Updating the Foreign Intelligence Surveillance Act

Orin S. Kerr†

INTRODUCTION

The Foreign Intelligence Surveillance Act of 1978[1] (FISA) has played a prominent role in the legal response to terrorism after the September 11, 2001 attacks. Following the attacks, amendments to FISA became a high-profile part of the controversial Patriot Act.[2] In December 2005, FISA regained the spotlight when the *New York Times* revealed that the Bush Administration had authorized the National Security Agency (NSA) to conduct domestic surveillance of international communications without obtaining FISA orders.[3] In August 2007, FISA was in the headlines again when Congress passed a controversial amendment to the statute, the Protect America Act of 2007.[4]

All of these controversies touched on different parts of the same question: is FISA outdated, and if it should be updated, how should it change? This broad question divides into two issues, the first relating to our basic values and the second relating to their implementation. The first question is whether FISA strikes the proper balance between privacy and national security. The second question is whether FISA implements its chosen balance in a way that accurately reflects the constitutional and technological realities of modern intelligence investigations. As often happens with matters of basic values, little headway can be made on the first question. Most of us have stubborn instincts about the severity of the terrorist threat on one hand and the threat to our civil liberties on the other. Barring another terrorist attack or disclosures of new privacy violations, individual views of what balance should be struck seem unlikely to budge.

This essay will focus on the second question, whether FISA's design is well tailored to the technology and constitutional law of mod-

† Professor, George Washington University Law School. This essay has been prepared for The University of Chicago Law School's Surveillance Symposium, hosted by the John M. Olin Program in Law & Economics and The University of Chicago Law Review.

1 Pub L No 95-511, 92 Stat 1783, codified as amended at 50 USCA § 1801 et seq (2007).

2 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act"), Pub L No 107-56, 115 Stat 272.

3 See James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, NY Times A1 (Dec 16, 2005) (reporting on the executive response to new terrorist threats and referring to the new law as a "legal sea change").

4 Pub L No 110-55, 121 Stat 552, codified at 50 USCA §§ 1805a–c (2007).

ern intelligence investigations. It argues that whatever balance FISA strikes, the statute must be rewritten to account for changes in both communications technology and Fourth Amendment doctrine over the last three decades. Like pet rocks and the Partridge Family, FISA's approach seemed natural in the 1970s. Its design made considerable sense in light of the Fourth Amendment law and communications technology of the era. In the last three decades, however, the constitutional and technological terrain has shifted. No matter what specific balance FISA strikes, its approach must recognize the new legal and technological environment.

Today's statute adopts what I will call a "person-focused" approach; its standards depend heavily on the identity and location of who is being monitored. The statute generally assumes that the subject of monitoring is a known person, and it then articulates standards for when that person's communications can be collected. This made sense in the era of the old-fashioned telephone network, when the government needed to identify a person before knowing what communications line to tap. But modern communications networks work very differently, and modern Fourth Amendment law accommodates the shift. Surveillance over modern packet-switched networks is often "data-focused"; the identity of who sent data or where that person is located often will be unknown or unknowable. Whereas traditional investigations were person-focused, tracing from people to their data, many of today's investigations are data-focused, tracing from data to the people who sent and received them.

In response to this change, Congress should supplement the existing person-focused FISA authorities with a complementary set of data-focused authorities. When the identity and/or location of the suspects monitored are unknown, the law should focus on the nature of the information collected. Surveillance practices should be authorized when the government establishes a likelihood that surveillance will yield what I call "terrorist intelligence information"—information relevant to terrorism investigations—subject to reasonable limits on the particularity of warrants. Surveillance would revert back to a more traditional approach if identity and/or location are known. If data-focused surveillance yields information that is specific as to the subject's identity and location, or such information is known from other sources, then the monitoring should proceed under the traditional person-focused legal authorities such as the existing FISA. The end result would be two different regimes of communications surveillance: a data-focused approach when identities or location are unknown and a person-focused approach when they are known.

I will make my case in three steps. The first step explores the person-focused approach to foreign intelligence dominant in the 1970s.

The second step explains the data-focused approach common today. Finally, the third step argues that the response to this shift should be to create a parallel set of data-focused surveillance authorities.

I. PERSON-FOCUSED FOREIGN INTELLIGENCE COLLECTION IN THE 1970S

Imagine the year is 1978. Jimmy Carter is President. The Bee Gees, Fleetwood Mac, and Steely Dan top the pop charts.[5] You can buy a new Pontiac Trans Am with an optional T-top roof for about $5,000.[6] Meanwhile, over in Washington, Congress is close to passing a new law to regulate foreign intelligence surveillance. Congress recognizes that spies and terrorists use home phones, public pay phones, and workplace telephones to communicate with others and share secrets. These spies and terrorists might also share secrets with conspirators in private places such as their apartments or foreign embassies. The purpose of the new law will be to regulate when the government needs a warrant to listen in.

But how should the new law work? The technology and constitutional law of the day provided a ready answer: the legal rules should hinge on the identity of who is being monitored and where the person is located. Monitoring some people in some places should require a traditional criminal law warrant; other people in other places should require a special national security warrant; and still other people in still other places should require no warrant at all. Surveillance law should be person-focused, looking to the "who" and "where" of the individual monitored.

