Reviving Telecommunications Surveillance Law

Paul M. Schwartz†

INTRODUCTION

Consider three questions. How would one decide if there was too much telecommunications surveillance in the United States or too little? How would one know if law enforcement was using its surveillance capabilities in the most effective fashion? How would one assess the impact of this collection of information on civil liberties?

In answering these questions, a necessary step, the logical first move, would be to examine existing data about governmental surveillance practices and their results. One would also need to examine and understand how the legal system generated these statistics about telecommunications surveillance. To build on Patricia Bellia's scholarship, we can think of each telecommunications surveillance statute as having its own "information structure."[1] Each of these laws comes with institutional mechanisms that generate information about use of the respective statute.[2] Ideally, the information structure would generate data sets that would allow the three questions posed above to be answered. Light might also be shed on other basic issues, such as whether or not the amount of telecommunications surveillance was increasing or decreasing.

Such rational inquiry about telecommunications surveillance is, however, largely precluded by the haphazard and incomplete information that the government collects about it. In *Heart of Darkness*,[3] Joseph Conrad has his narrator muse on the "blank spaces" on the globe. Marlowe says:

> Now when I was a little chap I had a passion for maps. . . . At that time there were many blank spaces on the earth, and when I saw

† Professor of Law, UC Berkeley School of Law, Director, Berkeley Center for Law and Technology. My work on this paper began while I was a Professor of Law at Brooklyn Law School, and it benefited there from the support of the Milton and Miriam Handler Foundation. It also received support from the Dean's Research Fund at Brooklyn Law School as well as a summer research grant from Boalt Hall. Patricia Bellia, Jon Michaels, Chris Slobogin, Stephen Sugarman, and Frank Zimring offered helpful suggestions.

1 Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 Vill L Rev 425, 429 (2005).

2 Id.

3 Joseph Conrad, *Heart of Darkness*, in Joseph Conrad, *Youth: A Narrative and Two Other Stories* 51 (William Blackwood and Sons 1902).

> one that looked particularly inviting on a map (but they all look that) I would put my finger on it and say, When I grow up I will go there.[4]

In this essay, we will visit the blank spaces on the map of telecommunications surveillance law.

This essay begins by evaluating the main parts of telecommunications surveillance law. The critical statutory regulations are: (1) the Wiretap Act;[5] (2) the Pen Register Act;[6] (3) the Stored Communications Act[7] (SCA); (4) the Foreign Intelligence Surveillance Act[8] (FISA); and (5) the different provisions for National Security Letters[9] (NSLs). Even for these more densely regulated territories, there are considerable blank areas, which we will explore.

Other parts of the surveillance landscape represent an even greater expanse of blank spaces on the legal map. There are a number of "semi-known unknowns" (to coin a phrase); these are kinds of telecommunications surveillance about which only limited public information exists—this surveillance also occurs outside a detailed legal framework. Specifically, the National Security Administration (NSA) is now engaged in telecommunications surveillance activities in the US of unknown dimensions. This surveillance activity poses a considerable threat to the legal structure of existing regulation: it takes place through secret authorities, rests on secret DOJ opinions, and information gathered from it is fed back into the established system, including the judicial structure for issuing warrants, in a secret fashion.

This essay concludes with the development of the concept of "privacy theater." Currently, the value of the collection of telecommunications statistics is largely ritualistic. It serves to create a myth of oversight. In addition, the NSA's warrantless surveillance creates a different kind of "privacy theater." Here, the ritualization affects the overall structure of telecommunications surveillance law. The myth here is

---

4 Id at 59.

5 Omnibus Crime Control and Safe Streets Act of 1968, Title III ("Title III" or "Wiretap Act"), Pub L No 90-351, 82 Stat 211, codified as amended at 18 USCA § 2510 et seq (2007).

6 Electronic Communications Privacy Act of 1986, Title III ("Pen Register Act"), Pub L No 99-508, 100 Stat 1848, 1868, codified as amended at 18 USC §§ 3121–27 (2000 & Supp 2002).

7 Electronic Communications Privacy Act of 1986, Title II ("Stored Communications Act"), Pub L No 99-508, 100 Stat 1848, 1860, codified as amended at 18 USCA § 2701 et seq (2007).

8 Foreign Intelligence Surveillance Act of 1978, Pub L No 95-511, 92 Stat 1783, codified as amended at 50 USCA § 1801 et seq (2007). FISA regulates collection of intelligence information about foreign powers and agents of foreign powers operating within the borders of the United States. In contrast, the Wiretap Act, Pen Register Act, and Stored Communications Act establish procedures concerning the gathering of information to assist in criminal investigations within the United States.

9 See, for example, 18 USCA § 2709 (2007).

that telecommunications surveillance is subject to the rule of law—the real action increasingly takes place, however, off the mapped spaces and within secret areas. This essay proposes that we go beyond myth and rededicate ourselves to the task of creating a telecommunications surveillance law that minimizes the impact of surveillance on civil liberties and maximizes its effectiveness for law enforcement.

I. TELECOMMUNICATIONS SURVEILLANCE LAW: THE STATUTES AND STATISTICS

In the US, different statutes regulate the government's telecommunications surveillance. A collection of statistics tracks these statutes; the respective statistics depend on the legal categorization of the surveillance. The statutes that regulate telecommunications surveillance in the US are the Wiretap Act, the Pen Register Act, the Stored Communications Act, the Foreign Intelligence Security Act, and the various NSL provisions. The first three statutes concern domestic surveillance activities; the last two require a nexus of some kind with a foreign intelligence investigation. In Part I, I describe these statutes, consider how statistics are collected, and examine the available statistics. In Part II, I evaluate the semi-known unknowns.

A. The Wiretap Act

1. The statute.

In 1968, Congress enacted the Wiretap Act, which is also known as Title III because of its place within that year's Omnibus Crime Control Act. The enactment of this statute followed two important decisions by the Supreme Court in 1967. In *Katz v United States*,[10] the Court found that warrantless wiretapping of a telephone conversation violated the Fourth Amendment.[11] In an earlier opinion that year, *Berger v New York*,[12] the Court found that the Fourth Amendment established important constitutional standards for authorization of a surveillance warrant.[13] The Court required that a warrant for wiretapping describe with particularity the conversations sought, be extended only upon a showing of continued probable cause, and meet other rigorous procedural standards.

In response to these two decisions, the Wiretap Act prohibits "intercept[ion]" of a "wire or oral communication" without judicial au-

10 389 US 347 (1967).

11 See id at 359.

12 388 US 41 (1967).

13 See id at 54–60 (finding that the New York state law under which the warrant in question was authorized was "without adequate judicial supervision or protective procedures").

thorization.[14] In comparison to the other statutes that regulate domestic surveillance, the Wiretap Act sets the highest procedural hurdles for government. Wiretapping is to be a last resort for law enforcement officials. Indeed, Congress set a statutory level in the Wiretap Act higher than the Fourth Amendment's own strictures: the Wiretap Act requires findings to justify a "super search warrant."[15] This warrant requires a higher standard of proof, for example, than a warrant for searches of a house.

The Wiretap Act requires that the government show probable cause that an "individual is committing, has committed, or is about to commit" a predicate offense, that is, a serious offense listed in the Act.[16] The government also must demonstrate that the surveillance will capture evidence of this crime.[17] The Wiretap Act calls for a further showing that alternatives to interception have failed, are unlikely to succeed, or will be too dangerous.[18] Even when it is permitted, law enforcement must seek to minimize surveillance of nonrelevant conversations.[19] For example, if a conversation strays into extraneous matters unrelated to criminal activities, the wiretapping must cease.

There are, however, two important limitations on the Wiretap Act. First, the Wiretap Act is limited to surveillance of content and does not regulate the interceptions of "telecommunications attributes."[20] Second, it regulates only the capturing of messages contemporaneously with their transmission.[21] We will analyze these restrictions below when considering the scope of the Pen Register Act and the Stored Communications Act.

---

14 18 USC § 2511(1)(a) (2000) (prohibiting interception); 18 USCA § 2516(1) (2007) (describing what crimes and offenses wiretaps may be authorized to investigate).

15 See 18 USC § 2518 (2000).

16 18 USC § 2518(3)(a).

17 See 18 USCA § 2516(1) (delineating the various instances when law enforcement may intercept communications during the course of an investigation); 18 USC § 2518(3)(b) (authorizing wiretaps when "there is probable cause for belief that particular communications concerning that offense will be obtained through such interception").

