surveillance.[13] For those of you who have never prosecuted cases or never seen a criminal wiretap order, Title III surveillance is different from FISA. Title III surveillance is typically live-monitored, meaning that when we put a tap on a telephone, we have agents who are sitting there listening to that tap twenty-four hours a day. So as the phone is picked up and the telephone conversation begins, they are listening in. Typically the order will last for thirty days,[14] and the order typically includes the requirement that the government provide "ten day reports" to the court.[15] The ten day report is used to keep the judge apprised on a regular basis of what the government is collecting. The minimization occurs on the spot; "minimization" meaning that while we may be up on your telephone, we have no right to listen to (nor are we interested in) your children setting up their play dates. So those calls need to be minimized. In the Title III context, calls are minimized by literally turning the recording device off, so the irrelevant conversation is never captured. In Title III, all interceptees will eventually be notified at some point after the interception period ends. [16] And lastly, if intercepts are to be used in a criminal case, the defendant is given all of the applications, all of the

[12] 50 U.S.C. § 1804(a)(7)(B) (2000).

[13] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub.L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510–2522 (2000)).

[14] 18 U.S.C. § 2518(5) (2000).

[15] 18 U.S.C. § 2518(6).

[16] 18 U.S.C. § 2518(8)(d).

orders, and typically all of the tapes. So, essentially, the entire surveillance is turned over to the defendant and defense counsel so they can review them thoroughly and determine exactly what they are going to argue the government did wrong in order to argue that the court should suppress the fruits of the wiretap.

Under FISA, in contrast, the tape is almost never live-monitored. The tap is put on the phone, the tape runs, and no one listens to it in real time. The court order that authorizes the surveillance can last up to 90 days if the target is a U.S. person.[17] A "U.S. person" is defined as either a U.S. citizen or a green-card holder; a non-U.S. person is everybody else.[18] For a U.S. person, a court order generally lasts 90 days;[19] for a non-U.S. person, it starts at 120 days[20] and can be renewed for a full year.[21] So, FISA orders last much longer than Title III orders. FISA minimization occurs after the fact. As I indicated, we generally do not live-monitor; instead, after the fact, we have agents and analysts listen to the conversations. If a conversation is not pertinent, meaning that there is not foreign intelligence information and there is not evidence of a crime, then it is not summarized. If the conversation is foreign intelligence or evidence of a crime, then a short summary of the conversation is prepared. But we always have the full tape. So, suppose five years after we initially reviewed a conversation, we learn something new. That new information may cause us to reconsider whether conversations that we thought at the time were not pertinent (and therefore were not written up) are actually pertinent. If that occurs, we can go back and listen to the conversation again. The basic rule of whether we can write up a conversation and thereby make it accessible to all with a need to know is that it must be foreign intelligence. That is the question agents and analysts have to ask: is it or is it not foreign intelligence?

Except in very rare circumstances, FISA interceptees are never told that they have been intercepted. Before a FISA intercept can be used in a proceeding, however, the other party has to be told that the information was obtained via a FISA order. But the litigation over FISA is very different from litigation over Title III. As you will remember, in Title III litigation, the government produces to the defense the applications, the orders, and the tapes. The defense is allowed to review all the documents to their heart's delight. In FISA, that is not the case. If the Attorney General certifies that disclosure of the applications and orders would harm national security, then the litigation proceeds ex parte. So, essentially, the government gives the applications and orders to the judge and argues to the judge in the criminal case that the orders were lawfully entered and the surveillance was lawfully conducted. The judge in the

[17] 50 U.S.C. § 1805(e)(1) (2000).
[18] 50 U.S.C. § 1801(i) (2000).
[19] 50 U.S.C. § 1805(e)(1).
[20] 50 U.S.C. § 1805(e)(1)(B).
[21] 50 U.S.C. § 1805(e)(2).

criminal case rules yea or nay; yes, it is okay, or no, it is not okay. The applications and orders only get turned over to the defense if a district court determines that disclosure is necessary to make an accurate determination of the legality of the surveillance. To date that has never happened. So we have never had a situation where the FISA applications had to be turned over. That is the basic primer on national security surveillance.

