William Mitchell Law Review

Volume 35
Issue 5 *Journal of the National Security Forum*

Article 2

2009

Responses to Ten Questions

William C. Banks

RESPONSES TO THE TEN QUESTIONS

William C. Banks†

9. Is the FISA Amendments Act of 2008 good policy? Is it constitutional?

It is widely understood that the political dynamics that led to the enactment of the Foreign Intelligence Surveillance Act (FISA) in 1978 were unique, and that the inter-branch compromises reached then authorized the means for electronic collection of foreign intelligence that served the Nation well for many years. The basic idea was simple: the Government can conduct intrusive electronic surveillance of Americans or others lawfully in the United States without traditional probable cause to believe that they had committed a crime, if it could demonstrate to a special Article III court that it had a different kind of probable cause: reason to believe that they are acting on behalf of foreign powers.

Since then, critics argue that the basic patchwork-like architecture of FISA became too rigid, too complicated, and too unforgiving to enable effective intelligence responses to crises. Would-be targets of surveillance are communicating in ways that stress or evade the FISA system (when, for example, the location of the target is difficult or impossible to determine). Because of switching technology, collection *inside* the United States is now often the best or only way to acquire even foreign-to-foreign communications. Furthermore, powerful computers and data mining techniques now permit computers to select potential surveillance targets from electronic databases of previously unimaginable size. The wholesale quality of such computer collection and data mining is incompatible with the retail scope of the original FISA process. At the same time, more Americans than ever are engaged in international communications and there is far

† Director of the Institute for National Security and Counterterrorism; the Laura J. and L. Douglas Board of Advisors Distinguished Professor, Syracuse University College of Law; and a professor of public administration at the Maxwell School of Citizenship & Public Affairs, Syracuse University.

greater intelligence interest in communications to and from Americans. Both circumstances increase the likelihood that the Government will be intercepting communications of innocent Americans, raising as many questions about the adequacy of the FISA safeguards, as about the adaptability of FISA architecture. This tension forms the context for a series of post-1978 amendments to FISA, culminating in the FISA Amendments Act of 2008 (FAA), which this essay examines.

THE ORIGINAL ARCHITECTURE

Until the 2008 amendments, FISA governed the electronic surveillance of persons in the United States for the purpose of collecting foreign intelligence. (FISA did not apply to surveillance conducted outside the United States, or to foreign-to-foreign telephone communications intercepted within the United States.) FISA "probable cause" required that targets of the surveillance had to be a "foreign power," an "agent of a foreign power," or, since 2004, a "lone wolf" terrorism suspect. Applications had to specify "facilities" where the surveillance would be directed and provide "minimization" procedures to assure that the "acquisition" of collected information would not be disseminated or retained outside authorized bounds. A special court that meets in secret was created to hear requests for orders to conduct the surveillance.

For a long time, the process worked well as a mechanism to regulate surveillance of known intelligence targets. The FISA process and its eventual orders have always been limited, however. FISA was concerned with "acquisition," not with the uses the Government might have for what is collected. FISA also assumed that officials know where the target is and what "facilities" he will use for his communications. Knowing this much enabled the Government to demonstrate the required "probable cause" to believe that the target was an agent of a foreign power, or more recently, a lone wolf. FISA did *not* authorize intelligence collection for the purpose of identifying the targets of surveillance, by collecting aggregate communications traffic and then identifying the surveillance target. In other words, FISA envisioned case-specific surveillance, not a generic surveillance operation, and its approval architecture was accordingly geared to specific, narrowly targeted applications. FISA was also based on the recognition that persons lawfully *in* the United States have constitutional privacy and free expression rights that stand in the way of unfettered

government surveillance.

TECHNOLOGICAL STRESSES ON THE ORIGINAL ARCHITECTURE

With the revolution in digital communications, however, the idea of a geographic border has become an increasingly less viable marker for legal authorities and their limits. Using the Internet, packets of data that constitute messages travel in disparate ways through networks, many of which come through or end up in the United States. Those packets, countless Skype calls, and instant messages originate from the United States in growing numbers. Nor do we think of our international communications as being in any way less private than our domestic calls. Because FISA was written to apply to broadly defined forms of "electronic surveillance" acquired inside the United States, digital technologies brought interception of previously unregulated communications inside the FISA scheme. Meanwhile, civil liberties groups complained that the data mining that was going on more or less without regulation was leading inexorably to greater governmental intrusions into our privacy.

Changing technologies have also turned the traditional sequence of FISA processes on its head. Just as we discovered after September 11 that investigators could enter transactional data about potential terrorists and come up with a list that included five of the hijackers—a sort of reverse of the typical FISA-supported investigation—our intelligence agencies now see the potential benefits of data mining as a means of developing the suspects that could be targets in the traditional FISA framework.