A. Wiretapping Technology in the 1970s and the Person-focused Approach

The technology of the 1970s made a person-focused approach seem natural if not inevitable. At that time, there were three basic ways the government could snoop on a person's private real-time communications. First, government agents could actually tap wires, physically inserting monitoring devices into the circuits that completed the calls. Second, agents could intercept calls sent over the airwaves, such as calls beamed by communications satellites or broadcast

---

5 *The Billboard 200, 1978*, online at http://www.billboard.com/bbcom/charts/yearend_chart_display.jsp?f=The+Billboard+200&g=Year-end+Albums&year=1978 (visited Jan 12, 2008) (listing also the Grease soundtrack and Billy Joel to round out the top five).

6 *1970s Car Models and Car Prices*, The People History, online at http://www.thepeoplehistory.com/70scars.html (visited Jan 12, 2008) (showing car prices ranging from the Ford Maverick at $1,995 up to the Jaguar XJS at $18,000).

by radio transmitters. Third, agents could install microphones such as bugging devices.[7]

These techniques normally required the government to begin by identifying a particular person whose communications would be monitored. Monitoring required a *target*—a specific subject, often in a known specific place, who was likely to say specific types of things to others. Consider a microphone. Microphones pick up sound waves, so they normally are installed in the same room as the target. The target must come first and the monitoring later. The same goes for tapping telephone lines. Before knowing what line to tap, the government had to identify a target likely to participate in the call. In the technology of the day, telephone circuits generally traveled in a relatively straight line between the parties to the communication. The interception occurred somewhere along the path. As a result, wiretapping required a known target—known in the sense of what phone he used and where he was located, if not his actual identity—so the government could trace that particular person's calls and listen to that particular circuit.

B. Fourth Amendment Law in the 1970s and the Person-focused Approach

The state of Fourth Amendment law in the 1970s echoed the person-focused nature of 1970s-era intelligence investigations. The Fourth Amendment prohibits unreasonable searches, which breaks down into two questions: first, what is a search, and second, when is a search unreasonable? In the mid-1970s, both inquiries focused heavily on who was being monitored and where that person was located.

The importance of the subject's identity and his physical environment was central to the Warren Court's famous 1967 decision on the meaning of "searches," *Katz v United States*.[8] Katz placed illegal bets from a pay phone, and the FBI taped a microphone to the top of the phone booth and picked up his calls. The Court's cryptic opinion held that the government had "searched" Katz because "the Fourth Amendment protects people, not places."[9] But how did the Fourth Amendment protect "people"? Justice Harlan's concurrence tried to elaborate, and in so doing, introduced the "reasonable expectation of privacy" test.[10] According to Harlan, the key was the context in which the person acted: events inside "a man's home" receive protection, but "objects, activities,

---

7 See House Miscellaneous Reports on Public Bills IX, HR Rep No 95-1283, 95th Cong, 2d Session 50–52 (1978) (discussing the three basic mechanisms of electronic surveillance).

8 389 US 347 (1967).

9 Id at 351.

10 Id at 361 (Harlan concurring).

or statements that he exposes to the plain view of outsiders" do not.[11] Although *Katz* was a Rorschach test, it suggested that the Fourth Amendment test hinged on the subject's identity and environment. The government's actions were a "search" because Katz happened to be a legitimate user of the phone booth who had closed the door and, in doing so, had made the booth his temporarily private space.

The leading precedent on the reasonableness of foreign intelligence searches, handed down in 1972, had a similar focus. In *United States v United States District Court*[12] ("*Keith*"), the Supreme Court ruled that national security wiretapping of "domestic organization[s]" was constitutionally unreasonable without a warrant because the threat of abuse was high and the burden on the government relatively modest.[13] The Court repeatedly emphasized the identity of the people monitored as key to the Court's holding: it might be a different case, the Court suggested, if the government had been monitoring "the activities of foreign powers" instead of domestic organizations.[14] Several circuit courts weighed in on the question before Congress enacted FISA in 1978. Three circuits held no warrant was needed when the government monitored an agent of a foreign power;[15] one circuit disagreed in dicta and concluded a warrant was still required.[16] Although this corner of the law remained uncertain in 1978, the basic principle echoed that of *Katz* and *Keith*: to know how the Fourth Amendment applied, you needed to know who was being monitored and in what context.

C. FISA Embraces the Person-focused Approach

When Congress began drafting foreign intelligence surveillance bills in the mid-1970s, it naturally adopted the person-focused approach reflected in then-existing technology and constitutional law. FISA's standards focused heavily on the identity and location of the person monitored. The basic structure of the statute assumes that the

---

11 Id.

12 407 US 297 (1972).

13 Id at 321.

14 Id at 308–09.

15 See *United States v Buck*, 548 F2d 871, 875–76 (9th Cir 1977) (noting the President's responsibility to safeguard the nation from foreign encroachment); *United States v Butenko*, 494 F2d 593, 607 (3d Cir 1974) (en banc) (stating that information regarding relations of this nation with foreign powers counsels court-ordered disclosure only in the most compelling situations); *United States v Brown*, 484 F2d 418, 426 (5th Cir 1973) (upholding a search based on "the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs").