18 See 18 USC § 2518(3)(c) (requiring that all reasonable and safe investigative procedures be exhausted before a judge authorizes the interception).

19 See 18 USC § 2518(5) (stating that each interception "shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter").

20 18 USC § 2510(4) (2000) (defining "intercept" as the "acquisition of the contents" of communications). For a description of "telecommunications attributes," see Part I.B.1.

21 See 18 USC § 2510(12) (2000) (including "transfer[s]," though not "storage," in the definition of "electronic communications"). See also *Steve Jackson Games, Inc v United States Secret Service*, 36 F3d 457, 461–62 (5th Cir 1994) (holding that interception of an "electronic communication" under the Wiretap Act requires that the acquisition of the communication be contemporaneous with its transmission).

2. The statistics.

The Wiretap Act provides for the collection of detailed statistics about law enforcement activity. Of all the telecommunications surveillance statutes, it provides for the most complete accounting of behavior. Pursuant to its mandate under the Wiretap Act, the Administrative Office of the United States Courts ("Administrative Office") has collected and published the required statistics, and in recent years has made them available on a dedicated website. These annual reports allow analysis of activity by the judiciary, law enforcement, and the targets of surveillance. We consider each of these aspects of the annual report in turn.

Regarding the judiciary, information is collected about the number of wiretap orders.[22] This statistic provides the easiest-to-grasp benchmark from the report, but must be used with caution as a proxy for the level of telecommunications surveillance. The two major caveats in this regard are, first, that a single order may authorize surveillance on more than one telephone account, and, second, that the Wiretap Act permits roving wiretaps.[23] In a roving wiretap, surveillance is centered on a person rather than an account or accounts. The roving wiretap issue is of somewhat limited significance, however, as their number remains modest. In 2006, for example, there were fifteen roving wiretaps, a notable increase from the eight in the preceding year.[24] Nonetheless, the statistic for the annual number of wiretap orders measures the output of the court system, but only offers an approximate sense of the level of surveillance that occurs each year under the Wiretap Act.

Turning to the numbers, one notes a steady rise over the last decade in the amount of wiretap orders. The number has increased from 1,186 in 1997, to 1,491 in 2001, to 1,839 in 2006.[25] This represents an

---

22 See 18 USC § 2519 (2000) (requiring the issuing or denying judge to report all interception orders to the Administrative Office).

23 For a discussion of roving wiretaps and the ability of a single order to authorize surveillance on multiple accounts, see Paul M. Schwartz, *German and US Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 Hastings L J 751, 762–63 (2003).

24 Administrative Office, *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving Interception of Wire, Oral, or Electronic Communications* ("*2006 Wiretap Report*") 9 (Apr 2007), online at http://www.uscourts.gov/wiretap06/contents.html (visited Jan 12, 2008).

25 Administrative Office, *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving Interception of Wire, Oral, or Electronic Communications* ("*1997 Wiretap Report*") 14 table 2 (Apr 1998), online at http://www.uscourts.gov/wiretap/contents.html (visited Jan 12, 2008); Administrative Office, *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving Interception of Wire, Oral, or Electronic Communications* ("*2001 Wire-*

increase of almost 55 percent. Moreover, wiretap orders over the last decade have increasingly become a phenomenon of state rather than federal courts. In 1997, there were 617 state orders and 569 federal orders.[26] In 2001, the breakdown was 486 federal orders and 1,005 state orders.[27] In 2006, there were 461 federal orders and 1,378 state orders.[28]

Regarding law enforcement, the official reporting reveals that almost all wiretap orders are sought and granted for drug-related crimes. In 2006, 80 percent of applications for intercepts, federal and state, cited a drug offense as the most serious crime under investigation.[29] The next largest categories are racketeering and homicide/assault, which were each specified in 5 percent and 6 percent, respectively, of applications.[30]

Moreover, wiretapping is primarily a phenomenon of a few jurisdictions. At the federal and state levels in 2006, four states, California (430 orders), New York (377), New Jersey (189), and Florida (98) accounted for 59 percent of all wiretap orders.[31] This pattern of use is likely independent of crime patterns, but rather reflects local law enforcement practice norms, including prosecutorial familiarity with the complex set of legal requirements for obtaining wiretap orders.

There is a separate reporting requirement for law enforcement encounters with encrypted communications. Beginning in the 1970s, government officials became concerned that commercial encryption software might hamstring law enforcement.[32] Although public access to encryption remains largely unregulated, concerns persisted about it becoming too powerful. As Senator Patrick Leahy remarked in 1999 in introducing a statute that amended the Wiretap Act to require enhanced reporting, "Encryption technology is critical to protect sensitive computer and online information. Yet, the same technology poses challenges to law enforcement when it is exploited by criminals to hide evidence or the fruits of criminal activities."[33] Since its 1999 amendment, the Wiretap Act has provided yearly evidence regarding

tap Report") 15 table 2 (May 2002), online at http://www.uscourts.gov/wiretap01/contents.html (visited Jan 12, 2008); *2006 Wiretap Report* at 15 table 2 (cited in note 24).

26 *1997 Wiretap Report* at 14 table 2 (cited in note 25).

27 *2001 Wiretap Report* at 15 table 2 (cited in note 25).

28 *2006 Wiretap Report* at 15 table 2 (cited in note 24).

29 See id at 19 table 3.

30 See id.

31 See id at 15–17 table 2.

32 Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* 67–85 (MIT 2d ed 2007).

33 145 Cong Rec S 15227–28 (Dec 3, 1999) (discussing the Continued Reporting of Intercepted Wire, Oral, and Electronic Communications Act).

the ongoing contest between law enforcement's decryption technology and targets' encryption software.[34]

The results are clear—targets rarely use encryption, and it almost never provides difficulties for law enforcement. In 2006, for example, law enforcement encountered no instances of encryption in wiretaps terminated that year and in none of these cases did it prevent officials from obtaining the plain text of communication.[35] Encryption has almost never prevented law enforcement from accessing the plain text of communications.[36]

On the target side, a total of 92 percent of all wiretaps in 2006 involved mobile communication devices.[37] In 2006, on average, a law enforcement use of an interception order captured the communications of 122 persons per order.[38] The average number of communications intercepted was 2,685 per wiretap.[39] The average percentage of incriminating intercepts per wiretap order in 2006 was 20 percent,[40] and this last statistic gives one pause. To be as clear as possible, this statistic is not inconsistent with each wiretap order leading to the collection of some incriminating intercepts. It means that on average 80 percent of the communications intercepted per order did not contain anything incriminating.

Is the glass 20 percent full or 80 percent empty? The Wiretap Act requires strict minimalization of the collection of extraneous information once surveillance occurs. Either these requirements are not being followed or inadequate procedures are in place. When 80 percent of all wiretaps fail to discover incriminating evidence, law enforcement officials are not obeying the statutory requirement of minimalization.

Finally, the *2006 Wiretap Report* details the results of wiretaps in terms of arrests as well as the number of motions made and granted to suppress with respect to interceptions.[41] Wiretaps terminated in 2006

---

34 See 18 USC § 2519(2)(b)(iv) (stating that the government must report "the number of orders in which encryption was encountered and whether such encryption prevented law enforcement from obtaining the plain text of communications").

35 See *2006 Wiretap Report* at 12 (cited in note 24).

36 In 2005, a state law enforcement authority reported its inability to decipher an encrypted communication from a wiretap in an earlier year. Administrative Office, *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving Interception of Wire, Oral, or Electronic Communications* ("*2005 Wiretap Report*") 11 (Apr 2006), online at http://www.uscourts.gov/wiretap05/contents.html (visited Jan 12, 2008). One wonders if possibly superior federal decryption resources would have overcome the obstacles to obtaining plain text in that case.

37 *2006 Wiretap Report* at 8 (cited in note 24).

38 Id at 23 table 4.

39 Id.

40 See id.

41 See id at 30 table 6.

led to the arrest of 4,376 persons and the conviction of 711 persons.[42] As arrests and convictions often do not occur within the same year as the use of an interception device, these numbers will increase over the next several years. In addition, law enforcement officials were able to draw on information gathered through wiretaps to impound large amounts of vehicles, weapons, and illegal drugs. Regarding motions to suppress, the Administrative Office does not provide this information in its 2006 summary report, but it may be calculated from documents that prosecutors file with the Office. In 2006, of the 283 motions to suppress 7 were granted and 61 were reported as pending.[43]

B. The Pen Register Act

1. The statute.

As noted above, the Wiretap Act contains important limitations on its scope, including a focus solely on the surveillance of content. It defines content as "any information concerning the substance, purport, or meaning" of "any wire, oral or electronic communication."[44] For example, during a conversation on a telephone, spoken words are transmitted over a wire, and these words constitute its "substance, purport, or meaning."[45] A variety of other information falls outside this category; we can refer to these data as "telecommunication attributes."

