INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

The Foreign Intelligence Surveillance Act
James A. Baker

Guest Presentations, Spring 2007
William G. Boykin, Richard J. Danzig, James A. Baker, Warren G. Lavey, John D. Bansemer, Michael J. Sulick, Robert A. Fein, Darryl R. Williams, Rob Johnston

September 2007

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-98-4 **I-07-1**

The Foreign Intelligence Surveillance Act

James A. Baker

March 1, 2007

James A. Baker, Esq., is counsel for intelligence policy at the U.S. Justice Department. Prior to joining the Justice Department's Office of Intelligence Policy and Review he served as a federal prosecutor handling numerous international white collar crimes for the department's Criminal Division. He is a fellow of the Institute of Politics at Harvard University's John F. Kennedy School of Government, and is currently teaching at the Harvard Law School. Mr. Baker received his undergraduate degree from the University of Notre Dame and his J.D. and M.A. from the University of Michigan.

Oettinger: It's a particular pleasure to introduce Jim Baker, who is counsel at the Justice Department and is deeply involved in making difficult decisions about privacy, information security, et cetera. That's what he's come to talk to us about.

Baker: Thank you. I appreciate the opportunity to come here and talk to you. Obviously I'm here to answer whatever questions I can possibly answer, but I thought that today it might be helpful for me to talk a little bit about the Foreign Intelligence Surveillance Act, or FISA, which is something I'm very familiar with.[1] I'll first explain what our office does, and then talk about FISA. That will lead to a quick overview of the NSA [National Security Agency] surveillance program. Then we'll see how much time we have left. If you have questions at any point during the presentation, go ahead and ask them. If I'm going to cover something later on I'll just say so, but that way I won't be trying to backtrack.

FISA was enacted in 1978. Let me talk first about the scope of the coverage of the act. There are really four parts to the act. One is the original part of the act, as enacted in 1978. It covers electronic surveillance. "Electronic surveillance" is a term that is defined in the statute. For those of you who are interested and want to look it up, the statute is Title 50 of the U.S. Code, sections 1801 through 1871. Those are the basic sections of the federal code.

"Electronic surveillance," as defined in the act, covers, in essence, more or less what you would think. It covers wire communications surveillance, radio communication surveillance, a variety of types of monitoring (such as a microphone in a room), and any surveillance that is targeted at a particular known U.S. person who is in the United States. So if you're intentionally targeting an American in the United States, then FISA applies. It does not apply to electronic

---

[1] The text of the FISA is available on-line at http://uscode.house.gov/download/pls/50C36.txt.

surveillance conducted outside the United States and not directed at people inside the United States. Any collection outside the United States that is directed at foreigners who are also outside the United States is not going to be covered under FISA. Congress thought about that in 1978, and decided that it was too difficult to try to draft an order or warrant requirement for that type of surveillance, so they didn't do it. That is handled outside of FISA.

Student: Then why is it called the *Foreign* Intelligence Surveillance Act? Can it be against U.S. citizens, or only foreign nationals?

Baker: It can be targeted at both. I'll talk about that in a second. It's foreign in the sense that it's distinguished from domestic. The idea is that domestic intelligence would be intelligence about groups operating inside the United States with no foreign connections. Without getting too much into the weeds here, that would mean if you were targeting surveillance, for example, against a Timothy McVeigh and his cohorts. They were domestic terrorists who blew up the Federal Building in Oklahoma City in 1995. There's no foreign connection there.

"Foreign intelligence" is a term that is also defined in the statute. It has to do with the activities of foreign governments, foreign powers, and their agents. I'll come back and describe those a bit more. The reason is that in the Constitution, in the Fourth Amendment, a different standard applies with respect to the types of activities that the government can engage in when it's dealing with the activities of foreign powers as opposed to ordinary crime control or domestic intelligence for internal security. That's why FISA is in that sense limited in its scope: it's intended to collect foreign intelligence information.

In addition to electronic surveillance, FISA covers physical searches inside the United States. Those are amendments that were adopted in 1994 following the investigation of Aldrich Ames. In connection with that, the attorney general of the United States, at the time Janet Reno, had authorized searches of Ames's residence and other property without a warrant. There were some concerns about what the courts would say about that, because it was a personal residence inside the United States, so the administration and Congress enacted a provision in 1994 to cover physical searches in the United States. These are physical searches that are conducted surreptitiously, for the most part, so without the knowledge of the target. There's no requirement to notify the target, unlike a criminal search warrant, where as a general matter you knock, you announce you're coming in, you do your search, and you leave a copy of the warrant and a listing of what items were seized. There are some exceptions to that. With FISA, by and large, these searches are conducted surreptitiously, so that ideally the subject of the search never knows that we've been there.