THE PRESIDENT RESPONDS: THE TERRORIST SURVEILLANCE PROGRAM

After September 11, President Bush ordered an expanded program of electronic surveillance by the National Security Agency (NSA). In December 2005, the *New York Times* reported that President Bush secretly authorized the NSA to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without obtaining orders from the FISA court. Although the details of what came to be called the Terrorist Surveillance Program (TSP) have not been made public, the NSA had monitored the telephone and e-mail communications of thousands of persons inside the United States where one end of

the communication was outside the United States and where there were reasonable grounds to believe that a party to the international communication was affiliated with al Qaeda or a related organization.

From news accounts and statements by Bush administration officials, it appears that the TSP operated in stages. With the cooperation of the telecommunications companies, the NSA first swept up all the traffic entering the United States at switching stations—so-called vacuum cleaner surveillance—wholesale collection. Second, that transactional data—addressing information, subject lines, and perhaps some message content—was computer mined for indications of terrorist activity. Third, as patterns or indications of terrorist activity were uncovered, intelligence officials at the NSA reviewed the collected data to ferret out potential threats, at the direction of NSA supervisors. Finally, the targets selected as potential threats were referred to the FBI for further investigation, pursuant to FISA, and the human surveillance ended for the others.

At first the Bush administration defended the legality of the TSP vigorously, but it was an uphill struggle. First, to the extent that the TSP targeted U.S. persons inside the United States, at least some portions of its surveillance were almost surely "electronic surveillance" as defined by FISA,[1] which in turn required applications for court orders to the Foreign Intelligence Surveillance Court (FISC). To the extent that Americans were only incidentally targeted, the definition less clearly applies to the collection.

Second, for foreign targets abroad, data arriving in the United States by satellite has always been unregulated by FISA, ironically because Congress was careful in 1978 not to reach NSA surveillance of radio traffic all over the world. But for digital traffic on fiber-optic cables FISA applied to collection inside the United States. (FISA did not apply if the surveillance occurred abroad, even if the call or e-mail was to an American inside the United States.)

1. 50 U.S.C. § 1801(f)(1) (2000) (defining "electronic surveillance" as "the acquisition by an electronic . . . device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes").

Third, FISA applications had to identify "targets" and "facilities" to be monitored, and the FISC had to make findings about each. There had to be probable cause that the target was a foreign power or its agents (or lone wolves) and the facilities had to be used, or about to be used, by the targets. As such, there was no way that FISA could have supported the wholesale, "vacuuming" programmatic surveillance as implemented by the TSP.

Fourth, Justice Department efforts to construe exclusivity and emergency provisions in FISA not to stand in the way of the executive program were not persuasive, and the constitutional arguments made in support of the TSP were based on courts of appeal decisions that permitted warrantless electronic surveillance for foreign intelligence purposes *before* FISA was enacted. FISA changed the constitutional calculus, and it provided a comprehensive scheme for regulating electronic surveillance for foreign intelligence collection.

FITTING TSP WITHIN FISA?

When the FISC took over administration of the TSP program in January 2007, Attorney General Alberto Gonzales advised the Senate Judiciary Committee that a FISC judge "issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization."[2] (He thus implicitly conceded that, notwithstanding the prior arguments made in support of the TSP, it did fall, after all, within the scope of FISA.) According to the Attorney General, all surveillance that had been occurring under the TSP would now be conducted with the approval of the FISC. He also stated that the President would not reauthorize the TSP when its current authorization expires.

Although we do not know for certain (as the orders have not been published), the January 2007 orders must have authorized surveillance of very broadly defined "targets" and "facilities." Al Qaeda and "associated terrorist organizations" could have been "targets" as a foreign power, because the original legislative history

2. Letter from Alberto R. Gonzales, U.S. Attorney Gen., to Patrick Leahy, U.S. Senator, & Arlen Specter, U.S. Senator (Jan. 17, 2007), *available at* http://www.fas.org/irp/congress/2007_cr/fisa011707.html.

of FISA explains that the term refers to the "individual or entity about whom or from whom information is sought." A group may be the target, even though the surveillance is directed at individuals. The traditional conception of "facilities" in FISA, however, is narrow, such as a single phone line or a single e-mail address. It could be interpreted broadly as place, and if it was construed to include the international switches owned by the telecom companies, surely al Qaeda and its affiliates use the switches in their international communications. Of course, lots of other people that have no connections to terrorism use those switches, too. Logically, if a switch can be a "facility," so too can all of Yahoo or Google, or even the U.S. telecom system or the Internet. If "facilities" is construed too broadly, the TSP may violate the particularity requirement of the Fourth Amendment and the long-standing proscription on general warrants.