What happened to national security surveillance post-9/11? First, not surprisingly I suppose, the use of FISA skyrocketed. In 2000, there were 1,005 FISA applications, all of which were granted.[22] Now that includes all types and includes renewals. So, a U.S. person FISA that is active for one year counts as four applications, because it would have an initiation and then it would have to be renewed every 90 days. In 2005, just five years later, the number of FISA orders was 2,074.[23] Our use of FISA doubled from pre-9/ll to 2005. The 2006 numbers are not yet out.[24] I do not know what that number will be as I have not yet seen the numbers. My guess is that it will be pretty much even with 2005 or down a little. I think it could be a little bit down because of the USA PATRIOT Improvement and Reauthorization Act.[25] That Act changed the rules on non-U.S. person FISAs. Such FISAs get renewed for a year, so there should be fewer of those than in years past when we had to renew them more often.[26]

So why the explosion of FISA? Is this a matter of the government in fact unduly spying on American people? Well I think there are a number of different reasons for the increase. First, the USA PATRIOT Act took down "the wall"—the artificial wall between foreign intelligence and criminal investigations that my colleague thinks is a good idea[27] and we thought was not a good idea. It is no longer necessary for FBI investigators to make a bright line determination whether the investigation is criminal or foreign intelligence. Instead, the agents can pool their information and figure out collectively from all of our

[22] Letter from John Ashcroft, Att'y Gen. of the U.S., to L. Ralph Mecham, Dir., Admin. Office of the U.S. Courts (Apr. 27, 2001), *available at* http://www.usdoj.gov/nsd/foia/reading_room/2000fisa-ltr.pdf.

[23] Letter from William E. Moschella, Assistant Att'y Gen., to L. Ralph Mecham, Dir., Admin. Office of the U.S. Courts (Apr. 28, 2006), *available at* http://www.usdoj.gov/nsd/foia/reading_room/2005fisa-ltr.pdf.

[24] Subsequent to this conference, the Department of Justice published the statistics for 2006. During 2006, the United States made 2,181 applications for authority to conduct electronic surveillance and physical searches under FISA, of which 2,176 were approved. Letter from Richard A. Hertling, Acting Assistant Att'y Gen., to Richard B. Cheney, Pres., U.S. Senate (Apr. 27, 2007), *available at* http://www.usdoj.gov/nsd/foia/reading_room/2006fisa-ltr.pdf.

[25] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub.L. No. 109-177, 120 Stat. 192 (2006).

[26] USA PATRIOT Improvement and Reauthorization Act of 2005 § 105(c) (codified at 50 U.S.C. 1842(e)(2)).

[27] Funk, *supra* note 3, at 1136–39.

information, whether gathered in the criminal context or the national security context, whether a person may be a terrorist or a spy.

Part of the reason for the increased use in FISA is purely personnel. After 9/11, the FBI moved thousands of agents who had been working traditional white-collar cases, bank robbery cases, and narcotic cases and put them to work in the national security area. So we have a lot more people conducting these investigations, and FISA is one tool in the toolbox. Part of the reason for the increase in the use of FISA is that we have greatly improved our information sharing within the U.S. government. So between the Bureau, the CIA, and NSA, and also with foreign governments, we are cooperating much more in terms of information sharing. As information comes into the Bureau, it is not unusual for us to conclude that FISA is the right tool to use to determine whether this individual, who is in the United States, has a corrupt relationship with a person in another country who is being controlled by that other country's intelligence service or by an international terrorist group.

What else has changed since 9/11? The Attorney General Guidelines that govern our conduct were changed. The guidelines now say to our agents: "We want you to use all of the tools in the toolbox—we don't want you to have an artificial distinction between criminal tools and national security tools."[28] Sometimes FISA is the right way to go, because it gives us time to determine the full scope of a terrorist's network. FISA is really designed for that: for the government to gather intelligence. But maybe as we are ascertaining the full scope of the network, we realize that there is some piece of it that needs to be immediately incapacitated. As Kelly Moore was talking about this morning,[29] when that happens, we need to be able to pull that person out, incapacitate him or maybe even persuade him, through the coercive effect of a potential criminal indictment, to cooperate with us. We want to be able to do all of that without compromising or taking down foreign intelligence collection if we are still benefiting from that collection. So what we are telling agents now is that they have to think outside of rigid parameters of criminal versus national security. They need to combine those two constructs and ask themselves: "What is the right way to protect American people?" Sometimes that means using both sets of tools. While I think people can quarrel about whether the law needed to be changed to accomplish that goal, as a practical matter a change in the law was required. Pre-9/11 it was almost impossible for agents working on a national security investigation that was using FISA to share the information they were

[28] *See* U.S. Att'y Gen., The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (Oct. 31, 2003) *available at* http://www.usdoj.gov/olp/nsiguidelines.pdf (unclassified version).