Student: Did Janet Reno not want to take it to the court because of worries about possible leaks?

Baker: No. There was no mechanism to take it to the FISA Court in 1993/1994, before these amendments were passed. There were concerns that a court in which Ames was being prosecuted might say "The government doesn't have the authority under the Constitution to do this kind of search without a warrant." I'm not sure that's a position that the Department of Justice would agree with today, but that was the concern at the time. Given the stakes and the importance of the Aldrich Ames case, it was not a case that you want to lose in court based on evidence being

suppressed. That was one of the motivating factors to encourage the Congress and the administration to seek amendments to FISA at that time.

FISA also covers, in different provisions, collection done using pen registers and trap-and-trace devices. A pen register is a device that records outgoing phone calls. Let's say you dial a number from your phone; this device will record in real time what number you're dialing. A trap-and-trace device is just the opposite: it's like Caller ID. It will record the incoming calls. It does not record the substantive content of the call—the spoken words—just the dialing information. Full content can be obtained under a different standard, and I'll try to talk about that in a few minutes.

In addition, there is a provision of FISA that was enacted in 1998 and amended in Section 215 of the Patriot Act. This provision allows the government to go to the FISA Court to obtain orders authorizing the collection of certain business records and other tangible things. It's sometimes referred to as the "library provision." It was quite controversial after the Patriot Act was enacted. There were certain amendments made to that provision in light of those concerns in the legislation that reauthorized the Patriot Act about a year and a half ago. We'll talk more about that if we have time.

So that's basically the scope of FISA.

The basic idea is that FISA is constitutional because it comports with the reasonableness clause of the Fourth Amendment, which says "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…." The courts have said that FISA is constitutional because the searches that it authorizes are reasonable.

There has been no exact decision on this, but there is an argument that FISA orders, FISA authorizations, also comply with the warrant clause of the Fourth Amendment, which says that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." So of the two parts of the Fourth Amendment, FISA is clearly constitutional under the reasonableness clause and the orders that are issued might also constitute actual warrants under the warrant clause of the Fourth Amendment.

The basic purpose of FISA, dating back to 1978, was to do two things at the same time: protect the security of Americans and, simultaneously, protect Americans from abuses by intelligence agencies. It was enacted following a number of disclosures, basically in the 1970s, regarding abuses of national security authorities by various and sundry intelligence agencies. I don't know if you've looked at the Church Committee reports in this course. For example, there were instances where the FBI [Federal Bureau of Investigation] was conducting electronic surveillance of Dr. Martin Luther King, Jr., as part of an investigation based upon information that he had associates who were members of the Communist Party of the United States. The investigation originally focused on collecting information about that, but then it became focused on discrediting Dr. King, in part because of his Communist Party connections, indirect though they may have been. It involved electronic surveillance of him to collect very personal information. It was intended only to collect very personal information; it wasn't intended at that

point to collect information about his interactions with anybody who was connected with the Communist Party. These recordings and the information from them were disseminated widely within and outside the U.S. government, including sending Dr. King a tape recording of one of his interactions with someone, along with a threatening letter. King assessed that it was a veiled threat that he should commit suicide or risk being exposed publicly. The FBI intended it "merely" to prompt a rift between King and his wife that would cause them to be divorced, which would lower his standing in the civil rights community. It was a very lengthy investigation that involved many other things, I'm sorry to tell you. That was one of the things that Congress was concerned about.

Another program that Congress was concerned about was something called Operation Shamrock, which was an NSA program that started in 1945 and continued until about 1973. It involved the collection of all or most outgoing international telegrams—telegrams going from the United States to foreign countries. At the end, it involved collection of about 150,000 telegrams per month. Back in the old days that was the way you communicated overseas quickly; there was no email. There was no attempt to try to reduce, or minimize, the collection of irrelevant information about U.S. persons, so all of that was collected. In addition, as part of Operation Shamrock, the communications of certain Americans were targeted, sometimes on the basis of their First Amendment activities: antiwar protestors, civil rights activists. That information was targeted and pulled out of these cables and collected. Congress was concerned about that, and that's why they put into FISA a variety of different procedures to ensure accountability within the executive branch, define the terms under which you could be an authorized target of surveillance, and provide certain mechanisms of oversight for such activities.