Some of this information already existed in 1968 at the time of the enactment of the Wiretap Act; technological changes also have created new and more detailed kinds of telecommunication attributes. Moreover, at least some of this information falls outside of the protection of the Fourth Amendment. In 1979, the Court decided *Smith v Maryland*,[46] a case involving the police's use of a "pen register."[47] This device permits the recording of telephone numbers that one dials. A similar machine, the "trap and trace" device, is used to capture the numbers received by a telephone. In *Smith*, the Supreme Court rejected the plaintiff's argument that the Fourth Amendment placed restrictions on law enforcement's access to information captured by either device. The *Smith* Court ruled that such information was non-

42 Id at 39 table 9.
43 See id at 88–115 table A-2, 246–65 table B-2.
44 18 USC § 2510(8) (2000).
45 Id.
46 442 US 735 (1979).
47 18 USC § 2510(8).

content information in which no constitutionally cognizable "legitimate expectation of privacy" existed.[48]

Congress reacted in 1986 to the *Smith* decision and the gap in the Wiretap Act's coverage by enacting the Pen Register Act.[49] This statute regulates law enforcement's use of pen registers and trap and trace devices. Recently, the Patriot Act[50] amended the Pen Register Act to include "dialing, routing, addressing, or signaling information" ("DRAS information") in its definition of the information that falls under the statute, which previously focused on "numbers dialed or otherwise transmitted."[51] IP addresses and email addressing information ("to" and "from" lines on email and routing) are an example of DRAS information.[52]

Pursuant to the Pen Register Act, law enforcement can obtain information through a lower standard than the Wiretap Act's super-warrant requirement.[53] Indeed, to anticipate the next section, the Pen Register Act also provides less rigorous requirements than the Stored Communication Act. Law enforcement officers can obtain information that falls under the Pen Register Act after filing an order with a court that states that the "information likely to be obtained . . . is relevant to an ongoing criminal investigation."[54] The Pen Register Act does not authorize judicial investigation of the substantive merits of this request. As long as the procedural requirements of the Pen Register Act are met, the court is to approve requests filed with it.[55]

2. The statistics.

Like the Wiretap Act, although in a less detailed manner, the Pen Register Act requires collection of information about its use.[56] Taken

48 442 US at 743–46 ("We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'").

49 See Pen Register Act, 100 Stat at 1868.

50 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.

51 Id § 216(a), 115 Stat at 288–90, codified at 18 USC § 3121(c) (2000 & Supp 2001).

52 See Daniel Solove, Marc Rotenberg, and Paul M. Schwartz, *Information Privacy Law* 296 (Aspen 2d ed 2006). See also Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 Nw U L Rev 607, 636–42 (2003) (characterizing the Patriot Act amendments to the Pen Register Act as merely the natural extension of existing law to emerging technologies).

53 See 18 USC § 3123 (2000 & Supp 2001) (denoting the elements required to obtain a surveillance order under the Pen Register Act).

54 Id.

55 See id (directing the court to enter an order authorizing pen register or trap and trace devices where "the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation").

56 18 USC § 3126 (2000) (directing the attorney general to report to Congress).

as a whole, the Pen Register's reporting requirements fall into a middle ground: less detailed than the Wiretap Act's, but more detailed than the Stored Communications Act's almost nonexistent reporting requirements. We first take a moment to explore the Pen Register Act's reporting requirements as expressed on paper—then we will analyze the most current statistical information available.

First, the Pen Register Act report requires a list of the period of interceptions authorized by order, and the number and duration of any extensions of the orders.[57] Recall that the Pen Register Act regulates information that is captured in transmission. Thus, similar to information collected under the Wiretap Act, this reporting requirement addresses the temporal dimension of surveillance. How long did the surveillance activity last?

Second, the report spells out the specific offense for which the Pen Register Act order was granted.[58] As in the Wiretap Act, this requirement acts as a check to ensure that the targets were involved in a predicate offense. Third, the report sets out the number of investigations involved.[59] This statistic gives a sense of the scope of the underlying law enforcement activity. Fourth, the report explains the number and nature of the facilities affected.[60] Fifth, it identifies the district of the applying law enforcement agency making the application as well as the person authorizing the order.[61]

At this juncture, something surprising can be reported: Pen Register Act reports are not publicly available and generally disappear into a congressional vacuum. At a presentation of this paper in June 2007, however, at The University of Chicago Law School's Surveillance Symposium, sponsored by the John M. Olin Program in Law & Economics and The University of Chicago Law Review, I discovered that Professor Bellia had succeeded in obtaining the official reports to Congress for 1999–2003 from the DOJ's Office of Legislative Affairs.[62]

---

57 Id.

58 18 USC § 3126(2).

59 18 USC § 3126(3).

60 18 USC § 3126(4).

61 18 USC § 3126(5).

62 Professor Bellia has generously shared these reports with me; I have posted these reports on my website at http://www.paulschwartz.net/penregister-report.pdf ("*Pen Register Reports*") (visited Jan 12, 2008) and shared them with interested academics and nongovernmental organizations. Until Professor Bellia was able to obtain these reports, the most recent publicly available Pen Register Act information was from 1998. For five years in the 1990s, from 1994 to 1998, a staff attorney at the Electronic Privacy Information Center (EPIC) with contacts on Capitol Hill found out the number of (1) pen register orders; and (2) extensions to the original orders. EPIC still posts these old statistics on its website. See *Approvals for Federal Pen Registers and Trap and Trace Devices 1987–1998*, EPIC, online at http://www.epic.org/privacy/wiretap/stats/penreg.html (visited Jan 12, 2008).

Interestingly enough, the reports do not appear to have been made annually, but as one document dump with five years of reports in November 2004.[63] The reports also fail to detail all of the information that the Pen Register Act requires to be shared with Congress.

This state of affairs is strange; it is somewhat similar to the archaic conditions prior to the New Deal and creation of the Federal Register and other methods for orderly publication of governmental records. Moreover, the lack of congressional interest in timely receipt of these reports is puzzling. There is, for example, no indication that Congress received the pen register reports for 2004, 2005, and 2006. This essay returns to this gap in knowledge in Part III below, where it develops the concept of "privacy theater."

Regarding the five years of pen/trap reports, a caveat is also important. These statistics only report *federal* use of these devices.[64] In comparison, the wiretap statistics list wiretaps in both *federal* and *state* jurisdictions.[65] If the trend for pen/trap statistics is similar to wiretap statistics, there is currently more state use of these devices than federal. Yet, no data are available regarding state pen/trap statistics.

As for the available federal statistics for pen/trap devices, these indicate a gradual decline in the amount of orders from 1999 to 2002, and then a large increase in 2003. In 1999, there were 6,502 orders; in 2000, 6,079; in 2001, 5,683; and in 2002, 5,311. Then, there was a dramatic rise in 2003 with 7,258 pen/trap orders.[66] The 2003 amount represents an 11.6 percent increase in federal use of pen/trap orders over the five-year period that began in 1999, and, more dramatically, a 29.9 percent increase from the preceding year. As a point of comparison, federal use of wiretaps declined over a similar period between 1999 and 2006.[67]

---

63 See *Pen Register Reports* (cited in note 62).

64 See id.

65 See, for example, *2006 Wiretap Report* at 19 table 3 (cited in note 24). State regulation of pen registers and trap and trace devices forms a diverse lot. Some state laws are modeled on the federal law. Others, as in California and New York, set a higher standard and require a judicial hearing, similar to when the government makes a wiretap request. James G. Carr and Patricia L. Bellia, *The Law of Electronic Surveillance* § 4:81 (West 2007). See also 86 Op Cal Atty Gen 198, Opinion No 03-406 6 (Dec 18, 2003) (finding that the California Constitution requires a judicial hearing before installment of a pen register by law enforcement and that court procedures in the federal pen register statute do not meet this state standard).

66 See *Pen Register Reports* at 5–9 (cited in note 62). The federal statistics also contain a notable internal gap: the DOJ reported in 2001 that it was "not able to obtain . . . statistics from the former INS," which had become part of the Department of Homeland Security. In 1999, the INS reported twenty-one pen/trap orders; in 2000, it reported ten.