16 See *Zweibon v Mitchell*, 516 F2d 594, 602 (DC Cir 1975) ("Although . . . there should be no category of surveillance for which the President need not obtain a warrant, our holding today does not sweep that broadly.").

government starts with a suspect and then seeks authorization to collect that person's communications. Although amendments to FISA have made slight progress away from that 1970s ideal, the assumption remains a basic principle of FISA.

To see why, we need to delve into FISA for just a paragraph or two.[17] As enacted in 1978, FISA was a surprisingly simple statute. It banned the government from conducting "electronic surveillance" without a FISA warrant, subject to some exceptions. The statutory definition of "electronic surveillance" became the core of the statute,[18] covering four specific categories of surveillance that largely tracked the three different technological methods. The most straightforward form of electronic surveillance was wiretapping telephone lines from inside the United States. Under the statute, the government needed a FISA warrant to wiretap a phone call inside the US if the call was "to or from a person in the United States" and no participant to the call had consented.[19] The remaining three categories of surveillance were more complicated, as they applied only when the person monitored had a Fourth Amendment reasonable expectation of privacy and a Title III warrant would have been required in an analogous criminal investigation.[20] In those circumstances, the government needed to obtain a FISA warrant to install a bugging device inside the United States,[21] to intercept a call transmitted over the airwaves if all the participants to the call were inside the United States,[22] and to intentionally target the phone calls of "a particular, known United States person who is in the United States"[23] from either outside the United States or within it.

As a practical matter, all four of these categories required the government to start with a person. The first category demanded the least amount of information: it merely required the government to know if the call was to or from a person in the United States. The remaining categories demanded more. It was impossible to know if a person had a reasonable expectation of privacy or whether Title III would require a warrant in analogous settings without knowing the specific individual context in which the communications were monitored. The reasonable expectation of privacy test is notoriously con-

17 For a general introduction, see David S. Kris, *The Rise and Fall of the FISA Wall*, 17 Stan L & Policy Rev 487 (2006); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo Wash L Rev 1306 (2004).

18 See 50 USC § 1801(f) (Supp 1978).

19 50 USC §§ 1801(f)(2), 1802(a)(1)(B) (Supp 1978).

20 50 USC § 1801(f)(1), (3)–(4) (Supp 1978).

21 50 USC § 1801(f)(4) (Supp 1978).

22 50 USC § 1801(f)(3) (Supp 1978).

23 50 USC § 1801(f)(1) (Supp 1978).

text sensitive, and as the Fifth Circuit has complained, Title III is "a fog of inclusions and exclusions."[24] Whether a warrant would be required might depend on such details as whether the suspect was calling from home or at work,[25] or whether calls had been placed without paying long-distance fees.[26] And of course the inclusion of monitoring "a particular, known United States person" requires the government to have a particular, known person in mind.

Other parts of the original statute reflected the same assumption. To obtain a warrant, the government needed to establish probable cause that the person targeted by the surveillance was a foreign power or an agent of a foreign power.[27] There were two basic types of agents of foreign powers: terrorists and foreign government spies.[28] The government also needed to establish that the foreign power or its agent was using the "facilities or places at which the electronic surveillance is directed."[29] All of these definitions presupposed that the government began with a known target. Before it could tap a phone line or place a bug, the government needed probable cause to believe that the target was an agent of a foreign power and needed to know where and in what setting the target would be communicating. The government also needed a dossier on its target before monitoring could occur. Person first, monitoring later.

Although FISA has been amended and updated several times, the person-focused approach has remained largely intact. The original wiretapping and bugging authorities are essentially the same today as they were in 1978. The definition of "electronic surveillance" has remained virtually unchanged,[30] and FISA wiretapping still requires proof that the subject of the monitoring is a foreign power or an agent of a foreign power.[31] Congress added physical search provisions allowing for searches of physical spaces[32] and compelling email contents

---

24 *Briggs v American Air Filter Co*, 630 F2d 414, 415 (5th Cir 1980).

25 A suspect calling from work may have waived his privacy rights, creating consent to monitoring. See 18 USC § 2511(2)(c)–(d) (1976).

26 Failure to pay call tolls triggered monitoring rights under the provider exception. See 18 USC § 2511(2)(a)(i) (1976).

27 50 USC § 1804(a)(7) (Supp 1978).

28 Compare 50 USC § 1801(c)(1) (Supp 1978) (defining terrorism), with 50 USC § 1801(d) (Supp 1978) (defining sabotage).

29 50 USC § 1805(a)(3)(B) (Supp 1978).

30 Compare 50 USC § 1801(f) (Supp 1978), with 50 USCA § 1801(f) (2007). The only difference is a minor amendment to § 1801(f)(2) to cover computer hacking investigations; a hacker can be monitored without requiring a court order.

31 The definition of "agent of a foreign power" has changed slightly, however. Compare 50 USC § 1801(b) (Supp 1978), with 50 USCA § 1801(b) (2007).