It's focused on protecting the privacy and security of Americans, but "Americans" is not really the term. In the statute it's "U.S. persons." A "U.S. person" includes a citizen, a permanent resident alien, a U.S. association, or a U.S. corporation. U.S. persons receive a higher degree of protection under the statute; for example, with regard to some of the definitions used in the act, and in terms of the minimization of communications collected to, from, or about Americans. "Minimizing" means we have to reduce to the extent practicable the amount of information we collect about Americans, the amount we retain, and the amount we disseminate.

There's a limitation with regard to targeting Americans. You cannot be targeted solely upon the basis of your First Amendment-protected activities. That's not permissible any more. The FISA Court, which I'll talk about in a bit here, reviews the applications that we file under a higher standard when it comes to Americans.

Oettinger: On the warrant side of the Fourth Amendment the term "probable cause" implies that something is known about something undesirable having been committed. That strikes me as something that is very relevant to criminal justice, but on intelligence matters you're more concerned with preventing something from happening than with discerning probable cause. I'm wondering whether that issue is one that the Congress has faced openly.

Baker: I think that was part of the debate that went on last summer. Congress considered and indeed the House passed a significant series of amendments to FISA, changing the definition of electronic surveillance with the idea of carving out certain types of collection from the definition

of FISA. That in a sense would have freed the government to collect that kind of information outside of FISA, without going through the FISA Court process. That is exactly what some of the folks were talking about.

As the Supreme Court has made clear, "probable cause" is a fluid concept and it's not reducible to a mathematical formula or to a percentage. It's intended to be a flexible, sort of practical kind of standard. It doesn't mean "no information whatsoever," but it means the kind of information that a reasonable and prudent person would rely on to take appropriate action. But you're right: in terms of collecting information there's a difference between probable cause and relevance. There's a lot of information that might be relevant to an investigation that you have to sort through to determine whether there is a higher probability that somebody's a bad guy, basically. The standard in FISA for full content collection is probable cause.

Student: If someone under surveillance under FISA then does something unrelated—say, he admits to cheating on his taxes on the telephone, or that he killed his wife—and this has nothing to do with international terrorism, would that be admissible in court? Would the court then call for a regular domestic warrant, or could they use that evidence in court?

Baker: You can use the evidence directly from the FISA. Congress made clear that if you collected this other type of information—it was lawfully obtained, and you didn't know you were going to obtain that when you got it—it can be used.

There was a famous case a number of years ago, I think in Missouri, where someone was under surveillance for totally different reasons. The husband was the target. The husband and the wife were in the United States. They were concerned that their daughter was becoming too Westernized, and this was a subject of discussion over a long period of time. What they ended up doing to solve their problem was to murder her, and the murder was recorded by a concealed microphone in the residence. That information was obviously given to the local authorities and they were prosecuted for murder. The information was used and everybody knew it was from FISA. That's what Congress intended when it enacted FISA.

If you're conducting electronic surveillance of Aldrich Ames, let's say, and you obtain information about his dealings with the Soviets, or the Russians, you can use that kind of information to prosecute him for espionage. It's connected closely to his intelligence activities. But then if you found that he was doing something else, some kind of an ordinary crime—fraud, a crime of violence, child pornography—if you obtained it lawfully pursuant to FISA you can use it in a criminal case.

To go back to your earlier question, there are only two types of targets under FISA: foreign powers and agents of foreign powers. That's it. Those terms are defined in the statute. Foreign powers include sort of what you would think of: foreign governments, foreign political organizations, factions of foreign nations (such as the PLO [Palestine Liberation Organization], for example), or international terrorist groups. They don't have to be on any particular list, or be designated by the secretary of state or anybody else as a terrorist group. If they meet the definition of foreign power under the statute they can qualify. It could be a group as small as two people, as long as they are engaged in activities that fall under the definition of international

terrorism. So it provides a significant amount of flexibility to the government to deal with new and emerging threats in that regard.

Foreign powers can also be entities that are directed and controlled by one or more foreign governments. A national airline, if it is directed and controlled by a foreign government, could be seen as a legitimate foreign power.

The definition of "agents of foreign powers" breaks up into two parts: one that involves non-U.S. persons, and one that involves any person. Non-U.S. persons can be targeted solely on the basis of their status. They could be obeying all the laws of the United States, yet if they're officers or employees of a foreign government, including foreign diplomats, they can be targeted merely on that basis. They don't have to be doing anything illegal. They don't have to be engaged in espionage; they can have paid all their parking tickets and otherwise be behaving lawfully, and yet their mere status would enable us to target them.