67 Compare Administrative Office, *Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving Interception of Wire, Oral, or Electronic Communications* ("*1999 Wiretap Report*") 14 table 2 (Apr 2000), online at

C. The Stored Communications Act

1. The statute.

As we have seen, the Wiretap Act's first limitation is its applicability solely to the content of communication. Regarding its second limitation, the Wiretap Act regulates only the "interception" of a communication during the period of its "transmission."[68] Interception, in the sense of the Act, means capturing the contents of a communication as it is being transmitted with any electronic, mechanical, or other device.[69] A transmission represents the contemporaneous, or near-contemporaneous, expression of a communication by the sender and its receipt by the recipient. A speaker talks on the phone, the listener listens: the event occurs in real time.

Many other kinds of telecommunications occur in asynchronous fashion. For example, sending an email may be the most ubiquitous form of telecommunications in the US today. Yet, an email is in transmission—at least as the term is understood under the Wiretap Act—for only a short period. Transmission is the time that it takes from clicking on the "send" command to the moment the message arrives at the server of the recipient's ISP.[70] Of course, an email is only accessible to the individual to whom it is sent once downloaded from the server. Yet, its "transmission" for legal purposes has ended before this final stage, which means that the Wiretap Act will almost never be implicated by internet communications. The annual statistics collected under the Wiretap Act confirm this view.[71]

The process for obtaining access to information under the Stored Communications Act is generally less rigorous than under the Wiretap Act.[72] Even under its strictest requirements, the Stored Communications Act does not compel use of a "super search warrant." This statute sets up a sliding scale of mechanisms to compel disclosure based on different factors.[73] Its requirements range from a "probable cause" search warrant without notice to the subscriber or customer at the

---

http://www.uscourts.gov/wiretap99/contents.html (visited Jan 12, 2008) (reporting 601 federal intercept orders), with *2006 Wiretap Report* at 15 table 2 (cited in note 24) (reporting only 461 orders).

68 18 USC § 2511(1)(b) (2000).

69 See 18 USC § 2510(4).

70 See *United States v Steiger*, 318 F3d 1039, 1049–50 (11th Cir 2003) (noting that "very few seizures of electronic communications from computers will constitute 'interceptions'").

71 In 2006, for example, less than 1 percent of all wiretap orders involved "transmissions via computer such as electronic mail." *2006 Wiretap Report* at 11 (cited in note 24).

72 For a lucid discussion of the privacy protections of the Stored Communications Act, see Orin S. Kerr, *Computer Crime Law* 504–07 (West 2006) (listing and commenting on the various personal privacy exceptions allowable under the Stored Communications Act).

73 See 18 USC § 2703(b)(1) (2000 & Supp 2001) (denoting the different levels of disclosure).

high end to a subpoena with notice at the low end.[74] Moreover, the Stored Communications Act is not restricted to a set of predicate offenses. Rather, law enforcement officials can access information pursuant to the Stored Communications Act for any criminal investigation.[75]

2. The statistics.

As less electronic information than ever before is "content" that is in "transmission," the Stored Communications Act is the most important form of legal regulation for the government when it engages in domestic law enforcement surveillance. Yet, there are almost no official statistics collected about the government's use of this statute. In contrast to the Wiretap Act's detailed reporting provisions, the Stored Communications Act contains only a single reporting requirement—and one that only addresses the use of a single statutory exception, which regards disclosure in an emergency.

In 2001, the Patriot Act added this emergency exception and the concomitant reporting requirement as amendments to the Stored Communications Act. The 2006 amendments permit voluntary disclosures to the government when "the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[76] The attorney general is to file a report on emergency disclosures with the House and Senate Judiciary Committees.[77] The reporting requirement is intended to provide a check against misuse of the emergency exception. So far, so good—except this information is not publicly available at present.

D. Foreign Intelligence Information: FISA and the National Security Letter Provisions

We now shift our attention from statutes that authorize collection of telecommunications information for domestic law enforcement purposes to those that permit it for intelligence purposes.

---

74 See id.

75 See 18 USC § 2703(d) (2000 & Supp 2001) (requiring a judge to issue a warrant for surveillance whenever the relevant governmental entity demonstrates that there are "reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation").

76 Patriot Act § 212, 115 Stat at 284, codified as amended at 18 USCA § 2702(b)(8).

77 18 USCA § 2702(d) (requiring the attorney general to report: (1) the number of accounts of voluntary disclosures received under the emergency exception; and (2) a summary of the basis for disclosures in those instances where emergency disclosure was made but the investigation pertaining to those disclosures was closed without the filing of criminal charges).

1. The statutes: FISA and National Security Letters.

a) FISA. The Foreign Intelligence Surveillance Act[78] provides the chief statutory regulation for the government's collection of information about foreign intelligence within the US. The enactment of this statute followed the Supreme Court's decision in *United States v United States District Court*[79] ("*Keith*") in 1972, and investigations in 1975–1976 in the Senate and House of violations of civil liberties by the US intelligence community.

In *Keith*, the Supreme Court found that the Fourth Amendment required a neutral magistrate to issue warrants for domestic national security wiretaps. The *Keith* Court refused to permit "unreviewed executive discretion" in light of the "pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[80] It also explicitly declined to address the constitutional requirements for surveillance of the agents of foreign powers.[81] Subsequent to this decision, congressional investigations by Senator Frank Church and Representative Otis Pike revealed a long history of intelligence abuses. These included national intelligence agencies wiretapping US citizens without judicial warrants.[82]

After over a half-decade of congressional discussion and debate, Congress enacted FISA in 1978. FISA governs when foreign intelligence gathering is "a significant purpose" of the investigation.[83] Pursuant to FISA, the government may both engage in real-time electronic surveillance and gain access to stored electronic communications.[84] To do so, however, it must meet statutory procedures and requirements.

A special federal court, the Foreign Intelligence Surveillance Court (FISC) reviews the government's requests for FISA warrants.[85] The FISC proceeds ex parte; the DOJ makes applications to it on be-

78 FISA regulates the collection of intelligence information about foreign powers and agents of foreign powers operating within the borders of the United States. In contrast, the Wiretap Act, Pen Register Act, and Stored Communications Act establish procedures concerning the gathering of information to assist in criminal investigations within the United States.

79 407 US 297 (1972).

80 Id at 317.

81 See id at 321–22.

82 United States Senate, 2 *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 105–07 (GPO 1976). The investigators also revealed other abuses, including: the IRS developing intelligence files on more than 10,000 individuals between 1969–1973 due to their political beliefs; the CIA opening nearly a quarter of a million first class letters in the United States between 1953–1973 and creating a computerized index of nearly 1.5 million names; and the US Army maintaining intelligence files on an estimated 100,000 Americans between the mid-1960s and 1971. Id at 95.

83 50 USC § 1804(a)(7)(B) (2000 & Supp 2001).

84 50 USC § 1802(a)(1)(A) (2000).

85 50 USC § 1803(a) (2000 & Supp 2001).

half of the CIA and other agencies.[86] Applications must include a statement of facts justifying the government's belief that the target is a foreign power or an agent of a foreign power, and, in cases of foreign surveillance, that the foreign power or its agent is using "each of the facilities or places at which the electronic surveillance is directed."[87] The government may appeal decisions of the FISC to a three-judge appellate court, the Foreign Intelligence Surveillance Court of Review.[88]

b) NSLs. In addition to FISA, several statutes permit the FBI to obtain personal information from third parties through National Security Letters.[89] An NSL is a written directive by the FBI in cases involving national security; it does not require judicial review. NSLs extend to financial records, certain aspects of credit reports, and, of particular interest for this essay, certain telecommunications attributes. The relevant NSL provision allows the FBI to obtain "subscriber information and toll billing records information, or electronic communication transactional records."[90] As the Inspector General of the DOJ explains, the kinds of information that the FBI can obtain about electronic communications through NSLs include: "[h]istorical information on telephone calls made and received from a specified number, . . . and local and long distance billing records"; "[e]lectronic communication transactional records (e-mails), including e-mail addresses"; "screen names"; and "billing records and method of payment."[91] The government may not use a NSL to obtain the content of telecommunications, whether of telephone calls or emails.[92]

The Patriot Act changed then-existing authority and expanded the FBI's authority to obtain information through NSLs.[93] First, it lowered the threshold for issuing an NSL by eliminating the requirement that the sought-after information involve a foreign power or agent of a foreign power.[94] The new test is that of "relevancy" to an investigation to protect against international terrorism or espionage.[95] Second,

---

86 See 50 USCA § 1804(a); 50 USCA 1842(d).

87 50 USCA § 1804(a).