The FISC might have counter-balanced such particularity concerns about "facility" by proposing more rigorous minimization procedures, required by FISA since 1978 to "minimize the acquisition and retention, and prohibit the dissemination" of nonpublic information about U.S. persons. The January 2007 FISC orders may have directed the Government to record the communications of only the portion of the switch used by the targets. The filtering capabilities of the government technology may permit it to do that. Then the probable cause determinations noted by the Attorney General and apparently approved by the FISC could have been made by executive branch personnel for follow-on surveillance, subject only to after-the-fact review by the FISC.

THE PROTECT AMERICA ACT OF 2007

Notwithstanding this speculative reasoning in support of the TSP under FISA, a different FISC judge decided in May 2007 not to continue approval of what had been the TSP under FISC supervision, and apparently determined that at least some of the foreign communications acquired in the United States are subject to individualized FISA processes. After a backlog of FISA applications developed, the Bush administration successfully persuaded Congress to pass statutory authorization for the program.

The administration emphasized the need to amend FISA to account for changes in technology and thus enable it to conduct

surveillance of foreign digital communications from within the United States. Yet providing statutory access to U.S. digital telecommunications switches would enable the NSA to access e-mail traffic traveling to or from U.S. servers, thus opening up a vast swath of U.S. person communications for government scrutiny.

As enacted in August 2007, the Protect America Act (PAA) determined that the definition of "electronic surveillance" in FISA should not extend to surveillance of a person reasonably believed to be outside the United States.[3] The PAA also permitted the Director of National Intelligence and the Attorney General to authorize collection of foreign intelligence "directed at" persons reasonably believed to be outside the United States, without obtaining an order from the FISC, even if one party to the communication was a U.S. citizen inside the United States. The PAA thus made less onerous the determination that the target is known to be abroad. Comparing the PAA to the TSP, the main differences were that the TSP allowed surveillance of targets inside the United States, and the predicate for collection authority under the PAA was the location of the target, not his status in relation to a foreign power or terrorist organization (as it was under the TSP).

THE FISA AMENDMENTS ACT OF 2008

The PAA expired by its own terms in February 2008 after Congress and the Bush administration failed to agree on a set of provisions that would grant broad, retroactive immunity to firms that participated in the TSP. The FISA Amendments Act of 2008 (FAA), enacted in July 2008, conferred the immunity sought by the administration and the telecommunications industry, but it insufficiently addressed important issues that continue to stand in the way of an effective legislative scheme for foreign intelligence surveillance.[4]

In essence, the FAA codified the PAA, with some additional wrinkles. The core of the new subtitle of FISA retains the PAA broad-based authorization to collect information "targeting" persons "reasonably believed to be located outside the United States to acquire foreign intelligence information." As with the PAA and the TSP, the FAA does not limit the Government to surveillance of particular, known persons reasonably believed to be

3. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552.
4. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

outside the United States, but instead permits so-called "vacuum cleaner" surveillance and data mining. In addition, the FAA targets do not have to be suspected of being an agent of a foreign power or, for that matter, they do not have to be suspected of terrorism or any national security offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance. Surveillance might be directed at a terrorist organization, a telephone number or e-mail address, or perhaps at an entire ISP or area code. Unlike traditional FISA applications, the surveillance permitted under the FAA does not require that the Government identify a particular known facility where the intercepted communications occur. On the positive side, for the first time surveillance targeting a U.S. citizen abroad is subject to FISA procedures, although those procedures are less demanding of the Government than traditional FISA surveillance conducted inside the United States.

A few attributes of the programmatic surveillance authorized by the FAA mark stark changes in FISA. First, some of the intercepted communications will be to or from American citizens (only intentional targeting of Americans is prohibited), and the surveillance producing the intercepts will not have been reviewed under pre-existing FISA requirements that the target be an agent of a foreign power or a lone wolf terrorist. Even the TSP targeted communications only where one party was outside the United States and there was probable cause to believe that at least one party to the communication is a member or agent of al Qaeda or an affiliated organization. The FAA eliminates any showing of individualized suspicion, even where communications of American citizens are the foreseeable consequence of the program orders.

Second, the Attorney General submits classified procedures to the FISC by which the Government will determine that acquisitions conducted under the program meet the program targeting objectives and satisfy traditional FISA minimization procedures. After a judge approves the program features, executive branch officials authorize the surveillance and issue directives compelling communications carriers to assist. Although details of the implementation of the program authorized by the FAA are not known, a best guess is the Government uses a broad vacuum cleaner-like first stage of collection, focusing on transactional data, where wholesale interception occurs following the development and implementation of filtering criteria. Then the NSA engages in

a more particularized collection of content after analyzing mined data. Although traditional FISA orders are still required for "intentional acquisition" of domestic communications, accidental or incidental acquisition of U.S. persons inside the United States surely occurs, especially in light of the difficulty of ascertaining a target's location. Nor do the minimization rules require the Government to discard communications of U.S. persons incidentally collected when the Government is targeting someone abroad. NSA may decide to retain any communications that constitute foreign intelligence, and there is no review of the NSA decisions.

