Privacy, Surveillance, and Law

Richard A. Posner†

"Privacy" is a word of many meanings. The meaning that is most relevant to this essay is secrecy—the interest in concealing personal information about oneself. But I need to distinguish between a person's pure interest in concealment of personal information and his instrumental interest, which is based on fear that the information will be used against him. In many cultures, including our own, there is a nudity taboo. Except in the sex industry (prostitution, striptease, pornography, and so forth), nudist colonies, and locker rooms, people generally are embarrassed to be seen naked by strangers, particularly of the opposite sex, even when there are no practical consequences. Why this is so is unclear; but it is a brute fact about the psychology of most people in our society. A woman (an occasional man as well) might be disturbed to learn that nude photographs taken surreptitiously of her had been seen by a stranger in a remote country before being destroyed. That invasion of privacy would not have harmed her in any practical sense. Yet it might cause her at least transitory emotional distress, and that is a harm even if it seems to have no rational basis (in that respect it is no different from having nightmares after watching a horror movie—another emotional reaction that is real despite being irrational from an instrumental standpoint). But if the stranger used the photos to blackmail her, or, in an effort to destroy her budding career as an anchorwoman for the Christian Broadcasting System, published the photos in *Hustler* magazine, she would have a different and stronger grievance.

In many cases of instrumental concealment of personal information, the motive is disreputable (deceptive, manipulative): a person might want to conceal his age, or a serious health problem, from a prospective spouse or his criminal record from a prospective employer. But the motive is not disreputable in all cases; the blackmailed woman in my example was not trying to mislead anyone in resisting the publication of the photos.

---

† Judge, United States Court of Appeals for the Seventh Circuit; Senior Lecturer in Law, The University of Chicago. This is a revised draft of my talk at The University of Chicago Law School's Surveillance Symposium, June 15–16, 2007. I draw heavily on my books *Not a Suicide Pact: The Constitution in a Time of National Emergency* ch 6 (Oxford 2006) and *Countering Terrorism: Blurred Focus, Halting Steps* ch 7 (Rowman & Littlefield 2007).

Legitimate deliberative activity is another example of legitimate instrumental concealment, because publicity hampers communication. When people are speaking freely, they say things that eavesdropping strangers are likely to misconstrue. When they speak guardedly because they are afraid that a stranger is listening in, the clarity and candor of their communication to the intended recipients are impaired. There is a social value in frank communications, including being able to try out ideas on friends or colleagues without immediate exposure to attacks from rivals or ill wishers. Legitimate strategic plans also require secrecy to be effective. Competition would be impaired if business firms could eavesdrop on competitors' planning sessions or otherwise appropriate their trade secrets with impunity.

These things are true of government as well as of private individuals and firms. Civil libertarians want government to be transparent but private individuals opaque; national security hawks want the reverse. People hide from government, and government hides from the people, and people and government have both good and bad reasons for hiding from the other. Complete transparency paralyzes planning and action; complete opacity endangers both liberty and security. Terrorists know this best. Eavesdropping imposes costs on innocent people because their privacy is compromised; but the costs it imposes on terrorists are even steeper because it thwarts their plans utterly and places them at risk of capture or death. Of course, from our standpoint as a people endangered by terrorism, the higher those costs the better.

Many people are frightened of the eavesdropping potential of modern computer technology. Suppose that the listening devices of the National Security Agency (NSA) gathered the entire world's electronic communications traffic, digitized it, and stored it in databases; that the digitized data were machine-searched for clues to terrorist activity; but that the search programs were designed to hide from intelligence officers all data that furnished no clues to terrorist plans or activity. (For all one knows, the NSA is doing all these things.) The data vacuumed by the NSA in the first, the gathering, stage of the intelligence project would, after screening by the search programs, present intelligence officers with two types of communication to study: communications that contained innocent references to terrorism and communications among the terrorists themselves. Engaging in either type of communication would be discouraged once people realized the scope of the agency's program, but the consequences for the nation would be quite different for the two types. Discouraging innocent people from mentioning anything that might lead a computer search to earmark the communication for examination by an intelligence officer would inhibit the free exchange of ideas on matters of public as

well as private importance. But discouraging terrorists from communicating by electronic means would discourage terrorism. Foreign terrorists would find it difficult to communicate with colleagues or sympathizers in the United States if they had to do so face to face or through messengers because they would know the government was eavesdropping on all their electronic communications. This is simply my earlier point writ large: protected communications are valuable to the persons communicating, whether they are good people or bad people, and this duality is the source of both the costs and the benefits of intercepting communications for intelligence purposes.