88 50 USC § 1803(b) (2000).

89 For an overview of NSLs, see DOJ, *Office of the Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters* ("*OIG Report on NSLs*") x–xiv (Mar 2007), online at http://www.usdoj.gov/oig/special/s0703b/final.pdf (visited Jan 12, 2008).

90 18 USC § 2709(a) (2000).

91 *OIG Report on NSLs* at xii (cited in note 89).

92 Id at 14 (distinguishing the subscriber, billing, and transactional information accessible with an NSL from "the content[s] of telephone conversations or email communications").

93 See Patriot Act § 505, 115 Stat at 365. For a general discussion of how the Patriot Act expanded the FBI's authority to access information using NSLs, see *OIG Report on NSLs* at 8–10 (cited in note 89).

94 See 18 USC § 2709(b) (2000 & Supp 2001).

95 See 18 USC § 2709(b)(1).

the Patriot Act decentralized authority to issue an NSL from a limited group of officials in FBI headquarters in Washington, DC to the head of any of the FBI's fifty-six field offices.[96]

A recipient of an NSL may petition a court for an order to set aside or modify the request.[97] The recipient of an NSL also faces a strict nondisclosure requirement, a gag order, which prohibits "disclos[ure] to any person" that the FBI "has sought or obtained access to information or records under this section."[98] A recipient of an NSL published an anonymous op-ed in the *Washington Post* in March 2007 providing a catalogue of the costs of NSL secrecy. Beyond the considerable personal stress that this requirement imposes, the author noted that his silence deprives the public of information about misuse of NSL authority. As the anonymous author states, "[b]ased on the context of the demand—a context that the FBI still won't let me discuss publicly—I suspected that the FBI was abusing its power and that the letter sought information to which the FBI was not entitled."[99] In September 2007, a federal district court found the NSL nondisclosure provisions unconstitutional under the First Amendment and the separation of powers doctrine.[100] The court also stayed its decision for ninety days to allow the government to appeal or pursue other courses of action.[101] In reaction to an earlier opinion in 2006 by the same court holding the NSL provisions unconstitutional, Congress had revised the statute's nondisclosure provisions.[102]

2. The statistics.

a) FISA. FISA requires annual reports to be filed with Congress and the Administrative Office. These reports provide skeletal

96 See 18 USC § 2709(b).

97 18 USCA § 3511(a) (2007) (providing for judicial review of NSLs and noting that "[t]he court may modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful").

98 18 USCA § 2709(c)(1) (2007).

99 Anonymous, *My National Security Letter Gag Order*, Wash Post A17 (Mar 23, 2007). The lack of public information allowed the FBI to continue its behavior: "Without the gag orders issued on recipients of the letters, it is doubtful that the FBI would be able to abuse the NSL power the way that it did." Id.

100 *Doe v Gonzales*, 500 F Supp 2d 379, 387 (SDNY 2007).

101 Id at 424.

102 Congress made the initial changes in the USA PATRIOT Improvement and Reauthorization Act of 2005 ("Patriot Reauthorization Act") § 128, Pub L No 109-177, 120 Stat 192, 228–29, (2006), codified at 18 USCA § 3511 (2007). Congress then made additional revisions in the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006 §§ 4–5, Pub L No 109-178, 120 Stat 278, 280–81, codified at 18 USCA § 2709(c)(4), (f) (2007). The earlier opinion from the district court was *Doe v Ashcroft*, 334 F Supp 2d 471, 494–511 (SDNY 2004). A second district court had also enjoined the government from enforcing the nondisclosure requirement of the statute. *Doe v Gonzales*, 386 F Supp 2d 66, 82 (D Conn 2005).

information, namely, "the total number of applications made for orders" of electronic surveillance and "the total number of such orders and extensions either granted, modified or denied."[103] FISA also requires the Attorney General to file reports on a semi-annual basis with the Senate and House Select Committees on Intelligence.[104] These reports are to concern "all uses of pen register and trap and trace devices" pursuant to FISA, including the total number of applications made and approved.[105] This information is made publicly available.

FISA reports reveal a dramatic increase in FISA orders. In 1997, there were 748 orders granted; in 2002, there were 932; in 2006, there were 2,181.[106] The increase over the last decade was 342 percent. These statistics are less than helpful, however, in understanding telecommunications surveillance for two reasons.

First, the numbers represent applications for both electronic and physical searches with no further breakdown given. In 1994, Congress amended FISA to allow physical searches as well as electronic ones.[107] The annual FISA reports henceforth lumped together both kinds of surveillance into one figure. Second, and even more significantly, these reports considerably undercount counterterrorism electronic surveillance because of one "semi-known unknown" to be discussed below: the Bush administration has carried out electronic surveillance of the type that FISA circumscribes, but without following this statute's requirements and without revealing the extent and precise nature of these activities.

The available evidence, nonetheless, indicates that 2006 was a highly active year for input from the FISA court. During this year, the FISC denied five of the government's applications, a number of refusals exceeded only in 1999.[108] The court also made substantive modifications to seventy-three proposed orders and denied one application in part.[109]

b) NSLs. In reauthorizing the Patriot Act in 2005, Congress required two important kinds of information to be released about NSLs. First, it expanded the existing reporting requirements. Prior and subsequent to the Patriot Act, the FBI provided classified, semi-annual

---

103 50 USC § 1807 (2000).

104 50 USCA § 1808(a)(1) (2007).

105 50 USCA § 1846 (2007).

106 DOJ, *Office of Legislative Affairs, Report to Nancy Pelosi, Speaker of the House of Representatives* ("*2006 FISA Report*") 1 (Apr 27, 2007), online at http://www.fas.org/irp/agency/doj/fisa/2006rept.pdf (visited Jan 12, 2008). For the 1997, 2002, and 2006 reports, among others, see http://www.fas.org/irp/agency/doj/fisa/#rept (visited Jan 12, 2008).

107 Intelligence Authorization Act for Fiscal Year 1995, Pub L No 103-359, 108 Stat 3423, 3443 (1994), codified as amended at 50 USCA § 1821–29 (2007).

108 See *2006 FISA Report* at 1–2 (cited in note 106).

109 Id.

reports to Congress on the FBI's use of NSLs.[110] The Patriot Reauthorization Act required the FBI to also issue annual public reports on the FBI's requests for NSLs.[111] Second, it required the inspector general of the DOJ to carry out an audit of the FBI's use of NSLs.[112]

The first kind of reporting is similar to that under FISA—it calls for release of a limited amount of statistical information. The attorney general is to submit "an aggregate report" to Congress that sets forth "with respect to the preceding year the total number of requests" made pursuant to NSL authority.[113] The NSL report for 2005 listed 9,254 NSLs that included US persons, and 3,501 different US persons implicated by these requests.[114] Yet, as the audit by the Inspector General reveals, these numbers substantially underreported the actual number of NSLs that the FBI issued. Instead of 9,254 NSL requests in 2005, the FBI issued 47,221 NSL requests.[115]

The flaws with the reporting begin with the explicit statutory exclusion for the public reports regarding "the number of requests for subscriber information."[116] Subscriber data are of particular interest for law enforcement, and hence, this omission skews the publicly released numbers downward and creates a misleading impression of the level of NSL activity. In addition, wide-reaching flaws existed in the FBI's tracking of NSLs. These involved shortcomings in the way that "the FBI records, forwards, and accounts for information about its use of NSLs."[117]

We now reach the second kind of reporting, which comes through the audit requirement. In its Patriot Reauthorization Act, Congress required a detailed examination by the DOJ's inspector general "of the effectiveness and use, including any improper or illegal use" of NSLs.[118] This kind of audit proved valuable in March 2006 when the Inspector General issued the first part of his review of the FBI's use of NSLs. As noted, the Inspector General found a dramatic underreporting of NSLs. Indeed, the total number of NSL requests between 2003 and 2005 to-

110 18 USC § 2709(e).

111 Patriot Reauthorization Act § 118, 120 Stat at 217–18 (noting that "[t]he report under this section shall be submitted in unclassified form").