When it comes to U.S. persons it's a different standard. There's a requirement that they be knowingly engaged in certain activities that at least may involve a violation of the criminal laws of the United States. They could be clandestine intelligence gathering activities; other clandestine intelligence activities; activities that constitute international terrorism or activities in preparation therefor; aiding, abetting, or conspiring with people in connection with those types of activities; or knowingly using false documents to enter the United States or using false or fraudulent documents within the United States at the behest of a foreign power. All of those activities qualify you as an agent of a foreign power, even if you are an American citizen or a permanent resident alien.

Again, the two things about that are that there's a "knowing" requirement: you have to know what you're doing. If you're an innocent dupe that's not going to cut it. There also has to be this nexus to a violation of the criminal law. You cannot, as I say, target domestic groups or persons who aren't connected to a foreign power.

Student: You say a higher standard applies in terms of intent. Could I get a FISA warrant through to try to determine that intent and then later find out what was going on?

Baker: It's "knowingly engaged in clandestine intelligence activities that involve or may involve a violation of criminal laws." You don't have to have proof to a certainty that it involves a violation; it *may* involve it. With respect to "knowingly" it's the same thing: you have to establish probable cause. Again, this is a flexible standard. It changes depending upon the circumstances. You look at the information that you have, whatever the facts are, and then you are allowed to draw reasonable inferences from those facts. If those reasonable inferences lead to a conclusion that there's a fair probability, based on the totality of the circumstances, that the person may be involved in a violation of criminal law and in clandestine intelligence gathering, that's it. So, on the one hand it's a defined set of terms, a defined standard, and yet built within it is flexibility.

Oettinger: There's a kind of bootstrapping penalty that's implied in the question. At some point, in order to get probable cause, can you do that without being in violation of the law?

Baker: Sure. You could obtain telephone records, which are not protected by the Fourth Amendment. You could interview witnesses and sources. There's no Fourth Amendment protection there either. There are other standards or parts of law that apply here. You can do physical surveillance of someone: watch what they're doing. You can obtain other types of records. You can do searches for publicly available documents.

Oettinger: So you can get there by other means.

Baker: The key thing is that FISA is an investigative tool. It's not an investigation. You do lots of different types of things in order to build your investigation and then, when you have enough information—and that can be very early, or even immediately in some instances, you use this highly intrusive technique. That's the idea. So, if you have enough facts to start out with you can go to it right away, but you have to get the facts from somewhere and have a basis to start this type of surveillance.

Student: You mentioned diplomats. What about embassies?

Baker: The standard is that you can target what is referred to as a "foreign power establishment," and that's premises or property that's under the exclusive and open control of a foreign government. If you have such a physical facility it can be targeted under FISA.

Student: What about the United Nations?

Baker: I'm not going to comment on any particular target. We "neither confirm nor deny" that we're targeting anybody; that is our basic standard response. If the United Nations would fall within the definition of a foreign power or agent of a foreign power, then in theory you could target it.

Student: Under the definition of foreign power, you mentioned the PLO as a faction. Does that mean that any foreign political party could be targeted?

Baker: Yes, any foreign political organization not substantially composed of U.S. persons.

Student: How about nongovernmental organizations?

Baker: You'd have to show that they fit one of these definitions. Is it a foreign government, or a component of a foreign government? Is it a foreign political organization, or is it an entity that is directed or controlled—either openly or covertly—by a foreign government or governments? You'd need some facts to establish that the organization would meet one of those standards.

Student: In answering the earlier question you said "foreign property." That covers embassies. Could you tap a diplomat's home if he just lived in Manhattan or wherever?

Baker: Let me give you the full answer here. The standard under FISA for full content collection, meaning the substance of all the communications, is probable cause. Even though a FISA order might not be a warrant, nevertheless, built within FISA is the probable cause standard, and that's in part what makes it reasonable.

The FISA Court has to find the following with regard to using the standard of probable cause. It has to find probable cause to believe that the target is a foreign power or an agent of a foreign power. With respect to electronic surveillance, the court also has to find probable cause "that the facilities or places at which the surveillance is directed are being used or are about to be used by a foreign power or an agent of a foreign power." So you have to show probable cause that the target is a foreign power or an agent, such as an officer or an employee of a foreign power, and that the places or facilities subject to surveillance are being used by an agent of a foreign power; again, an officer or an employee of a foreign government. That's enough. You've met those two parts of the standard. So, if somebody has an apartment or a house somewhere, then you have to establish probable cause that that person is an agent of a foreign power and is using it or is about to use it.