A further distinction, at once critical and problematic, is between the involuntary and the voluntary disclosure of personal information. The former is illustrated by surreptitious interception of letters, email, phone conversations, and other communications. Another illustration is the installation on a large scale (as in London) of surveillance cameras that photograph pedestrians, a security measure that enabled the identification of the terrorists who attacked the London transit system in 2005. If an entire city is known to be under camera surveillance, the surveillance is not surreptitious, but submission to it is as a practical matter involuntary except for people who never leave their homes.

A far greater amount of personal information is revealed voluntarily than involuntarily, as these words are conventionally used. But the case of the pervasive surveillance cameras, avoidable only by never leaving one's home or by moving to another city, suggests that the distinction is often tenuous. No one is required to drive and therefore to have a driver's license. But if you want to drive legally, you need a license, and to get a license you must disclose certain personal information to the motor vehicle bureau; and driving is a practical necessity for most adult Americans. A federal statute forbids colleges and other educational institutions to reveal a student's grades without his or her consent. Yet virtually all students give their consent because otherwise a prospective employer is likely to assume the worst. (If no students disclosed voluntarily, the employer would be stymied; but the best students have a strong incentive to disclose, and once they disclose the next tier has a similar incentive, and so on until the entire privacy policy unravels.) To get a good job, to get health and life insurance, to get bank credit, to get a credit card, you need to reveal personal information. Every time you make a purchase other than with cash you convey information about your tastes, interests, and income that may well end up in some easily accessible database. Every time you use E-ZPass or some equivalent automatic toll system, your location is recorded. Digitizing medical records helps doctors and patients by making it much easier, swifter, and cheaper to transfer these records when a patient switches doctors, is treated by a new doctor in an

emergency, or needs to consult a specialist. But once the records are digitized, rather than existing solely in the form of hard copies in the office of the patient's primary physician, the physician-patient privilege is undermined because the risk that unauthorized persons will gain access to the records is increased. Nevertheless the movement to digitize medical records is inexorable.

The *reductio ad absurdum* would be to argue that since you do not have to own a phone, if the government announces that it is going to tap all phones and you continue using your phone, you have "voluntarily" disclosed the content of your calls to the government. That is a bad argument (and likewise if the government decides to read your emails), but it would not be if the issue were government access to digitized medical records, even if the government *required* all medical records to be digitized and sharable over the internet. That measure would have a justification unrelated to a desire to snoop; and the disclosure of medical information to the doctor in the first place, the information that goes into the records, is voluntary.

As these examples suggest, a person would have to be a hermit to be able to function in our society without voluntarily disclosing a vast amount of personal information to a vast array of public and private demanders. This has long been true, but until quite recently the information that people voluntarily disclosed to vendors, licensing bureaus, hospitals, public libraries, and so forth, was scattered, fugitive (because the bulkiness of paper records usually causes them to be discarded as soon as they lose their value to the enterprise), and searchable only with great difficulty. So although one had voluntarily disclosed private information on innumerable occasions to sundry recipients, one retained as a practical matter a great deal of privacy. But with digitization, not only can recorded information be retained indefinitely at little cost, but also the information held by different merchants, insurers, and government agencies can readily be pooled, opening the way to assembling all the recorded information concerning an individual in a single digital file that can easily be retrieved and searched. It should soon be possible—maybe it is already possible—to create comprehensive electronic dossiers for all Americans, similar to the sort of dossier the FBI compiles when it conducts background investigations of applicants for sensitive government employment or investigates criminal suspects. The difference is that the digitized dossier that I am imagining would be continuously updated.