32 50 USC §§ 1821–29 (2000).

from ISPs[33] that are similar; they require probable cause that the target of the search is a foreign power or its agent and that "the premises or property to be searched is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power."[34]

In contrast, the less invasive FISA authorities added after 1978 are more data-focused. Congress added subpoena-like authority to compel evidence from third parties in the form of National Security Letters (NSLs) and § 215 orders,[35] and a pen register and trap and trace section analogous to the pen/trap provisions used in criminal investigations.[36] These sections are keyed to whether the *information* collected is relevant. The law permits data collection when "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[37] Why the focus on information instead of people for these particular powers? The likely reason is that pen/trap and NSL authorities are preliminary powers. They regulate less intrusive measures designed to reveal agents of foreign powers rather than monitor known ones.

But should the data-focused approach of the less invasive FISA authorities be replicated throughout the statute? In the remainder of this essay, I make the case that it should.

II. THE NEW LAW AND TECHNOLOGY OF DATA-FOCUSED FOREIGN INTELLIGENCE INVESTIGATIONS

Let's fast-forward to the present. George W. Bush is President. Justin Timberlake, Beyoncé, and Fergie top the pop charts.[38] You can buy a new Toyota Prius for about $20,000.[39] Meanwhile, over in Washington, Congress is considering amending the thirty-year-old FISA. Should it? This Part explains why it should.

Specifically, this Part explains how the person-focused FISA of 1978 rests on assumptions about technology and constitutional law that are often no longer valid today. The technology and constitutional law of intelligence investigations has become heavily data-focused

---

33 50 USC § 1805(c)(2)(B) (2000).

34 50 USC § 1823(a)(4)(A)–(C) (2000).

35 See generally Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J Natl Sec L & Policy 37 (2005).

36 50 USC §§ 1841–46 (2000). The parallel authorities used in criminal investigations are found in 18 USC §§ 3121–27 (2000 & Supp 2002).

37 50 USC § 1842(c)(2) (2000 & Supp 2001).

38 This makes me miss the Bee Gees.

39 *Toyota Prius—2008 Models: Pricing & Touring*, online at http://www.toyota.com/prius/models.html (visited Jan 12, 2008).

rather than person-focused. Both internet technologies and modern Fourth Amendment law key more to information collected and less to who sent or received it. Many investigations will unfold just as they did in the 1970s. However, in many cases the government will not know who sent or received particular communications or where that person was located. Nor will it necessarily need to know that information, because location and identity are much less important than relevance. What matters is the information rather than the individual who served as its source.

A. Foreign Intelligence Investigations Today and the Data-focused Approach

Intelligence investigations often work very differently today because of the central role of the internet and the nature of surveillance in packet-switched networks.[40] Whereas traditional phone calls required a closed circuit between the parties, modern communications networks work by breaking down communications into packets and then sending them across a sea of connected computers.[41] This switch has profound implications for what data the government can see and how intelligence investigations must work.

To see why packet switching is so important, we need to understand a bit about what packets are and how packet communications are sent and received. Packets are really just strings of zeros and ones, each equivalent to roughly a page of information.[42] The string of data in a packet begins with a "header," roughly equivalent to the addressing information on a letter. The header explains what the packet is about: its origin and destination IP addresses, what kind of program it refers to, its overall length, and other similar information. The header is followed by the payload of the packet, which is the actual communication transferred.[43]

Notably, computers automatically create the header when a communication is sent; the user has little control over it. When the communication arrives, the header normally will be discarded and not saved.[44] In contrast, the sender normally has control over what kind of information appears in the payload. Although casual users normally have no need to think of such things, those worried about detection

---

40 See K.A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 Yale J L & Tech 128, 143–46 (2007).

41 See id.

42 See Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw U L Rev 607, 649–50 (2003).

43 Id at 612–15.

44 Id at 614.

can take steps to control and minimize the information their payloads reveal. Payloads can be encrypted, for example, or otherwise organized to reveal as much or as little information as the sender wishes.

We also need to know a little bit about how communications are sent and received. When one computer connected to the internet wants to send a communication to another computer, it breaks down the communication into packets, puts headers at the front of each packet, and then sends the packets out into the network.[45] The packets are then shuffled along by computers known as "routers" that look at the packet header and then direct the packet along the path that seems likely to get the packet to its destination most quickly. Importantly, the quickest path usually bears no resemblance to how the crow flies: packets are often routed across the country or even across the world thanks to particularly fast channels known as internet "backbones."[46] For example, if I am in Washington and request a webpage from a webserver in Chicago, the packets of traffic may travel to California or even a foreign country in the course of delivery.

Why do these details matter? They matter because they mean that modern network surveillance often works very differently than traditional telephone wiretapping or bugging. In particular, today's surveillance tends to be divorced from the identity and location of the parties to the communication. There is no known wire linked to a known person with known characteristics. Instead, a surveillance device must be inserted into a stream of packet traffic that either is configured to copy all the traffic for subsequent analysis or else to filter in real time based on known characteristics of the traffic.[47] Whether the filter is done in real time or later on, the data stream must be screened for known traffic characteristics rather than known identities. The focus must be on the data, not known persons who sent or received that data.