Student: You included national airlines, or is that a separate category?

Baker: That's an entity directed or controlled by a foreign government. It's the same thing: you have to establish probable cause that this facility or that place is being used or is about to be used by that entity.

For physical search you have to show probable cause to believe that the premises or property to be searched is owned, used, possessed by, or in transit to or from a foreign power or an agent of a foreign power. So it covers a lot of stuff. It's geared more toward physical searches.

That's the standard for full content collection. The standard under FISA for non-full content collection—that's the pen registers, the trap-and-trace devices, and the orders for obtaining other kinds of records that I mentioned earlier—is, in essence, relevance. The information sought has to be relevant to an appropriate investigation, to obtain foreign intelligence information or protect against international terrorism or clandestine intelligence activities. So it's clearly a lower standard. The basic idea there, according to the statute, is that the information sought has to have some pertinence to the ongoing investigation. It's information that's going to be helpful to the investigation in some way. It can't be just random, irrelevant, spurious information. This lower standard applies to material that's not protected by the Fourth Amendment. In particular, it's the dialing data that you voluntarily share with the telephone company, or any type of business records where you're engaged in a transaction, where the government is not intercepting those communications as they're going by, but rather they're going, let's say, to some kind of establishment and getting the financial records or other kinds of records.

These business record applications—Section 215 applications—are made by the FBI director or by his designee. Our office files them. There's a relevance test. You can obtain any physical thing—documents, records, whatever—that you could obtain with a grand jury subpoena or some other kind of a court order.

There is another limitation with respect to this part of FISA that says that you cannot obtain this type of information when an investigation is based solely on First Amendment-protected activities. There is also a requirement for minimization procedures to reduce the amount of irrelevant information you obtain. Under the most recent amendments, someone who receives one of these orders can consult with an attorney and can challenge the order in court.

Before I talk about the FISA Court, let me back up and talk about my office. Probably I should have talked about it at the start, but it fits in here. My office, the Office of Intelligence Policy and Review [OIPR], is part of the National Security Division of the Department of Justice. The National Security Division was created last year, so it's a relatively recent creation. It consists of OIPR, as well as two parts of the department that came from the Criminal Division: the Counterespionage Section and the Counterterrorism Section.

Oettinger: Is that where Mo [Maureen] Baginski came from?

Baker: No, she was in the FBI. She was across the street.[2]

Our office receives requests from intelligence agencies—meaning the FBI and the NSA—to file applications with the FISA Court on their behalf. The requests come in; we review them to ensure they meet the requirements of the statute, prepare the applications, and take the applications to the appropriate official who is going to certify them. Each application must have a certification as part of the accountability requirement. We get them signed by the director of the FBI, the secretary of defense, the director of national intelligence, the secretary of state, or the national security advisor, but principally it's the director of the FBI or the secretary of defense or the deputy secretary of defense. Then the attorney general signs each one. We file approximately 2,000 a year, or roughly 50 a week, so it's a fair number of cases. We're quite busy tracking down these certifying officials and the attorney general. Then we file them with the FISA Court.

The FISA Court consists of eleven sitting federal district court judges, so they sit in their normal duty as regular district court judges. There's one judge from the District of Massachusetts, for example. There's a schedule for their appearing—being the duty judge in that sense. They fly down to Washington on Monday, hear all the cases that week, and fly back on Friday. They're busy enough that they're pretty much just doing FISA work when they're down there. There are three local judges by statute, so if there are emergencies or things over the weekend you can always get to a judge.

The judges are selected by the chief justice of the United States. They are appointed for terms of up to seven years, and then they go back to their regular duties.

Each application is heard by a single judge, so even though there are eleven judges on the court only one judge is reviewing an application at any particular time. This is exactly the same thing that happens with respect to an application in a criminal context to conduct electronic surveillance, to do a wiretap. Given the volume, the FISA Court is hearing cases nearly every day, including on weekends. Should there be an appeal—and there's only been one appeal in almost thirty years—it goes to something called the Foreign Intelligence Surveillance Court of Review, which consists of three appellate court judges who, again, have been selected by the chief justice. They've only heard one case, which was a few years ago, and that had to do with the wall between intelligence and law enforcement. That's a subject for a different day; we could be here for hours on that alone, but I'd be happy to come back if you want to talk about that at some point.