[29] Moore, *supra* note 2, at 838–40; Comments of Kelly Moore, Lewis & Clark Law School Symposium on "Crimes, War Crimes, and the War on Terror" (Apr. 20, 2007), *available at* http://lawlib.lclark.edu/podcast/?p=199.

collecting with criminal agents. That inability to share made it more difficult for us to arrest the person and charge him criminally, because the two sets of agents could not share information back and forth.

That has changed. There is now ample sharing of information, and we can now readily use criminal charges to incapacitate people from doing harm and to improve our human intelligence cadre. So is all of that a good thing? I think it is. I think it is a good thing for the safety and security of America. Are there civil liberties concerns? There absolutely are. There is no doubt that there are civil liberties concerns that come with the explosive use of a tool like FISA. FISA is the most intrusive tool that we have. It should be used sparingly, and it should be used only when it is necessary. In part, resource constraints help to ensure that. Because what we learned very quickly is that we cannot have every agent who is working counter-terrorism say, "I want a FISA," because that level of demand simply crashes the system. We do not have enough lawyers, we do not have enough translators, and we do not have enough agents to do that. So there had to be some level of prioritization of the work that we were doing. And that happened.

It took a while post-9/11 for us to figure out that we could not actually give FISA coverage to every agent that wanted it, but we have now figured that out. We have internal processes in place to make sure that the cases that need FISA get it and that long-running FISAs are being maintained for good reasons. We do not want agents to go up on a group that they are investigating and then keep the FISA up gathering intelligence just for the sake of gathering intelligence. We are looking at the long-running FISAs and saying, "What is your plan? Where are you going with this?" So as a matter of internal policies, we are putting constraints on long-running electronic surveillances.

That is an overview of the world of electronic surveillance, at least from my perspective in terms of what the FBI is doing. When I asked Professor John Kroger what I was supposed to talk about here, he said, "Talk about electronic surveillance, and you might want to talk about national security letters, because they've been in the press a lot." So, while they are not surveillance, let me give you the five-minute version of why you should not believe everything you read in the paper about national security letters.

First, what is a national security letter? Essentially, a national security letter is an administrative subpoena. It is an administrative subpoena that can be used to obtain only very limited classes of records. We can obtain phone records, that is subscriber information and also what we used to call toll billing information or long distance records. We can obtain electronic communication records that would cover internet usage, not content—just the facts of who owns the account and pen register-type data (who the account has had contact with). We can obtain financial records, credit card records and bank records, and we can obtain credit reports. We cannot obtain any other type of record with a national security letter. Notwithstanding what you read in the paper or hear from

your friends at the ACLU, we cannot obtain library records, we cannot obtain tax records, we cannot obtain health records, and we cannot obtain school records with a national security letter. National security letters are limited to the very specific types of records I have just listed for you.[30] As with FISA though, the use of national security letters has mushroomed since 9/11. And all the factors that we have talked about before are the reasons for that increase. We have a lot more people working counterterrorism now, and this is a tool that is available in counterterrorism cases.

The USA PATRIOT Act[31] changed the national security letter statutes in two ways. Prior to the change in the law, we had to show specific facts that would lead the person issuing the national security letter to conclude that the person about whom we were getting the records was a terrorist or a spy. So, you had to already know that the target was a bad guy before you could get the records that would facilitate making that determination. Put differently, the statute put the cart before horse, and it never made a lot of sense. That standard was changed by the USA PATRIOT Act to a requirement that the records sought simply need to be relevant to a national security investigation.[32] So the records we seek to obtain with a national security letter must be relevant to a national security investigation. The second change made by the Patriot Act was to the identity of authorized issuers.[33] Before the USA PATRIOT Act, all national security letters had to come to FBI Headquarters and be signed by a high ranking individual. The USA PATRIOT Act changed that so now the special agent in charge of the field office can sign a national security letter.[34] Special Agents in Charge are high-ranking officials, but devolving signing authority into the field made the process far more efficient.

The Department of Justice Inspector General (IG) was mandated by Congress as part of the USA PATRIOT Improvement and Reauthorization Act of 2005 to audit the FBI's use of national security letters.[35] The law mandated two audits. One was to cover the period from 2003 to 2005, and we are going to have the joy of seeing yet another report from him at the end of this year, because the law also mandates an audit for 2006. I will tell you now that you will see the same problems discussed in the 2006 audit that were discussed in the audit of 2003 to

[30] OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS, at xi–xiv (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf.

[31] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 365 (codified at 18 U.S.C § 2709).