In this new world, the location of the surveillance no longer correlates to the location of the individuals surveilled. In particular, any point on the network will include a great deal of what James Risen has called "transit traffic"—communications traffic that just happens to be passing through.[48] Given the dominant role of the United States in modern communications technology, much of that transit traffic is directed through communications switches in the United States.

---

45 See Preston Gralla, *How the Internet Works* 13–14 (Que Millennium ed 1999) (explaining the packet-based nature of internet communications).

46 See id at 5 (noting that private companies who sell access to their lines build backbones, which are very high capacity lines that carry enormous amounts of internet traffic).

47 See Kerr, 97 Nw U L Rev at 649–51 (cited in note 42).

48 See James Risen, *State of War: The Secret History of the CIA and the Bush Administration* 50 (Free 2006).

Communications service providers in the United States end up playing host to a great deal of traffic sent and received from individuals located abroad.[49] Monitoring a particular river of packet-based traffic in the United States will pick up an incredible diversity of traffic, ranging from your mom's family email to parts of an encrypted phone call sent from Afghanistan to Iraq.[50]

Further, the kind of characteristics that the government might use to identify foreign intelligence information usually no longer includes a link to known individuals or places. Imagine the military seizes an al Qaeda computer in Iraq and sends it for analysis. That analysis might reveal the use of particular service providers, particular programs, particular encryption methods, or other information about traffic characteristics. However, it is unlikely to reveal anyone's identity: terrorists presumably do not use identifying email addresses like osama.binladen @gmail.com. Nor is it particularly likely to reveal anyone's location with any certainty: although IP addresses can give clues to location, they are not a clear indication of it.[51] In this setting, the government's goal must be to identify traffic that might provide sources of information rather than particular individuals likely to have it.[52]

B. The Fourth Amendment Today and the Data-focused Approach

Fourth Amendment principles that apply to foreign intelligence surveillance have also shifted since the 1970s, albeit less dramatically than the technology. Like the technology, the law has shifted from a person-focused approach to more of a data-focused approach. Today's Fourth Amendment focuses less on who is monitored or in what context and more on the information collected and the programmatic purpose of the surveillance regime.

Consider the evolution of the Fourth Amendment "search" doctrine. In 1967, *Katz* proclaimed that "the Fourth Amendment protects people, not places,"[53] which suggested that the law would make individualized determinations into how much the government invaded a person's privacy. But the law evolved differently. Instead of making individualized determinations, surveillance law has tended to focus on the methods of surveillance and the information the government col-

---

49 See id at 50–51.

50 Id at 51–52.

51 Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* 6–8 (Oxford 2006).

52 See Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U Chi L Rev 245, 252 (2007) (noting that FISA in its current form "remains usable for regulating the monitoring of communications of known terrorists, but it is useless for finding out who is a terrorist").

53 389 US at 351.

lects. Although much of the law remains uncertain,[54] existing law has hardened into rules that pay little attention to identity or context. Some techniques never amount to Fourth Amendment searches, including undercover operations,[55] the installation of pen registers,[56] intercepting cordless phone calls,[57] surveillance in public,[58] and acquiring noncontent account records.[59] Other techniques are always or virtually always searches, such as wiretapping the contents of landline phone calls.[60] The rule-like nature of the Fourth Amendment "search" doctrine means that how the Fourth Amendment applies often does not depend on who is monitored or where.[61]

The law governing the reasonableness of searches has changed as well. With the benefit of hindsight, we can now see that *Keith* was an early application of the Fourth Amendment's "special needs" doctrine,[62] which permits relaxed Fourth Amendment standards when government actors conduct searches and seizures for reasons beyond

---

54 Many of the rules remain constitutionally uncertain, including those that apply to email, text messages, and cell phone calls. See Orin S. Kerr, *Computer Crime Law* 298–445 (West 2006) (analyzing the extent of Fourth Amendment protection for remotely stored and directed data).

55 See *United States v White*, 401 US 745, 748–54 (1971) (reasoning that because a defendant does not have the right to exclude an informer's testimony, the defendant does not have the right to exclude a more accurate version of it made possible by a wiretap recording).

56 See *Smith v Maryland*, 442 US 735, 741–42 (1979) (finding that a defendant assumes the risk that information will be conveyed to others when he or she transmits that information to a telephone company).

57 See *Price v Turner*, 260 F3d 1144, 1148–49 (9th Cir 2001) (holding that according to an objective standard, the defendant did not have a reasonable expectation of privacy for phone conversations that were readily susceptible to interception); *In re Askin*, 47 F3d 100, 104–06 (4th Cir 1995) (same); *McKamey v Roach*, 55 F3d 1236, 1239–40 (6th Cir 1995) ("No reported decision has concluded that a cordless telephone user has a reasonable expectation of privacy in his cordless phone conversations under … the Fourth Amendment."); *Tyler v Berodt*, 877 F2d 705, 706–07 (8th Cir 1989) ("Courts have not accepted the assertions of privacy expectation by speakers who were aware that their conversation was being transmitted by cordless telephone.").

58 See *Katz*, 389 US at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *United States v Ellison*, 462 F3d 557, 561 (6th Cir 2006) (en banc) (holding that information on the defendant's vehicle license plate is not protected under the Fourth Amendment as it is subject to public view).