---

[2] FBI Headquarters is located across Pennsylvania Avenue from the Department of Justice in Washington, D.C.

Student: The reading that we did last week by Mark Lowenthal[3] talked about the number of cases that had come up to the FISA Court since its inception, and it was something like 4,500. Only four were rejected. Is that an accurate number, and has the proportion rejected since 9/11 changed?

Baker: The number of applications, going back to 1979, is reported publicly. It's more than 20,000 now. I would say that probably fewer than ten have been denied, and only two of those denials were ever appealed. The cases that were denied were actually approved in terms of our having probable cause and a legitimate target, but the court did not want us to use certain rules that would have allowed more information sharing and interaction with the prosecutors. So the FISA Court of Review construed that as an effective denial, even though it was approved. We nevertheless were allowed to appeal it.

Student: What does that tell us about the overall process? Are the NSA and the FBI doing their jobs, or is the court just a rubber stamp?

Baker: People ask that all the time. Here's my answer on that. Everybody does their job. The FBI and the NSA do their jobs; they submit the applications to us. We do our job: we prepare applications that we think meet the requirements of the statute. There's back and forth with the intelligence agencies over these cases. Some cases come in and they are obviously sufficient and obviously high priority. They move through the system quickly. Other cases need work. It just makes sense. So we have a back and forth with the agencies with respect to those cases. If we are satisfied we recommend to the attorney general that he or she sign the application. Then it gets filed with the FISA Court. So I think the idea is that everybody is working through the system to try to make sure that these applications meet all the requirements of the statute when they go forward.

Having said that, there is a significant amount of interaction between the government and the FISA Court. Remember: this is what we call in the law an *ex parte* proceeding, which means that there's only one side appearing before the FISA Court. There's nobody representing the target. If we present applications to the FISA Court, the court might say "We're not satisfied with this particular minimization procedure you have here. We want you to tighten that up a bit." Or they might say "We think the facts with respect to this particular issue are a little bit weak. Don't you have anything else? Can you supplement that in any way?"

Then we'll go back to the FBI field office, wherever it might be, and ask "Do you have any more facts about this particular thing?" They will say "Yes, we do." So they write it up, we attach that as an addendum, and it goes to the court. So there's never any denial there. The court has just asked for more information.

To deny a case, just practically speaking, means a lot of work, and it means a lot of work for us to appeal it. If there are cases that we can work our way through to get to where we—the

---

[3] Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: Congressional Quarterly Press, Third Edition, 2006).

executive branch—want to be, then we have this dialogue and this back and forth with the FISA Court.

In terms of the court being a rubber stamp, they have denied a certain number of cases. Whenever they deny them they set down a marker. In addition, they've modified many cases. I think that two years ago there were two denials and seventy-nine or so modifications, where we couldn't work out something with the court informally, and they still felt strongly about something, so they modified the order in some fashion.

Finally, again, when it came to this very important issue of the wall and the sharing of information, the government tried to have the court approve procedures that would have allowed a lot more sharing of information and a lot more interaction with prosecutors. The FISA Court would not go along with that post 9/11. It issued an opinion saying "No, you can't do that, for the following reasons." The government was then forced to take an appeal from that ruling. It was all seven judges (at that time there were seven judges on the court). So, on one of the most important issues to the government post 9/11, the FISA Court said "No, you're going too far." That's evidence that the FISA Court itself, now eleven judges, is not just going to go along with everything we come up with.

Student: It sounds like a very important decision. Did they basically turn that one down because they felt that it jeopardized operational security?

Baker: No, not because of that. It was a long discussion, but the basic idea was that FISA was intended primarily to obtain foreign intelligence information, and that foreign intelligence information was distinct from evidence of a crime. If your point was to obtain primarily evidence of a crime, and the prosecutors were heavily involved in the process, that was a contravention of the original statute, and they wouldn't go for it.

The FISA Court of Review said "No, that's not right. As long as the evidence you're trying to obtain is related to or part of a foreign intelligence crime, such as espionage, terrorism, or document fraud—passport fraud—in support of one of those things, and it's not ordinary crime, you can seek and obtain evidence of a crime. You also have to retain the realistic option of doing something other than just prosecuting the person, such as collecting information about their tradecraft, who their handlers are, things like that, and you can deal with the person in some other fashion. In general, as long as you meet those two requirements, you can have all this interaction with the prosecutors."