The personal information that an organization collects in the course of its dealings with its customers and employees often has commercial value to another organization as well, to which the collector might therefore sell the information. Through such transactions, expanding pools of personal information about individuals are cre-

ated. The rational seller will, it is true, balance the profit from such a sale against the cost in possible loss of customers. Many people are reluctant to provide personal information to a supplier, an insurer, and so forth, without a contractual assurance that the information will not be resold to another organization; and so such assurances are common. Nevertheless, a vast amount of personal information is exchanged and pooled because much information is in official records that the public is legally entitled to inspect (such as registries of title to real estate and most court records, including records of bankruptcy proceedings, often rich in personal information), or because it has found its way onto the web or was disclosed accidentally or deliberately despite a promise not to disclose it, or because the customer failed to demand a promise of confidentiality. Also, digitized information tends to have many more loci than paper documents. It usually resides in a number of different computers to which many persons may have access—including hackers. Living a normal American life, one cannot avoid disclosing to strangers a tremendous amount of personal information that will find its way into publicly accessible, readily searchable databases; and so one's privacy, or much of it, is blown.

At this point, however, I must introduce a further distinction: between the desire to conceal information about oneself (privacy as secrecy) and the desire that such information not be used against oneself (a subset of privacy as secrecy). Americans are not known for reticence or personal modesty. Most of us are quite casual about disclosing personal information to strangers, provided it is not likely to boomerang against us. The widespread use of that most indiscreet of communications media, the internet, is not the only evidence of this. People have become blasé about having their personal belongings x-rayed, and their persons searched, by security personnel at airports. They are overheard everywhere talking loudly on cell phones. They are oblivious to the mushrooming of surveillance cameras, interior as well as exterior. Fewer people make use of encryption programs to conceal their electronic communications than invite strangers to read their correspondence; Gmail, Google's popular email service, automatically searches the text of an email and posts advertisements keyed to its content.

The fact that one cannot negotiate modernity without continuously revealing personal information to a variety of demanders has habituated most Americans to radically diminished informational privacy. In this new culture of transparency, the degree to which a disclosure of personal information inflicts harm on a person depends less on what information is disclosed than to whom and to how many, and to what use it is put by the persons to whom it is disclosed. Maybe most of us no longer care much if strangers know intimate details of our

private lives, though this depends on who the strangers are and whether the details that each possesses are likely to be combined to create a comprehensive dossier.

Intelligence officials like to say that the information they are interested in is actually more limited than the information that a medical provider or public health officer, a prospective spouse or employer, a health or life insurer, or even a bank or other seller of goods or services would like to have. That is both correct and incorrect. In the initial computer sifting designed to pick out data meriting scrutiny by an intelligence officer, only facts bearing on national security will trigger scrutiny. But once an individual is identified as a possible terrorist or foreign agent, the government's interest in him will explode. Besides obtaining contact information, it will want to learn about his ethnicity and national origin; education and skills; previous addresses and travel (especially overseas); family, friends, and acquaintances; political and religious beliefs and activities; finances; any arrest or other criminal record; military service (if any); mental health and other psychological attributes; and a range of consumption activities, the whole adding up to a comprehensive personal profile.

If these profiles are digitized, pooled, and searched electronically to reveal links and interactions among individuals, the intelligence services will have access to a body of information of potentially very great utility for identifying and tracking members of terrorist cells and piecing together their financial and other support networks. They will, for example, know everything that Amazon.com knows about an individual's preferences in books and movies because they will have gotten the information from Amazon.com, and they will know a great deal more about the individual by pooling that information with information from other sources, public and private. This indicates, by the way, the great extent to which national security data gathering does *not* depend on electronic surveillance that would raise questions under the Fourth Amendment or under statutes such as Title III (the general federal wiretap statute)[1] or the Foreign Intelligence Surveillance Act[2] (FISA). The Defense Department's Able Danger project[3]

---

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

2 Foreign Intelligence Surveillance Act of 1978, Pub L No 95-511, 92 Stat 1783, codified as amended at 50 USC § 1801 et seq (2007).

3 Shane Harris, *Army Project Illustrates Promise, Shortcomings of Data Mining*, Government Executive (Dec 7, 2005), online at http://www.govexec.com/dailyfed/1205/120705nj1.htm (visited Jan 12, 2008) (describing the Able Danger project and the extensive use of data mining for intelligence gathering).

demonstrated that valuable intelligence could be obtained without the kind of surveillance that normally requires a warrant.