A third problematic feature of the FAA is, ironically, that the legislation *follows* the thirty-year FISA model of focusing on targets and their location for the purposes of authorizing and conditioning surveillance and data collection. With modern communications capabilities, it is not possible to tell reliably in many cases where an individual is when a communication is made. From the Government's perspective, the downside of relying on a target's location as a basis for conducting lawful surveillance was softened when the PAA and FAA provided that the Government had only to reasonably believe that the target is abroad. However, one inevitable problem with the relaxed standard is that more warrantless surveillance of persons inside the United States will occur.

Fourth, whatever one thinks of the constitutionality or policy value of the programmatic surveillance authorized by the FAA, the legislation fails to prescribe processes for what happens next with the data that is collected through the approved program. On what bases and according to what processes and accountability mechanisms do officials determine to look more closely at individualized pieces of the traffic? Apparently, NSA used algorithms that purported to identify terrorist suspects out of the vacuumed mass of data. How exactly could such a data-driven process sort the innocuous call to me from my Muslim friend abroad from one that is worthy of further investigation? Is the limited human follow-on surveillance then a minimal intrusion that we should be prepared to accept, if we are assured that the brief surveillance will end and a traditional FISA application would follow as if further electronic surveillance is deemed worthwhile?

Finally, under the FAA what can the Government do with information acquired about U.S. persons who communicate with

foreign targets? Rules for dealing with "incidentally collected" U.S.-person information were developed when America's primary national security focus was overseas. The current focus on calls coming into and out of the United States will require some adjustments in managing the risk of acquiring communications of innocent Americans. As it now stands, minimization does not prevent the Government from retaining information incidentally collected on Americans.

CONCLUSION

When I first became a student of FISA, twenty years ago, I struggled to understand when a friend, who worked inside the FISA process, told me that we should worry less about what is collected and how, and more about how what is collected is used. Eventually I learned about the importance of the now-lowered wall that separated foreign intelligence from law enforcement, and about how minimization could protect private information.

Meanwhile the digital revolution and our data-driven society resulted in private industry having access to personal identifying information about most Americans. The constitutional and statutory law grew up around the premise that our voluntary sharing of that personal information with our credit card companies and ISPs and banks eliminated any reasonable expectation of privacy in that information. When the Government more prominently and aggressively began collecting and then mining that stream of data, especially after September 11, through pen registers, trap and trace devices, national security letters, and acquisition of so-called "business records," only a few limits were set on their use. Yet when the TSP was exposed, based on the same techniques, there was widespread condemnation of the Bush administration. Why?

Part of the reason is that Americans did not know that the Government could be sucking up our international telecommunications traffic, incoming and outgoing, and we suddenly feared that our conversations and e-mails were being read by someone at the NSA. Once we learned more about the program, we also feared that officials were continuing to monitor our communications, without cause and without the approval of any judge.

As we learned more about the TSP and its follow-on iterations, as authorized by the FISC and then Congress, it became clear that

the real privacy intrusion occurs not at the initial stage of flagging our calls or e-mails, but at the point that someone looking at aggregate data for patterns or suspicious activity decides to personally review an individual's communications. In other words, we should be worried about what the data is used for, not that it is collected.

Although information sharing has been a mantra in recent years, and curtailing the uses of collected data cuts against sharing, important reasons exist for imposing controls in the newest FISA program. Data mining is more than the "automation of traditional investigative skills."[5] The "automation" may have a greater impact on personal privacy because the mass of data mined will generate more false positives than traditional police work, and absent controls, the data may be preserved indefinitely for any use, including human review. To defend data mining by arguing that computers are not sentient beings and thus cannot invade privacy is to ignore what happens to the data after it is mined.

The PATRIOT Act amendments to FISA were made permanent in 2005, but the lone wolf provision, added by the intelligence reform legislation in 2004, sunsets at the end of 2009. The Justice Department will undoubtedly seek reauthorization of these provisions before they expire, providing a good opportunity to revisit the shortcomings in FISA. Lone wolf presents its own challenge to the integrity of FISA—the authority to conduct secret electronic surveillance of an individual who engages in terrorist activities effectively eliminates the need to demonstrate foreign agency that had always been part of the Government's obligation in a FISA application. Regardless of whether Congress rethinks how it describes the categories of potential targets for traditional FISA surveillance, it should take advantage of the lone wolf reauthorization to provide greater controls and accountability for the data mining and follow-on surveillance authorized by the FAA.

5. *Contra* K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2, 50 (2003) ("[D]ata mining is no more than the computational automation of traditional investigative skills . . . .").

***