112 Id § 119, 120 Stat at 219–21 (setting out requirements and submission dates for the inspector general's audits).

113 Id § 118(c)(1), 120 Stat at 218.

114 Letter from William E. Moschella, Assistant Attorney General, to J. Dennis Hastert, Speaker of the House of Representatives 5 (April 28, 2006), online at http://www.usdoj.gov/nsd/foia/reading_room/2005fisa-ltr.pdf (visited Jan 12, 2008).

115 *OIG Report on NSLs* at xix (cited in note 89).

116 Patriot Reauthorization Act § 118(c)(1)(A), 120 Stat at 218. For a discussion, see *OIG Report on NSLs* at xix (cited in note 89).

117 *OIG Report on NSLs* at xvi (cited in note 89).

118 Patriot Reauthorization Act § 119(a), 120 Stat at 219.

taled at least 143,074.[119] Of these NSLs requests, as the Inspector General found, "[t]he overwhelming majority . . . sought telephone toll billing records information, subscriber information (telephone or e-mail) or electronic communication transactional records under the [Electronic Communications Protection Act] NSL statute."[120]

The Inspector General also carried out a limited audit of investigative case files, and found that 22 percent of them contained at least one violation of investigative guidelines or procedures that was not reported to any of the relevant internal authorities at the FBI.[121] Finally, the Inspector General also found over seven hundred instances in which the FBI obtained telephone records and subscriber information from telephone companies based on the use of a so-called "exigent letter" authority.[122] This authority, absent from the statute, was invented by the FBI's Counterterrorism Division.[123] Having devised this new power, the FBI did not set limits on its use, or track how it was employed. Witnesses told the Inspector General that many of these letters "were not issued in exigent circumstances, and the FBI was unable to determine which letters were sent in emergency circumstances due to inadequate recordkeeping."[124]

II. SEMI-KNOWN UNKNOWNS: NSA DOMESTIC SURVEILLANCE

NSA surveillance has now moved into the US. An article in the *New York Times* in December 2005 revealed that the NSA was intercepting communications where one party was located outside the US and another party was inside the US.[125] After this story broke, President George W. Bush and then–Attorney General Alberto Gonzales confirmed, in general terms, this NSA activity.[126] In addition, the NSA is likely accessing purely international calls (foreign-to-foreign) that pass through telecommunications switches physically located in the

119 *OIG Report on NSLs* at xlv (cited in note 89).

120 Id.

121 Id at xxxi.

122 Id at xxxv–xxxvi.

123 See id at xxxv–xxxvii.

124 Id at xxxiv. Indeed, "in most instances, there was no documentation associating the requests with pending national security investigations." Id.

125 See James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, NY Times A1 (Dec 16, 2005).

126 Letter from William E. Moschella, Assistant Attorney General, to Pat Roberts, Chairman, Senate Select Committee on Intelligence, et al ("Moschella DOJ Letter") 1 (Dec 22, 2005), online at http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf (visited Jan 12, 2008) ("As described by the President, the NSA intercepts certain international communications into and out of the United States of people linked to al Qaeda or an affiliated terrorist organization.").

US.[127] There also has been some evidence, although at present inconclusive, that the NSA is accessing purely domestic communications—and without judicial warrants. In August 2007, in a few days of feverish activity immediately before its summer recess, Congress enacted amendments to FISA through the Protect America Act of 2007;[128] this law formally authorized one or more of these semi-known unknowns.

We begin this tale, still shrouded in secrecy, at the beginning. According to media reports, President Bush signed a secret executive order shortly after the terrorist attack on 9/11; the order authorized NSA access to foreign transit data routed through the US as well as certain foreign-domestic communications.[129] Due to the growth of fiber optic networks and the digitalization of telecommunications traffic, exclusively international emails or telephone calls are now routed through telecommunications switches located in the US.[130] The presidential authorization for the program or programs has been shared neither with Congress nor the public. The DOJ opinions said to declare the activities lawful remain secret.[131] President Bush also has blocked the granting of security clearances to lawyers at the DOJ's Office of Professional Responsibility (OPR) who were set to investigate the role of DOJ officials in authorizing warrantless NSA surveillance.[132] Attorneys at OPR have never been denied security clearances in the past.[133] This investigation was, however, reopened by Attorney General Michael Mukasey, the successor to Alberto Gonzales; the White House refused comment as to whether President Bush had "changed his mind about granting access to classified information."[134]

---

127 See James Risen, *State of War: The Secret History of the CIA and the Bush Administration* 49–51 (Free 2006) (describing the growth of transit traffic—purely international calls passing through the United States—and how the NSA gained access to the transit traffic).

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

129 See Risen and Lichtblau, *Bush Lets U.S. Spy on Callers*, NY Times at A1 (cited in note 125).

130 See id.

131 See id. For the legal justification of the program to Congress, see Moschella DOJ Letter at 2 (cited in note 126) (noting that the president's responsibility to protect the nation "includes the authority to order warrantless foreign intelligence surveillance within the United States, as [several courts] to have addressed the issue have concluded").

132 Murray Waas, Aborted DOJ Probe Probably Would Have Targeted Gonzales, Natl J 35–36 (Mar 15, 2007), online at http://news.nationaljournal.com/articles/0315nj1.htm (visited Jan 12, 2008) ("Bush personally intervened to sideline the Justice Department probe in April 2006 by taking the unusual step of denying investigators the security clearances necessary for their work.").

133 See id ("Michael Shaheen, who headed OPR from its inception until 1997, told [the magazine] . . . that his staff 'never ever was denied a clearance.'"). Indeed, the Bush administration granted security clearances to "a large team" of prosecutors and FBI agents, in the words of the chief of OPR, to investigate the leaks of information that led to the *New York Times*'s disclosure of the program's existence. Id.

134 Evan Perez, *Mukasey Reopens Internal Probe*, Wall St J A8 (Nov 14, 2007) (discussing the DOJ's perceived willingness to operate without yielding to White House pressure as a result of a new Attorney General).

During the debate about the Protect America Act, the Administration continued to deny congressional requests for information about the NSA's warrantless surveillance activities.[135]

There is also the possibility that in one of its US-based programs, the NSA is engaged in surveillance of purely domestic communications. In May 2006, *USA Today* revealed an additional NSA program in which at least one telephone company, AT&T, was providing the NSA with the telephone calling records of tens of millions of Americans.[136] This program is said to involve access to domestic telecommunications attributes. *USA Today* reported, "The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans."[137] Moreover, Seymour Hersh, in *The New Yorker*, stated that the NSA, subsequent to its program of collecting data about calls, "began to eavesdrop on callers (often using computers to listen for key words) or to investigate them using traditional police methods."[138] Computer searches are likely carried out around key words and link analysis.[139]

The information gathered in the NSA programs is then secretly fed back into the established legal system of telecommunications surveillance. According to James Risen, the Bush administration obtains FISA court approval for wiretaps "in part on the basis of information gathered from the earlier warrantless eavesdropping."[140] Two of his sources estimated that approximately 10 to 20 percent of the annual FISA warrants are based on information garnered through the NSA domestic surveillance program.[141] Thus, there may be several programs in which the NSA is engaged in surveillance within the US, including some in which data mining is used.

After claiming that its surveillance activity could not be made compatible with FISA, the Bush administration changed course in

---

135 Id.

136 Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today A1 (May 11, 2006) (reporting that the NSA was collecting phone records, though not listening to or recording actual conversations). *USA Today* subsequently admitted that it could not confirm BellSouth and Verizon participation in the NSA program. See Frank Ahrens and Howard Kurtz, *USA Today Takes Back Some of NSA Phone-record Report*, Wash Post A02 (July 1, 2006) (noting that "USA Today stood by much of its initial report, saying it had followed up with lawmakers and intelligence and telecom sources").

137 Cauley, *NSA Has Massive Database*, USA Today at A1 (cited in note 136).

138 Seymour M. Hersh, *National Security Dept. Listening In*, New Yorker 24, 25 (May 29, 2006) (charting the NSA's wiretapping activities from before FISA through to the present day).

139 See id (describing "'chaining,' in which subsequent calls to and from the American number were monitored and linked").

140 Risen, *State of War* at 54 (cited in note 127) (noting this method as one way "to cover up the NSA's role in the domestic surveillance of people inside the United States").

141 Id.

January 2007 and announced that it had brought at least one of its surveillance programs under the FISC's supervision.[142] In May 2007, Mike McConnell, the Director of National Intelligence, also informed Congress that the Bush administration would not commit itself to continue seeking FISA warrants.[143] Then, at some time in the spring of 2007, a secret FISC decision raised roadblocks to the NSA's surveillance activities.[144] The FISC opinion was said to concern a NSA request for a so-called "basket warrant" under which the FISC was to issue a warrant not on a case-by-case basis regarding specific suspects, but more generally to cover surveillance activity involving multiple targets.[145] The Administration leaked information about this ruling, made noises about the threat of imminent terrorist attacks, and pressured Congress in August 2007 to enact the Protect America Act.