Privacy is the terrorist's best friend, and the terrorist's privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: the internet, with its anonymity, and the secure encryption of digitized data which, when combined with that anonymity, make the internet a powerful tool of conspiracy. The government has a compelling need to exploit digitization in defense of national security. But if it is permitted to do so, intelligence officers are going to be scrutinizing a mass of personal information about US citizens. And we know that many people do not like even complete strangers poring over the details of their private lives. But the fewer of these strangers who have access to those details and the more professional their interest in them, the less the affront to the sense of privacy. One reason people do not much mind having their bodies examined by doctors is that they know that doctors' interest in bodies is professional rather than prurient; and we can hope that the same is true of intelligence professionals.

I have said both that people value their informational privacy and that they surrender it at the drop of a hat. The paradox is resolved by noting that as long as people do not expect that the details of their health, love life, finances, and so forth, will be used to harm them in their interactions with other people, they are content to reveal those details to strangers when they derive benefits from the revelation. As long as intelligence personnel can be trusted to use their knowledge of such details only for the defense of the nation, the public will be compensated for the costs of diminished privacy in increased security from terrorist attacks.

I now want to bring law into the picture. After the Supreme Court ruled in a conventional criminal case that wiretapping and, by implication, other forms of electronic surveillance were to be deemed "searches" within the meaning of the Fourth Amendment,[4] Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[5] Title III created procedures for obtaining warrants for electronic surveillance that were modeled on the procedures for conventional search warrants.[6] Ten years later—and thus long before the danger of global terrorism was recognized and electronic surveillance

---

4 See *Katz v United States*, 389 US 347, 353 (1967).

5 82 Stat at 211.

6 See Nicholas J. Whilt, *The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties That Make Defense of Our Nation Worthwhile*, 35 Sw U L Rev 361, 371 (2006) (stating that Congress modeled Title III after the constitutional guidelines in *Katz*).

transformed by the digital revolution—the Foreign Intelligence Surveillance Act was enacted.[7] It is a complicated statute, but basically it requires that interceptions in the United States of the international communications of a US citizen, or permanent resident, or of anyone in the United States if the interception is made here, be conducted pursuant to warrants based on probable cause to believe that one of the parties to the communication is a foreign terrorist.

That is the wrong approach as 9/11 has taught us and as Congress is beginning to recognize, evidenced by amendments to FISA enacted since the conference for which this paper was prepared.[8] (The amendments were to be in effect for only six months; Congress is now considering a more permanent restructuring of FISA.) FISA in its pre-amendment form remains usable for regulating the monitoring of communications of known terrorists, but it is useless for finding out who is a terrorist,[9] even though "the problem of defeating the enemy consists very largely of finding him."[10] Hence the importance of "collateral intercepts"—such as intercepts of communications that seem likely to yield information of intelligence value even if probable cause to believe that a party to the communication is a terrorist is lacking.

It is true that surveillance not cabined by a conventional probable cause requirement produces many false positives—interceptions that prove upon investigation to have no intelligence value. But that is not a valid criticism. The cost of false positives must be balanced against that of false negatives. The failure to detect the 9/11 plot was an exceptionally costly false negative. The intelligence services have no alternative to casting a wide net with a fine mesh if they are to have reason-

---

7 See 92 Stat at 1783.

8 See Protect America Act of 2007, Pub L No 110-55, 121 Stat 552, codified at 50 USCA §§ 1805a–c (2007).

9 See, for example, K.A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 Yale J L & Tech 128, 135–36 (2007) (noting that FISA "provides no mechanisms for authorizing advanced technical methods" to identify terrorists); K.A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, NYU Rev L & Sec, Supp Bull on L & Sec 2–3 (Spring 2006), online at http://ssrn.com/abstract=889120 (visited Jan 12, 2008) (noting that FISA "does not provide a mechanism for programmatic pre-approval of technical methods like automated data analysis or filtering that may be the very method for uncovering" connections between individuals and terrorist groups). Taipale's Center for Advanced Studies in Science and Technology Policy has published useful analyses of the use of data mining for national security. See http://www.advancedstudies.org (visited Jan 12, 2008). See also notes 11, 14.