59 See *United States v Fregoso*, 60 F3d 1314, 1321 (8th Cir 1995) (holding that telephone company customers do not retain a reasonable expectation of privacy in account information held by the telephone company).

60 This is, of course, one of the lessons of *Katz*, 389 US at 353, and *Berger v New York*, 388 US 41, 55–56 (1967).

61 The major exception is that a person with no voluntary contacts with the United States has no Fourth Amendment rights under *United States v Verdugo-Urquidez*, 494 US 259, 274–75 (1990) (noting that, "for better or worse," we live in a world of nation-states and it is the responsibility of the political branches of government to determine the rules for search and seizure regarding important American interests abroad).

62 See generally Scott E. Sundby, *Protecting the Citizen "Whilst He Is Quiet": Suspicionless Searches, "Special Needs" and General Warrants*, 74 Miss L J 501 (2004) (arguing that Fourth Amendment concern over special needs mirrors similar concerns over the general warrant doctrine).

traditional law enforcement. Since *Keith*, the Supreme Court has refined and generalized the special needs doctrine; over time its emphasis has changed. Whereas *Keith* focused on identity, modern special needs cases focus on the "programmatic purpose" of governmental conduct.[63] The initial inquiry identifies the overarching purpose of the government's surveillance scheme rather than the identity of who is searched or seized.[64] The non–law enforcement interests involved are then balanced against the intrusiveness of the government's conduct.[65] Like the Fourth Amendment's search inquiry, reasonableness looks less to identity and context of the person monitored and more at the nature of the government's conduct.[66]

III. A DUAL APPROACH TO FOREIGN INTELLIGENCE SURVEILLANCE

Changes in technology and constitutional law since the 1970s suggest the need for new statutory principles for foreign intelligence investigations. In this section, I suggest a new approach: the law should offer two distinct sets of authorization to conduct monitoring instead of one. When the identity and/or location of the suspects monitored are unknown, the law should focus on the nature of the information collected. Rules governing surveillance practices should focus on the likelihood that surveillance will yield what I call "terrorist intelligence information"—information relevant to terrorism investigations. The approach would focus on data rather than people.

Surveillance would revert back to a more traditional approach if identity and/or location are known. If data-focused surveillance yields information that is specific as to the subject's identity and location, or such information is known from other sources, then the monitoring should switch to operating under the traditional person-focused legal authorities such as the existing FISA statute. The end result would be two different regimes of communications surveillance: a data-focused approach when identities or location are unknown and a person-focused approach when they are known.

---

63 See, for example, *Ferguson v City of Charleston*, 532 US 67, 81 (2001) ("In looking to the programmatic purpose, we consider all the available evidence in order to determine the relevant primary purpose.").

64 See id at 78–79 (identifying, "as an initial matter," the purpose of the drug test in question as the critical difference between the case at hand and previous similar cases); *Indianapolis v Edmond*, 531 US 32, 41–42 (2000) (stating that the Court has allowed suspicionless searches only in limited circumstances according to the intended purpose of the search).

65 *Ferguson*, 532 US at 78.

66 Of course, identity often still matters in Fourth Amendment law. For example, a US citizen has full Fourth Amendment rights wherever they are in the world. On the other hand, a person with no voluntary contacts with the US lacks any Fourth Amendment rights at all. *Verdugo-Urquidez*, 494 US at 274–75.

A. Probabilities of Terrorist Intelligence Information

When identities and/or location are unknown, legal authority to conduct foreign intelligence surveillance should be keyed to the probabilities of collecting terrorist intelligence information. Slightly modifying language already found in FISA, terrorist intelligence information could be defined as information "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[67] If the notion of relevance is too broad, the definition could be narrowed a bit to include only information "relevant *and material* to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."

The basic approach is conservative, as it mirrors traditional Fourth Amendment law standards used in criminal cases. Fourth Amendment standards for probable cause and reasonable suspicion are keyed to the likelihood of collecting evidence or contraband that could be relevant to a criminal case. Similarly, standards for foreign intelligence surveillance should be keyed to the likelihood of collecting information relevant to an investigation into terrorism. Exactly what powers would correlate to what probabilities would depend on how Congress wants to draw the privacy/security balance, which as I noted in the Introduction is beyond the scope of this essay. But presumably, the basic notion would be to correlate the likelihood that terrorist intelligence information will be collected with the invasiveness of the surveillance practice; the more invasive the practice, the greater the threshold required. For example, authority to intercept content might require probable cause, while authority to collect addressing information might require reasonable suspicion or even a lower standard.

One important advantage of this approach is that if a warrant process is used at this early stage, warrants could be issued based on traffic characteristics when identities are unknown and unknowable. For example, the government may have discovered clues of likely traffic patterns or practices characteristic of traffic that yield terrorist intelligence information. Perhaps the government has discovered that particular service providers, software programs, encryption methods, or combinations of all of the above are particularly likely to reveal such information. Instead of having to establish that the communications are likely to involve "agents of foreign powers," or that they are located in any particular place, the government would focus simply and directly on the likelihood that the particular surveillance tech-

67 50 USCA § 1842(c)(2) (2007).

nique would reveal the information sought.[68] The identity of the individuals and their location would become irrelevant.