This statute will sunset after six months,[146] which gives Congress a chance to reconsider the matter. This reevaluation is desperately needed; the Act creates an excessively broad carve-out from FISA that allows the NSA access not only to foreign-to-foreign transit data, but also to communications with a domestic component. The exceptions threaten to swallow the rule; the carve-out in the Protect America Act permits surveillance that will dwarf traditional FISA-regulated activities.

Electronic surveillance is freed of FISA constraints under the Protect America Act if the surveillance is "directed at a person reasonably believed to be located outside of the United States."[147] Thus, this telecommunications surveillance can sweep in communications with a domestic component as long as the surveillance itself is not "directed at" a person in the US, but a person abroad. The critical term, "directed at," is not defined in the Act, but left to the attorney general

142 Eric Lichtblau and David Johnston, *Court to Oversee US Wiretapping in Terror Cases*, NY Times A1 (Jan 18, 2007) (reporting that the Justice Department had reached an arrangement with the Foreign Intelligence Surveillance Court that would allow court approvals to be provided with sufficient speed such that national security would not be compromised).

143 See James Risen, *Administration Pulls Back on Surveillance Agreement*, NY Times A18 (May 2, 2007) (mentioning McConnell's claim that the Constitution authorized the president to order warrantless wiretaps).

144 See Greg Miller, *New Limits Put on Overseas Surveillance*, LA Times A16 (Aug 2, 2007) (noting that recent limitations on FISC-authorized eavesdropping have prompted new concerns about national security); Michael Isikoff and Mark Hosenball, *Terror Watch: Behind the Surveillance Debate*, Newsweek Online Exclusive (Aug 1, 2007), online at http://www.newsweek.com/id/32596 (visited Jan 12, 2008) (examining the FISA judge's ruling to limit the NSA's eavesdropping capabilities and the ruling's likely effects).

145 Miller, *New Limits Put on Overseas Surveillance* LA Times at A16 (cited in note 144). One anonymous official was quoted as saying that the FISC ruling concerned cases "where one end is foreign and you don't know where the other is." Id.

146 See Protect America Act of 2007 § 6(c), 120 Stat at 557, codified at 50 USCA § 1803 note.

147 50 USCA § 1805a.

to shape through the creation of "reasonable procedures."[148] Note as well that a link with an agent of a foreign power or terrorist is not needed; rather, "a significant purpose of the acquisition" must merely be "to obtain foreign intelligence information."[149]

This law also permits the FISC a negligible role at best. It assigns the FISC the task of issuing advisory opinions; this role raises significant Article III questions. As for the substance, such as it is, of the judicial role, the attorney general is first to develop "reasonable procedures . . . for determining that the acquisition of foreign intelligence information . . . concerns persons reasonably believed to be located outside the United States."[150] Procedures are also to be developed for minimization of the collection of nonpublic information about US citizens—a similar requirement is already in place for FISA.[151] As noted above, however, Wiretap Act statistics show that the minimization under that statute has proven highly unsuccessful. The FISC then evaluates whether the attorney general's determination regarding the reasonableness of the procedures is "clearly erroneous."[152]

Finally, the Protect America Act's information structure is weak. The attorney general is to inform four congressional committees on a semi-annual basis of acquisitions made under the statute, including incidents of noncompliance.[153] This reporting provision is especially problematic because of recently resigned Attorney General Alberto Gonzales's record of evasive congressional testimony on multiple topics, including, of particular relevance in this context, the administration's warrantless surveillance outside of FISA.[154]

In summary, a new era in telecommunications surveillance is underway. A secret parallel system of telecommunications surveillance exists, and information collected in it is fed back into the official system in a fashion that leaves no traces. This system is built on secret presidential authorizations; secret DOJ legal opinions; nonbinding presidential promises; denials of security clearances to DOJ attorneys to squelch internal investigations; an executive that refuses to provide Congress and the public with necessary information; and, most recently, acquiescent congressional legislation enacted in ignorance of the true dimensions of NSA activities.

---

148 50 USCA § 1805b(a)(1).

149 50 USCA § 1805b(a)(4).

150 50 USCA § 1805b(a)(1).

151 50 USCA § 1805b(a)(5).

152 50 USCA § 1805c(b).

153 Patriot Reauthorization Act § 118, 120 Stat at 217–18.

154 As *The Economist* sarcastically explained regarding some of the Attorney General's congressional testimony, "[P]erhaps Mr Gonzales is merely a weasel and not a perjurer." *Alberto Gonzales: A Visit to the Hospital*, Economist 35 (Aug 4, 2007).

III. THE GROWTH IN BLANK SPACES, THE RISE OF PRIVACY THEATER, AND TOWARDS THE REVIVAL OF TELECOMMUNICATIONS SURVEILLANCE LAW

We began this essay with a quotation from Conrad about the "blank spaces on the earth."[155] On the domestic side, here has been a significant movement in surveillance activity away from the capturing of content pursuant to the Wiretap Act, which is the most carefully regulated and reported-on area of telecommunications surveillance. Of more importance today is the collection of telecommunications attributes under the Pen Register Act and the Stored Communications Act. Yet, we lack access to any statistical data about activities under the latter, and have less than full and up-to-date information regarding the former.

At this juncture, one is reminded of Bruce Schneier's concept of "security theater," which I wish to develop to include the idea of "privacy theater." According to Schneier, security theater is action that seeks to increase our feeling of security without actually making us safer.[156] As an example, a requirement to show ID before entering an office building, a common obligation in New York and other cities, does nothing to increase our security against terrorists. As for privacy theater, it seeks to heighten a feeling of privacy protection without actually accomplishing anything substantive in this regard. As a prime example, the DOJ occasionally sends information to Congress about pen register activity, scholars dutifully and approvingly note this statutory requirement, and then . . . well, nothing happens. The information disappears into a congressional void.

This demonstration of privacy theater shows a structuring of behavior that proves ineffectual. Yet, the payoff of this structure is through its value as a ritual. Organization theory provides multiple illustrations of the importance of rituals in organizing collective behavior. Organizations draw on and develop "vocabularies of structure" that help legitimize ends, and, in turn, entities that follow established "myths of formal structure" demonstrate their fitness.[157] From this perspective, the Wiretap Act established a useful organizational model in 1968, and the Pen Register Act followed this information structure in 1986. This privacy ritual involves recourse to a formal

---

155 See note 4 and accompanying text.

156 See Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* 38 (Copernicus 2003).

157 See John Meyer and Brian Rowan, *Institutionalized Organizations: Formal Structure as Myth and Ceremony*, in Walter W. Powell and Paul J. DiMaggio, eds, *The New Institutionalism in Organizational Analysis* 41, 50–51 (Chicago 1991) (discussing how "rationalized institutions create myths of formal structure which shape organizations").

structure for collection and transfer of statistical information about telecommunications surveillance. In turn, FISA returned to this model in 1978 by adopting its own reporting requirements.

The ritual creates and supports a myth—one of privacy oversight. In the myth, the counting and tracking of law enforcement activity implies that someone somewhere is drawing lessons from these statistics and that the surveillance system, in turn, will be reformed if needed. In contrast, the Stored Communications Act in 1986 deviated from this model—the likely reason for its failure to draw on the established myth was the uncertainty, still continuing to this day, regarding the place of telecommunications attributes within the information privacy landscape. It is also striking that so little has been done to improve the collection and use of statistics about telecommunications surveillance. The privacy oversight myth, nevertheless, persists.

As for the semi-known unknowns, this area of telecommunications surveillance presents a series of large blank spaces. There are several secret NSA programs that were first subject only to improvised legal processes and now have been granted a large, albeit temporary, statutory carve-out from FISA by a Congress kept in the dark. As Senator Jay Rockefeller, a member of the Senate Intelligence Committee, complained in September 2006, "I have been requesting without success specific details about the program, including: how many terrorists have been identified; how many arrested; how many convicted; and how many terrorists have been deported or killed as a direct result of information obtained through the warrantless wiretapping program."[158] At that time as well as today, "not one person in Congress has the answers to these and many other fundamental questions."[159] One can recall another insight of Schneier's: "Secrecy contributes to the 'trust us and we'll make the trade-offs for you' mentality that ensures sloppy security systems."[160]

This essay concludes by considering two areas for reforms. The first concerns foreign intelligence surveillance and the second concerns the

---

158 Senator Jay Rockefeller, Press Release, *Rockefeller Says Administration Still Withholding Information on NSA Warrantless Surveillance Program* (Sept 13, 2006), online at http://www.senate.gov/~rockefeller/news/2006/pr091306.html (visited Jan 12, 2008).