10 Bradley W.C. Bamford, *The Role and Effectiveness of Intelligence in Northern Ireland*, 20 Intell & Natl Sec 581, 586 (2005), quoting Frank Kitson, *Low Intensity Operations: Subversion, Insurgency, Peace-keeping* 95 (Faber 1971).

able prospects of obtaining the clues that will enable future terrorist attacks on the United States to be prevented.[11]

The NSA's Terrorist Surveillance Program—the controversial program, secret until revealed by the *New York Times* in December 2005,[12] for conducting electronic surveillance without warrants and therefore outside the boundaries of FISA[13]—involves an initial sifting, performed by computer search programs, of electronic communications for clues to terrorist activity. The sifting uses both "content filtering" and "traffic analysis" to pick out a tiny percentage of communications to be read. Content filtering is searching for particular words or patterns of words inside the communication. Traffic analysis is examining message length, frequency, and time of communication and other noncontent information that may reveal suspicious patterns; thus traffic analysis cannot be foiled by encryption because the information is not content based.[14] The NSA has obtained call records from telephone companies to aid in its traffic analysis. If the agency has the phone number of a known or suspected terrorist, it can use call records to determine the most frequent numbers called to or from that number, and it can then determine the most frequent numbers called to or from those numbers and in this way piece together a possible terrorist network—all without listening to any conversation. That comes later.

So the search sequence is interception, data mining, and finally a human search of those intercepted messages that data mining or other

---

11 A further drawback of FISA is that it is now possible to buy a VoIP (Voice over Internet Protocol) telephone to which a local US phone number can be assigned even if the phone is used outside the United States. See Taipale, 9 Yale J L & Tech at 147 n 51 (cited in note 9). Two terrorists in Pakistan could be talking to each other by means of such phones yet the NSA would think it a conversation between two US persons in the United States, which FISA does not permit the government to intercept. This is an example of how FISA has been rendered obsolete by unanticipated technological advances.

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

13 For a range of views on the legality of the program (whatever exactly it is), see generally *Terrorist Surveillance and the Constitution* (Federalist Society 2006).

14 See Hazel Muir, *Email Gives the Game Away*, New Scientist 19 (Mar 29, 2003) (discussing technology that uses computer algorithms to analyze emails to potentially identify criminal or terrorist networks). Skeptics of the value of data mining for intelligence abound. See, for example, Jeff Jonas and Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining* 2 (Cato Institute 2006) (acknowledging the potential benefits of data mining but arguing that it should not be used because it would waste taxpayer dollars and infringe on privacy and civil liberties). But see Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs, Hearing before the Senate Committee on the Judiciary, 110th Cong, 1st Sess 154 (2007) (testimony of Kim A. Taipale, Executive Director, Center for Advanced Studies in Science and Technology Policy) (rebutting the skeptics of data mining by advocating its value and asserting that it can help promote security while still protecting privacy if properly designed).

information sources have flagged as suspicious. Computer searches do not invade privacy because search programs are not sentient beings. Only the human search should raise constitutional or other legal issues.

Communications read by an intelligence officer and thus "searched" in the legal sense could as a technical matter include what FISA forbids unless there is probable cause to believe that a party to the communication is a terrorist or an agent of a foreign power: communications to which a US citizen is a party, communications to which a person (not necessarily a citizen) in the United States and a person abroad are parties (if intercepted in the United States), and communications that are entirely domestic. Although the Bush Administration has denied that it is monitoring purely domestic communications, such monitoring is within the Terrorist Surveillance Program's feasible technical scope.

A Senate bill (S 2453 in the last Congress) to revise FISA contemplated the submission of the Terrorist Surveillance Program and any future such programs to the Foreign Intelligence Surveillance Court for an opinion on its legality[15]—a problematic procedure because federal courts are forbidden to render advisory opinions. A court might even hold that a surveillance "program," as distinct from the surveillance of a specific, named individual, is a "general warrant," which the Fourth Amendment expressly forbids.

In an abrupt about face, the Bush Administration announced on January 17, 2007 that henceforth it would seek warrants for interceptions of the sort that the NSA had been conducting without warrants under the Terrorist Surveillance Program.[16] The reason suggested in media accounts was that negotiations with the Foreign Intelligence Surveillance Court had reassured the Administration that the court would issue warrants for such interceptions. There was thus a whiff of S 2453 and a hint of a revised understanding by the Foreign Intelligence Surveillance Court of the outer boundaries of FISA; for it seems that the program would continue, only with warrants. General Hayden, the author of the program when he was Director of the NSA, had said it involved a "subtly softer trigger" for an interception than the Act allowed.[17] This implied, if the program was indeed unchanged,

---

15 See S 2453, 109th Cong, 2d Sess (Mar 16, 2006), in 152 Cong Rec S 2313 (Sept 13, 2006). The full text of the bill can be found at http://www.govtrack.us/data/us/bills.text/109/s/s2453.pdf (visited Jan 12, 2008).