Student: Has the NSA always gone through the Department of Justice in the application process to the FISA Court?

Baker: Yes.

Student: How much did the community—the NSA and the FBI—have input to the way the new law and amendments were crafted? Are the operators satisfied with the way the laws read now that they can do what they need to do?

Baker: It depends on whom you talk to. Some operators will never be satisfied with having to go to a court, and some are totally satisfied.

One of my last points here is that FISA works. That's my statement to you. One of the things about FISA is that once you've obtained a court order to do this type of surveillance or collection everybody throughout the system is satisfied that it's being done lawfully, so there's no question about that. What it means is that the information you collect can be disseminated widely through the government and it can be used in a criminal case. You have to protect sources and methods, as we say: you don't want to reveal exactly what techniques you're using. If you obtain information from techniques and methods outside of FISA, you have to worry about what you want to disclose in a criminal case, and you have to worry sometimes about whom you're going to disseminate this information to, because it's sensitive for a lot of reasons.

The second point is that Congress was quite clear when it enacted FISA originally that it was not attempting to prohibit any type of collection. No particular surveillance technique was barred by the statute. The idea was that if you're going to conduct electronic surveillance it has to be done through the mechanism of the statute. That then leads into the NSA program, which I can comment on.

Oettinger: Even if everything is lawful, there's a question of policy and balance. One of the things that keeps recurring in what you're describing is minimization. The implication is that for reasons connected with privacy, the First Amendment, or the Fourth Amendment, you need to reduce as much as possible the amount of information kept about a particular target. Now, the pros of that are clearly evident. The con seems to be that if you're looking for patterns and you're throwing away the irrelevance and the history, you are in the worship of minimization to some extent tying one hand behind your back. To what extent is that a reasonable balancing act? If so, how much consideration is given to it? I'm puzzled by the emphasis on minimization as a built-in goal.

Baker: It's built in in the sense that it's one of the features. You could come up with some other way to make your collection reasonable, but having minimization procedures is one way that your collection activities become reasonable, because you're trying to reduce, to the extent reasonably feasible, the amount of information you collect, retain, and disseminate about U.S. persons. Indeed, the statute defines minimization, and it basically says that you have to design these procedures reasonably, on the one hand to protect privacy, and on the other hand to enable the government to obtain, produce, and disseminate foreign intelligence.

For example, in the legislative history of FISA, Congress talked about a situation where you're conducting electronic surveillance of a switchboard, because the target may work in some organization. Let's say a hundred people work there. If the target works there, and you've established probable cause that the target is using the phone in that office building somewhere, and all the calls go through the main switchboard, you can, if you have to, collect on the switchboard; that is, all the calls to and from everybody inside the organization using that switchboard. So you have to acquire all those communications. You've done the best you can. You're minimizing at the stage of acquisition, but you have to be flexible, because of the setup of the phone system and where the target is. What you do then is try to reduce how much

information you retain that's connected to all those ninety-nine other people in that office, and you only disseminate information that has to do with your actual target. That's how you boil it down. In some instances you can collect a lot of information on the front end; keep it; have it sitting there, if that's what you have to do for collection reasons, and then you winnow it down as you go through this system. It's intended to be reasonable.

Student: What happens to the information on the other ninety-nine people? Do you automatically destroy it, or is it like what we mentioned earlier: that you find out that someone targeted under FISA is committing fraud? Is that actionable, even though they weren't the original target of FISA?

Baker: Again, if you came across somebody committing fraud or some other type of crime, and you came across that information, you listened to it, and recognized for what it was, you can keep it and use it in a criminal prosecution. What happens generally to all the other material is going to be governed by the minimization procedures that are approved by the court. We come forward and we say "In this particular case we have to collect on this switchboard. Here's what we're going to do, Judge. Here's how we're going to handle this information." We have to explain to the court exactly what we're going to do. The court says "Yes, we think that's reasonable under these circumstances, so go ahead with it." That could involve destruction; it doesn't necessarily have to, because most FISA surveillance is done by recording everything, and then sorting through it later. So the privacy protection there is under FISA Court supervision.

Student: To follow up on that, if you're looking at a foreign institution, such as a business, couldn't you come across something to do with competitive advantage? For example, the government is holding on to something that's very close and dear to a manufacturing process. How is that process mitigated? It's not a civil rights issue; it's more ambiguous.