159 Id. More recently, some information has been shared with the congressional Intelligence Committees, though it is reasonable to be skeptical about the extent of this disclosure. See Mark Mazzetti, *Key Lawmakers Getting Files about Surveillance Program*, NY Times A12 (Feb 1, 2007) (noting that select members of Congress had received secret documents relating to the NSA's domestic eavesdropping program). *The New York Times*'s editorial board has called for President Bush to turn over documents about the warrantless spying program to Congress and to share the FISC opinion on the government's surveillance with the public. Editorial, *The Need to Know*, NY Times A14 (Aug 11, 2007) (remarking on the problems inherent with the Protect America Act's lack of privacy protections).

160 Schneier, *Beyond Fear* at 279 (cited in note 156).

statistics about telecommunications surveillance in the US. The goal is to break out of the ritual of "privacy theater"; specifically, the need is to create strong congressional oversight, meaningful discussion within the executive branch itself, and informed public debate. An improvement in the quality and quantity of information will serve these aims.

The first area of reform concerns the NSA surveillance programs and the NSLs. The NSA activities undermined the previous legal framework for telecommunications surveillance law. In the words of the bipartisan Markle Foundation Task Force on National Security in the Information Age, the current need is for a restoration of "intragovernmental and public confidence that articulated rules are being followed" in "a publicly-established framework agreed upon by the executive branch and Congress."[161] The Protect America Act does not represent a successful attempt to establish a framework that will restore such confidence—Congress legislated from a position of ignorance as to executive branch activities, and there is only uncertainty as to how and whether its provisions will be followed. Its narrowing of FISC's role is especially problematic.

The Protect America Act should be replaced by a statute that only authorizes a carve-out for foreign transit data and that provides a robust role for FISC oversight. Beyond that, the issue of data mining involving domestic communications raises complex and controversial issues—and, here, blue ribbon panels and scholarship already have begun to point to how this technique can be used in a fashion consistent with the rule of law.[162]

More information can be gained through auditing of NSA activities. On a promising note, Congress demonstrated in 2006 the potential for improvements in this area by creating both an NSL reporting requirement and an inspector general audit obligation for NSL use. On a unpromising note, Congress backslid in 2007 in enacting the Protect America Act, which permits open-ended, unaudited reports to be filed with it by the attorney general. In contrast, a competing House bill required the inspector general to audit compliance with the guidelines for cases involving surveillance of a US citizen as well as "the

161 Markle Foundation Task Force on National Security in the Information Age, *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment* 22 (July 2006), online at http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf (visited Jan 12, 2008).

162 For a summary, see generally Ira S. Rubinstein, Ronald D. Lee, and Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U Chi L Rev 261 (2008).

number of persons in the United States whose communications" were intercepted.[163]

As for the Inspector General audit of NSLs, it revealed a need for ongoing oversight of the FBI's use of these extrajudicial searches as well as reform of current NSL provisions. Here, a good start would be to modify the overarching "gag rules" to allow disclosure in most circumstances once ongoing telecommunications surveillance ends.

Beyond the NSA and NSL surveillance, Congress should revise the existing statutory models for gathering statistics. Its goal should be to improve the information structure of this area of law by creating an annual telecommunications surveillance index. Instead of the bits and pieces of scattered reports released each year, Congress should create one annual report card that measures and publicizes government's performance in this area. As Neal Katyal has stated, "[r]eporting requirements are powerful devices" that promote external checks by Congress as well as strengthening bureaucrats in administrative agencies, who can act as a check on excessive executive power.[164]

There are five steps that Congress should take towards the creation of this index. First, the respective telecommunications surveillance statutes should be amended so the Administrative Office receives copies of all telecommunications surveillance statistics collected pursuant to statute. Since 1968, the Administrative Office has demonstrated its ability to collect and release such information and analysis. The Administrative Office should prepare its own analysis of these statistics as it has done for Wiretap Act information. As a first step towards this goal, the Pen Register Act should be amended so reporting under it is made to the Administrative Office.

Second, the annual index should include information about law enforcement activity under the Stored Communications Act. In 2000, the House Committee on the Judiciary held hearings on a bill containing provisions for reporting on government access to information under the Stored Communications Act. The House Report on that bill noted the lack of "publicly available data on which to base" an assessment of the "effects of governmental access to e-mail and other

---

163 Improving Foreign Intelligence Surveillance to Defend the Nation and the Constitution Act of 2007, HR 3356, 110th Cong, 1st Sess, in 153 Cong Rec H 9685 (Aug 3, 2007). This bill also required FISC approval of each application for electronic surveillance under it. Id. For a previous bill that would have more narrowly amended FISA to permit NSA access to foreign transit data, see Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006, S 3877, 109th Cong, 2d Sess (Sept 7, 2006). See also Editorial, *Spying on Americans*, NY Times A20 (May 2, 2007) ("[Senator Diane Feinstein] offered some sensible changes for FISA, but the administration and the Republican majority in the last Congress buried her bill.").

164 Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from Within*, 115 Yale L J 2314, 2341–42 (2006).

computer communications."[165] The bill's reporting requirements would roughly track those of the Pen Register Act's provisions.[166]

Third, the annual index should include expanded information about government activity under FISA. For example, Peter Swire advocates "greater reporting to Congress and the public on how FISA is used in criminal cases."[167] The Wiretap Act offers a useful model in this regard; it requires reports on the number of prosecutions and convictions. Swire suggests, moreover, that to the extent that new legal arguments are presented to the FISA court, this information should be made public.[168] In addition, as part of a sorely needed revisiting of the Protect America Act before it sunsets, Congress should adopt a system for collecting information about the annual number of "certifications and directives issued" under the statute's carve-out from the FISA warrant requirements as well as the number of US persons whose communications were intercepted.

Fourth, the idea of an annual index requires harmonization of the information collected. The goal should be to give a clear picture of how activities in different statutory areas relate to one another. Existing reporting requirements should also be tweaked to improve their quality. A few examples will suffice. FISA should be amended to separate statistics for physical and electronic searches. Wiretap Act reports should include information about the number of connections placed under surveillance per year, and not merely the number of orders. Moreover, Wiretap Act reports should require jurisdictions that have no activity in a given year to file a report with it. Such filing will insure that a zero for the jurisdiction reflects no surveillance activity, rather than a report never sent to the Administrative Office.

Fifth, there should be audit functions under telecommunications surveillance statutes. As an example, the Pentagon's Technology and Privacy Advisory Committee called in 2004 for annual audits of any data mining programs involving personal information of US citizens.[169]

---

165 Electronic Communications Privacy Act of 2000, HR Rep No 106-932, 106th Cong, 2d Sess 10 (2000) (lamenting that there was little data with which to understand the effects of the Electronic Communications Privacy Act of 1986).

166 See id (annual required reporting included: the fact that an order was applied for, the type of order applied for, whether the order was granted, the predicate offense, and the agency applying for the order).

167 Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo Wash L Rev 1306, 1367 (2004).

168 See id.

169 DOD, Technology and Privacy Advisory Committee, *Safeguarding Privacy in the Fight against Terrorism* 52 (Mar 2004), online at http://www.cdt.org/security/usapatriot/20040300tapac.pdf (visited Jan 12, 2008) (recommending that the government adopt additional privacy precautions when collecting private data, and suggesting that these additional precautions will eventually aid various agencies in protecting national security).

There should also be independent investigation of law enforcement activities under the other statutes.

CONCLUSION

In 1967, one year before enactment of the Wiretap Act, the President's Commission on Law Enforcement and Administration of Justice warned of the risks of unregulated governmental surveillance. The Commission stated, "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively."[170] This warning has the even greater resonance today—the amount of personal data that individuals generate now is vastly greater than in 1967. The legal structure for regulating telecommunications surveillance by the government should be reformed. This essay has described areas for needed attention and suggested an initial set of needed steps.

[170] President's Commission on Law Enforcement and Administration of Justice, *The Challenge of Crime in a Free Society* 202 (GPO 1967).