16 See Eric Lichtblau and David Johnston, *Court to Oversee U.S. Wiretapping in Terror Cases*, NY Times A1 (Jan 18, 2007).

17 Shane Harris and Tim Naftali, *Tinker, Tailor, Miner, Spy: Why the NSA's Snooping Is Unprecedented in Scale and Scope*, Slate Magazine (Jan 3, 2006), online at http://www.slate.com/id/2133564 (visited Jan 12, 2008).

that the Foreign Intelligence Surveillance Court was willing to bend the Act to bring the Bush Administration back into the fold. Other possibilities, however, were that the program had proved unproductive, that the Administration was hoping to moot legal challenges to the program that it expected to lose, or that it did not think it could convince a Democratic Congress to amend the Act to the Administration's liking.

The recent amendments to which I have referred have clarified the situation somewhat, though only temporarily since, as I said, they expire in six months.[18] They seem not to be addressed to data mining, and the extent to which that is being conducted remains unclear. They authorize the attorney general and the director of national intelligence to implement a program of intercepting electronic communications for the purpose of conducting surveillance on persons "reasonably believed" to be abroad, even if the other parties to their communications are inside the United States and are US citizens and even if the interceptions take place in the United States. Notably, there is no requirement of a warrant for such interceptions. However, the procedures that the government adopts for implementing this surveillance program have to be submitted to the Foreign Intelligence Surveillance Court, which can invalidate them if it determines that they are a "clearly erroneous" implementation. (That court is an Article III court, and Article III courts may not render advisory opinions—which places this provision of the amendments under a cloud.) Communications carriers are required to cooperate with the government in intercepting the communications covered by the program.

What is most notable about the amendments, as indeed of the Terrorist Surveillance Program to which they seem addressed, is their backing away from reliance on warrants to prevent abuses of electronic surveillance. The warrant is a poorly designed means for balancing the security and liberty interests involved in counterterrorist surveillance. It is true that instead of requiring probable cause to believe that the target of an interception is a terrorist, FISA could be amended to require merely reasonable suspicion. But even that would be too restrictive from the standpoint of effective counterterrorism; effective surveillance cannot be confined to suspected terrorists when the object is to discover who may be engaged in terrorism or ancillary activities. Further attenuation of FISA's standard for obtaining a warrant might be possible without running afoul of the Fourth Amendment. Conceivably the issuance of a warrant could be authorized on the basis of a showing that while the target was probably not a terrorist, national security required making assurance doubly sure by inter-

---

[18] For the text of the amendments, see Protect America Act of 2007, 121 Stat at 552.

cepting some of his electronic communications. A model might be the criterion for issuing a search warrant to the Canadian Security Intelligence Service, where a warrant can be issued on the basis of a factually supported "belief, on reasonable grounds, that [it] ... is required to enable the Service to investigate a threat to the security of Canada."[19] Such a criterion might pass muster under the Fourth Amendment, which requires probable cause for the issuance of a warrant but does not state what it is that there must be probable cause to believe. The Supreme Court has said that there must be probable cause to believe that the search will yield contraband or evidence of crime—when the search is part of a criminal investigation.[20] The Constitution binds the government more tightly when it is exerting its powers to convict people of crimes than in other areas of government activity. A search intended not to obtain evidence of crime but to obtain information about terrorism might, as under Canadian law, require only probable cause to believe that the search would yield such information.

The lower the standard for getting a warrant, however, the more porous the filter that the requirement of a warrant creates, bearing in mind the ex parte character of a warrant proceeding. If all the application need state is that an interception might yield data having value as intelligence, judges would have no basis for refusing to issue the warrant. Alternatively, reliance on warrants could invite legislation to expand the reach of the criminal laws relating to terrorism in order to make it easier to establish probable cause to believe that a search will reveal evidence of a crime. That expansion could raise issues under the First Amendment, since the natural route for expanding criminal laws against terrorism is to criminalize extremist speech or even attendance at extremist (though peaceful) speeches and rallies, as activities that may be preparatory to or encouraging of terrorism.