[32] USA PATRIOT Act § 505 (codified at 18 U.S.C. § 2709).

[33] *Id.*

[34] *Id.*

[35] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 119, 120 Stat. 192, 219 (2006).

2005, because, of course, we have not had an opportunity to fix those problems yet. The IG found essentially three problems with our use of national security letters.

First, a single unit in headquarters used what we call "exigent letters" to short-circuit the national security letter process.[36] The employees in that unit would simply give the telephone company a letter that said, in essence, "There is an emergency. I will give you a grand jury subpoena in the future. You give me the records now." There were two problems with that process. First, there was not always an emergency, although frequently there was. And second, they were generally not following the exigent letters with grand jury subpoenas; they were generally following them with national security letters, although sometimes no process at all followed. The IG found the process of getting a record with the promise of future coercive process to be objectionable. From my perspective, if it really was an emergency, then we are entitled under the Electronic Communications Privacy Act[37] to obtain the records with no process. Ultimately providing process, to me, seems like belts and suspenders. But nonetheless the IG objected to the practice so we have now barred it. But, in the case of an emergency, we can obtain these records without any legal process. Our process now is to give the telephone company a letter that says, in substance, "There is an emergency. The emergency is X. If you agree X is an emergency, then you can give me the records." The phone company has to agree under the statute. Section 2702 of Title 18 provides the statutory authority under which a phone company can give us records with no process. So we have responded to that finding from the IG. We do not let our agents short circuit the national security letter process except in cases of true emergency, and the letter has now been changed to make it very clear to the telephone company that any production of documents is voluntary on its part.

The second issue that the IG raised was with our Congressional reporting of national security letters.[38] He is quite correct that our Congressional reporting numbers were off. Our current system is a "fat finger system"; it is slightly better than the 3x5 card system that the current system replaced, but it is not an electronic system. To make a long story short, we have a lot of human errors involved in tabulating the numbers we are required to report to Congress. While we are incredibly embarrassed that the numbers we have historically reported are not entirely accurate, from an oversight perspective, we believe that the numbers we reported were not off by an order of magnitude. So for example, if we have reported that there were about 40,000 national security letters used in a year, the number is likely to be higher than that. The actual number may be 50,000, but it will not be 400,000. So, from an

[36] OFFICE OF THE INSPECTOR GEN., *supra* note 30, at 87–89.

[37] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. § 2518(7)).

[38] OFFICE OF THE INSPECTOR GEN., *supra* note 30, at 31–36.

oversight perspective, I think that Congress in fact was informed of the basic order of magnitude of our use of this tool. Having said that, we are in the process of developing an entirely automated system for preparing national security letters that will automatically capture the numbers we are required to report to Congress. That system should alleviate all of the errors in our Congressional reporting and many of the administrative errors the IG found in the national security letters he examined.

And the final issued raised by the IG related to unreported intelligence oversight board violations.[39] In the world of national security, there is an executive order that requires the intelligence community to self report any violation of law or policy committed during the course of a national security investigation.[40] These reports are made to the President's Intelligence Oversight Board. To fulfill that obligation, as a matter of FBI policy, we tell our employees that when they find that they have made a mistake and gathered information wrongfully, they must report it to the Office of General Counsel as a potential intelligence oversight board violation. In the IG's review of national security letters, he looked at 293 national security letters and reported that he found 22 potential intelligence oversight board violations that had never been reported.[41] Twenty-two out of 293 is a lot. We required the field to report all 22 that the IG had identified to the Office of General Counsel. As it turned out, there were actually only 5 (roughly 1.5% of the total) that really were intelligence oversight board violations. Even 1.5% is too high an error rate, but it is not a 10% error rate, and it definitely is not a 22% error rate, which was one of the headlines that was in the report.

We can do better. We have done a lot of work, and we are doing a lot of work in terms of training our agents and educating our agents to make sure that they understand the rules, including what they can do and what they cannot do. But this is an important tool to us. We were not happy about this report, and some in Congress are threatening to restrict our ability to obtain documents through national security letters. From our perspective, restricting this valuable tool would cause real harm to our ability to achieve our mission, which is to keep the country safe.

---

[39] *Id.* at 67–85.

[40] Exec. Order No. 12,334, 46 Fed. Reg. 235 (Dec. 8, 1981); Exec. Order No. 12,863, 58 Fed. Reg. 177 (Sept. 15, 1993).

[41] OFFICE OF THE INSPECTOR GEN., *supra* note 30, at 78.