B. Particularity and Terrorist Intelligence Information

Basing surveillance rules on the probability of collecting terrorist intelligence information raises important questions of warrant particularity. Particularity refers to the scope of the surveillance permitted by a court order.[69] Probability and particularity are always linked; the broader the permitted surveillance, the greater the likelihood that it will uncover *some* kind of evidence at *some* point. If a warrant is broad enough, the chances that it will collect relevant information approaches 100 percent. So the key question is, assuming Congress wants to monitor the first stage of surveillance with warrants, how particular should warrants keyed to terrorist intelligence information become?

Particularity wasn't a major issue when FISA was adopted because focusing on a person ensures particularity. Warrants will be particular when identity comes first; monitoring limited to a known specific person attempts to target only that person's communications. Consider a traditional 1970s-style wiretapping case. If the FBI thinks that Bob is a Soviet spy and seeks to tap his phone calls, the natural scope of the surveillance is any phone call believed to be by or to Bob. Tapping the neighbor's phone, or the telephone of a random person across town, makes no sense at all. After tapping Bob's phone and collecting the calls, the government can then minimize the recorded communications and use the relevant information.

Switching to an information-based surveillance system over a modern packet-switched network makes particularity extremely important, however. Whereas person-based monitoring implied particularity, data-focused monitoring requires difficult line drawing. Here's an example. Imagine that the government has reason to believe that an al Qaeda cell uses a particular ISP in Kabul and a particular type of software to communicate about a terrorist plot targeting the United States. In this case, the government has probable cause to believe that monitoring the ISP would uncover terrorist intelligence information. But how broad can the monitoring be? Can the government look at all of the traffic coming to or from that ISP in Kabul? Or can it only look at traffic to or from that ISP that uses that particular software?

---

68 Consider *United States v Grubbs*, 547 US 90, 96–97 (2006) (stating that in evaluating the constitutionality of anticipatory warrants, which are no different in principle than ordinary warrants, probable cause analysis should consider the likelihood that the sought-after material will be present at the site of the search).

69 See *Maryland v Garrison*, 480 US 79, 84–85 (1987) (explaining that the intended purpose of the particularity requirement was to limit general searches).

Or only some specific portion of the traffic from that ISP using that software? How about every communication to or from Afghanistan that uses the software? How particular must the surveillance be—and more specifically, how narrowly must a warrant authorizing the surveillance be written?

The Constitution offers little guidance on this issue, but it likely imposes only very modest and deferential limits on the scope of monitoring. First, we don't know if the Fourth Amendment demands a warrant at all for this sort of surveillance.[70] Second, the particularity requirement is practical and context sensitive; courts often state that the requirement is relaxed when there is no practical way to draft a warrant more narrowly to collect the evidence sought.[71] To the extent that the Fourth Amendment does speak to the question, the *Keith* case suggests that the guide is a balancing of interests: warrants can be constitutionally particular so long as their breadth is "reasonable both in relation to the legitimate need of Government" and any competing Fourth Amendment rights.[72]

This standard likely permits quite broad monitoring in most circumstances. If the government has probable cause, the legitimate needs of government will be clear; it generally will be difficult to limit the monitoring without making it less effective. On the other hand, the competing Fourth Amendment interests will often be vague and hypothetical. Only individuals who have voluntary contacts with the United States enjoy Fourth Amendment rights,[73] and how much heavily computerized national security monitoring infringes whatever rights that exist remains highly unclear. Given that, the constitutional balance likely can be struck in favor of quite broad government monitoring in most cases.

Should narrower monitoring be required as a matter of policy? I don't know of a principled way to enforce more limited monitoring.

---

70 There are two reasons for this. First, the special needs exception may make a warrant unnecessary. Second, the individuals monitored may lack a sufficient connection to the United States under *Verdugo-Urquidez* to have Fourth Amendment rights in the first place.

71 See, for example, *United States v One Parcel of Real Property Described as Lot 41*, 128 F3d 1386, 1394 (10th Cir 1997) ("[T]he warrant was as particular as it could be and, therefore, comported with the requirements of the Fourth Amendment."). Notably, however, the precedents consider particularity with respect to the items to be seized, not the places to be searched. See, for example, *United States v Harris*, 903 F2d 770, 775 (10th Cir 1990) ("A warrant that describes items to be seized in broad and generic terms may be valid if the description is as specific as circumstances and nature of the activity under investigation permit."). It is unclear how the same concept would apply to "places to be searched," which presumably would be the question for the scope of surveillance.

72 407 US at 322–23.

73 See *United States v Verdugo-Urquidez*, 494 US 259, 274–75 (1990) (holding that the Fourth Amendment did not apply to the defendant, a Mexican citizen whose Mexican home was searched).

There are many ways to limit monitoring, based on ranges of IP addresses, particular programs, or other identifying characteristics, but it's hard to devise a rule that would be nonarbitrary in light of the wide range of ways technology can be manipulated. A requirement of "reasonable" particularity judged on a case-by-case basis may be the best standard.