Warrants that satisfy FISA's standard as traditionally understood should continue to be required for all physical searches, because they are far greater intrusions on privacy than electronic interceptions, and for all electronic surveillance for which FISA's existing probable cause requirement can reasonably be satisfied (mainly cases in which the government wanted to intercept communications of a person who they had probable cause to believe was a terrorist). With these exceptions, civil libertarians' preoccupation with warrants is not only harmful to national security (and possibly to civil liberties if it induces legislation to expand the reach of the criminal law) but also anachronistic.

---

19 Canadian Security Intelligence Service Act, RSC, ch C-23, § 21(2)(a) (1993).

20 *Zurcher v Stanford Daily*, 436 US 547, 554 (1978) ("Under existing law, valid warrants may be issued to search *any* property ... at which there is probable cause to believe that fruits, instrumentalities, or evidence of a crime will be found.").

The government's ready access to the vast databases that private and public entities compile for purposes unrelated to national security has enabled it to circumvent much of the protection of privacy that civil libertarians look to warrant requirements to secure.[21]

There are a number of possible measures, apart from requiring warrants, that Congress could adopt in order to minimize abuses of domestic surveillance. If all were adopted, the risk of such abuses would be slight. The temporary FISA amendments take tiny steps in this direction. Bolder steps would include the following:

1. Congress could create a steering committee for national security electronic surveillance, composed of the attorney general, the director of national intelligence, the secretary of homeland security, and a retired federal judge or justice appointed by the chief justice of the Supreme Court. The committee would monitor all such surveillance to assure compliance with the Constitution and federal statutes. The requirement in the temporary amendments that the attorney general and the director of national intelligence devise procedures for a new warrantless surveillance program is one of the tiny steps to which I referred.[22] The other, and legally dubious one, is requiring submission of the procedures for approval by the Foreign Intelligence Surveillance Court; that court becomes in effect the steering committee.
2. The NSA could be required to submit to the steering committee, to departmental inspectors general, to the Privacy and Civil Liberties Oversight Board (a White House agency created by the Intelligence Reform Act), to the congressional intelligence and judiciary committees, and to an independent watchdog agency of Congress modeled on the GAO every six months a list of the names and other identifying information of all persons whose communications had been intercepted in the previous six months without a warrant, with a brief statement of why these persons had been targeted.
3. The responsible officials of the NSA could be required to certify annually to the watchdog groups that there had been no violations of the statute during the preceding year. False certification would be punishable as perjury. But lawsuits challenging the legality of the Terrorist Surveillance Program should be precluded.

---

21 See, for example, Arshad Mohammed and Sara Kehaulani Goo, *Government Increasingly Turning to Data Mining; Peek into Private Lives May Help in Hunt for Terrorists*, Wash Post D3 (June 15, 2006) (discussing the government's extensive purchasing of consumer and other personal information from private companies for data mining purposes).

22 See Protect America Act of 2007, 121 Stat at 552–53.

Such lawsuits would distract officials from their important duties to no purpose if the kind of statute that I am suggesting were enacted. The statute should sunset after five years.

4. The use of intercepted information for any purpose other than investigating threats to national security would be forbidden. Information could not be used as evidence or leads in a prosecution for ordinary crime—this to alleviate concern that wild talk bound to be picked up by electronic surveillance would lead to criminal investigations unrelated to national security.

   Violations of this provision would be made felonies punishable by substantial prison sentences and heavy fines. But the punishments must not be made too severe lest they cause intelligence officers to steer so far clear of possible illegality that they fail to conduct effective surveillance. The risk of abuses is not great enough to justify savage penalties in order to deter them, because intelligence officers have no interest in assisting in the enforcement of criminal laws unrelated to national security. A neglected point is that violations of privacy and civil liberties tend to emanate from the White House and the top management level of executive branch agencies rather than from the working or middle-management levels.

5. To limit the scope of surveillance, "threats to national security" should be narrowly defined as threats involving a potential for mass deaths or catastrophic damage to property or to the economy. That would exclude, for the time being anyway, ecoterrorism, animal-rights terrorism, and other political violence that, though criminal, does not threaten catastrophic harm (yet).