Baker: Again, you have to minimize dissemination. You can only disseminate foreign intelligence and you can only use information for lawful purposes. Handing over trade secrets to some U.S. company—is that foreign intelligence information? You'd have to make that case to the FISA Court. At the same time, if it's that kind of an organization—if we've established that it's controlled by a foreign power—the government has an interest in finding out what it's doing. Is it violating export laws, such as sneaking high-tech materials that are export controlled outside the United States? If it is, and is doing it at the behest of a foreign power, the government has an interest in obtaining that information.

Student: Does precedence play any role in FISA, in terms of making an argument for doing something on the basis of previous cases? Is that incorporated in the law at all?

Baker: Yes, it is. To the extent that there are relevant cases that happen outside FISA, we look at those, especially when the Supreme Court issues a ruling regarding what "probable cause" means, for example. But by and large, the FISA Court precedents are going to be known only to the FISA Court and to us. We're not going to be disclosing them publicly, because they're classified. The one opinion I was talking about before regarding the interaction with prosecutors was an opinion that was published. But most of their rulings are not published. They're classified, so generally

nobody can see them, other than the FISA Court and the government. But there are precedents, and it's a court like any other court in that sense.

Student: For what purposes, and using what standards, might the FISA Court publicly publish something?

Baker: You'd have to ask them why they published this one decision. It's the only published opinion of the court. It's relatively lengthy. They could publish that opinion because it had to do with a policy/legal/constitutional issue, and you could have that discussion without overly involving classified information. It wasn't really discussing a technique or a source, so you could write an opinion in a way that laid out all the issues and did not contain classified information. So I think that's why they did it. Obviously, the government reviewed the opinion before it was released to make sure there wasn't anything classified in it. It's the same thing with the Court of Review decision. That's published, and you can read that as well.

Student: If you want to record something, does the court have to give separate approval for each recording technique? For example, if you say "We're going to record the switchboard, and we're also going to wiretap him," do they have to approve each and every one? Do they have to say "You can do A and B, but not C"?

Baker: Yes. The applications have to describe the means of surveillance that are going to be used. The reason you do that is so that the court can assess whether or not the minimization procedures are adequate. Obviously, if you think about it, the type of information you collect when you're tapping a phone is different from the information you'll get when you put a microphone into a room. If you have a microphone in this room you're going to collect the communications of all these people talking at this particular time, whereas if you have a phone that's in a house and only one person lives there, the minimization needed is different.

Student: Is there ever any need for analysts from the intelligence community to appear before the court to explain why they need certain things, or is it purely legal people?

Baker: It's mostly lawyers, but we do have folks from the agencies come. Somebody from an agency comes for every case. When it's an FBI case, somebody from the FBI comes. Usually it's a supervisory special agent from headquarters who shows up. When it's an NSA case, it's a representative from the NSA, probably not down to the level of an analyst per se. It's a higher ranking official who is part of their oversight and compliance organization.

In a particular case where there's some issue you can bring in anyone you want to. We might want to bring in somebody to explain to the judge that it's a complicated case, and we want to explain what's going on, what the facts are, or what the technique is, or something like that. That kind of thing does happen, too.

Student: How quickly do these cases move? Is it rapid fire? It sounds as though if it's complicated and you have a bunch of people involved it can take some time.

Baker: There's a provision under FISA that allows the attorney general to authorize emergency surveillance for a period of up to about seventy-two hours. So if there's an emergency case the

intelligence agencies come to us. It can be done orally, over the phone, or whatever. They explain their situation to us, and if we're satisfied we can go to the attorney general. The attorney general can approve it, and then we have to prepare an application and file that within seventy-two hours.

The one thing that I didn't get to talk about was the NSA program. The NSA surveillance program now is being discontinued by the president, because we have obtained orders from the FISA Court that provide the NSA, to the satisfaction of the NSA and the president, the necessary speed and agility to do under FISA what was being done under the NSA surveillance program. As we've described publicly, they are complex, innovative applications that took a number of years to pull together, to work through, so those have been filed and approved by the FISA Court. I can't tell you what's going on with respect to those, but it's something the FISA Court was satisfied with—or at least the judge who approved them was satisfied with them—as well as the investigative agencies, the Justice Department, and the White House.

Oettinger: We promised to release you at three o'clock. We've passed that. Here's a small token of our appreciation.

Baker: Thank you; I appreciate it.

Acronyms

FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
NSA	National Security Agency
OIPR	Office of Intelligence Policy and Review
PLO	Palestine Liberation Organization

INCSEMINAR2007

ISBN 1-879716-98-4