C. A Dual-path Approach

Importantly, I envision this approach working in tandem with the existing person-focused approach found in the current FISA statute. Congress should enact two sets of surveillance rules: a data-focused regime when identity and location are not known with certainty, and a person-focused regime when identity and location become known.[74] Under this proposal, surveillance could occur in two stages. In the first stage, when identity remains unknown, the government could use the one-size-fits-all data-focused approach to surveillance. The government would be allowed to conduct broad monitoring for a particular window of time based on probable cause to identify terrorist intelligence information. However, if the surveillance yields information that establishes identity and/or the location of the individuals monitored—or if that information happens to be known for other reasons, such as in a traditional foreign government spying case—the rules would switch to a traditional person-focused approach.

The strength of this approach is that it would best fit the regime to the circumstances. When identity and location are known, it may be unnecessary to rely solely on probabilities of data collection. Instead, the law can channel the monitoring into more definite rules depending on what is known of identity and location. For example, imagine two investigations that begin with known data about a likely terror cell. The government obtains warrants authorizing the surveillance in both cases. In the first case, the government learns that the cell is located in Iraq and appears to consist entirely of non-US persons. In the second case, the government learns that the cell is located in Brooklyn and includes US citizens. Under a dual-pronged approach, the discovery of identity and location could lead the monitoring to switch over to different rules. For example, the monitoring of the group known to be outside the United States could occur without any judicial oversight; the monitoring of the group that includes US citizens in the United States could occur pursuant to a traditional FISA warrant.

---

74 I read Judge Posner's contribution in this symposium to suggest something similar. See generally Posner, 75 U Chi L Rev 245 (cited in note 52).

There may be difficult questions of when the switch from the first regime to the second should occur. Perhaps monitoring should be allowed under the first regime until identity or location become clearly known, however long that may take. Alternatively, perhaps monitoring under the first regime should be allowed for only a specific window of time. Unfortunately, it is difficult if not impossible to resolve such operational questions without access to the classified details of how investigations actually work. The basic goal should be to tailor the regime to the context of the known facts; how to implement that goal depends on the specifics of how national security investigations work that remain classified.

D. Objections

There are two serious objections to my proposal. The first is that I have left out the most important question: what should the rules be at the initial stage? Should the initial stage be regulated by a warrant process, or should the initial stage remain unregulated by the courts until identities become known? Here I fall back on my initial caveat: where to draw the line between security and privacy is beyond the scope of this essay. Those who tilt towards the security end of the scale likely will want the initial stage to remain unregulated; those who tilt towards the privacy side likely will want a default warrant requirement. I take no position on which approach is preferable, as my goal is to offer a new framework rather than resolve its application.

A second criticism is that my approach simply makes an implicit practice explicit. That is, the intelligence community must already have some default practices that are followed before identities become known. If the law hinges on identity, some presumptions must be followed before identities are apparent. This is true, but I think making those presumptions explicit would be a major step forward. The government's presumptions and default practices are classified, which means that no one on the outside knows how the executive branch translates the concepts of FISA into operating rules. Amending FISA to account for these existing stages would bring the executive's practice into the open so Congress could make the decision of how to regulate the initial stage. The details of how the intelligence agencies execute the commands of FISA will always be and should always be hidden from public view. But the basic choice of how to regulate surveillance when identities are unknown can and should be made in the open by Congress.

CONCLUSION

Recommending changes to the law of national security investigations always suffers from the veil of secrecy that surrounds them. The investigations are classified. As outsiders, we're stuck trying to get a sense of the present practice and how to improve it based only on a small set of clues. Recommendations for reform are necessarily based on guesses—guesses of how cases work, of how they progress, and of how much the balance between privacy and security might change depending on particular changes in the rules.

My hope is that my proposal is general enough to be useful despite that difficulty. At bottom, it rests on a basic difference between traditional physical and telephone investigations and the new internet investigations. The former starts with individuals and then collects data; the latter normally will start with data and then try to connect the data to people. My basic contribution is that the switch requires different legal regimes owing to the different facts of the different types of investigations. Unless this principle is recognized in FISA, it is likely to operate *sub silentio* rather than out in the open. For example, the Protect America Act of 2007 implicitly recognizes this new problem: its major alteration to FISA is the explicit conclusion of surveillance "directed at a person reasonably believed to be located outside of the United States."[75] It then provides for a certification before the FISA court that "there are reasonable procedures in place for determining that the acquisition of foreign intelligence information . . . concerns persons reasonably believed to be located outside the United States."[76]

The fact that the new statute focuses on procedures designed to monitor those "reasonably believed" to be outside the United States should reinforce the importance of monitoring rules when location and identity are often difficult to identify. Under the new statute, the government must enact "procedures" for developing default answers to how the major categories of the existing statute fit. Although the FISA court has some modest role in approving these procedures, for the most part the rules at these early stages are unknown. But in an internet age these procedures are as important as the statute itself; in a world where location and identity are unknown, means of implementation become as important as former rules based on unknowable categories. Instead of keeping these defaults secret, Congress should regulate them specifically; the rules should be chosen in public by Congress rather than in secret by the executive branch.

---

75 50 USCA § 1805(a) (2007).

76 50 USCA § 1805b(a)(1) (2007).