Congressional action is also needed to protect the phone companies that cooperated with the NSA's surveillance program from potentially immense liability for allegedly having violated federal law protecting the privacy of telephone records; a number of suits are pending. The intelligence system is enormously dependent on informal assistance from private companies in communications, banking, and other industries. At times such assistance is made a legal duty, as in the federal law requiring banks to report cash transactions of $10,000 or more; and this is also a feature of the new amendments to FISA.[23] Were it not for the threat of liability, which the amendments do not address, voluntary assistance would probably as in the past be all the government needed. But if voluntary assistance—even when tendered in a national emergency, as in the wake of the 9/11 terrorist attacks—

---

23 Protect America Act of 2007, 121 Stat at 552.

places companies in legal jeopardy, such assistance will dry up. FISA needs to be amended not only to authorize more extensive domestic surveillance than its anachronistic terms permit but also to insulate from liability conduct that may have violated the Act or some other statute but that would be permitted under the amended regime.

Until the temporary amendments were enacted, the type of approach that I am advocating (call it the "nonwarrant" approach) for regularizing domestic surveillance was getting little attention from Congress and the Bush Administration, possibly because the Administration wanted to retain a completely free hand and thought it could fend off the sort of restrictions that I have sketched. (It is remarkable how tepid the public reaction to the Terrorist Surveillance Program has been.) A related possibility is that the Administration's aggressive claims of presidential power prevented it from acknowledging the legitimacy of congressional controls over intelligence and hence of a legislative solution to the controversy over the program. Still another possibility was (and is) that because no one is in charge of domestic intelligence, authority over which is divided among the attorney general, the FBI director, the Department of Homeland Security, and the director of national intelligence (among others), no one is formulating a comprehensive legislative and public relations strategy for ending the controversy over the role of electronic surveillance in such intelligence. (At this writing, the only confirmed senior official in the Justice Department is the solicitor general.) And another possibility is the grip of our legalistic culture, which makes us think that the regulation of national security *must* be modeled on the regulation of criminal law enforcement. The temporary amendments suggest, however, that the logjam may be breaking, though one of the reasons, it appears, is that the Administration's decision to bring the Terrorist Surveillance Program under FISA resulted in a paper jam at the Foreign Intelligence Surveillance Court as the number of warrant applications soared.

We should be playing to our strengths, and one of the greatest of them is technology. We may not be able to prevail against terrorism with one hand tied behind our back. Critics of surveillance argue that since our enemies know that we monitor electronic communications, they will foil us by simply ceasing to use such communications. That is wrong. We know it is wrong because we do intercept terrorist communications.[24] But if it were true that our monitoring caused the terrorists to abandon the telephone and the internet, that would be an enor-

---

[24] See, for example, James Bamford, *"He's in the Backseat!,"* Atlantic Monthly 67 (Apr 2006) (describing the NSA's interception of communications from a suspected Yemeni terrorist and the concomitant drone strike).

mous victory for counterterrorism, as it is extremely difficult to coordinate and execute a major terrorist attack if all communications among the plotters must be face to face to avoid detection. The greater danger is that encryption and other relatively cheap and simple countermeasures will defeat our surveillance.

Opponents of efforts to amend FISA point out that the Foreign Intelligence Surveillance Court has almost never turned down an application for a warrant. In 2005, for example, although more than 2,000 applications were filed, not a single one was denied in whole or in part.[25] The inference the critics wish drawn is that FISA is not inhibiting surveillance. The correct inference is that the Justice Department is too conservative in seeking warrants. The analogy is to a person who has never missed a plane in his life because he contrives always to arrive at the airport eight hours before the scheduled departure time. The effect of our legalistic culture is to cause law enforcement agencies, notably the FBI, to avoid not only violating the law but also steering so close to the wind that they might be accused, albeit groundlessly, of violating the law or of being "insensitive" to values that inform the law, even when those values have not been enacted into law.

---

[25] Letter from William E. Moschella, Assistant Attorney General, to J. Dennis Hastert, Speaker of the House of Representatives 2 (Apr 28, 2006), online at http://www.fas.org/irp/agency/doj/fisa/2005rept.pdf (visited Jan 12, 2008).