DISTINGUISHED LECTURE

SURVEILLANCE AND THE CONSTITUTION

CHRISTOPHER SLOBOGIN†

Table of Contents

I. INTRODUCTION

It is an honor and a pleasure to give this lecture to the students and faculty of Wayne State University Law School. I am also glad this lecture is open to members of the public. The topic I am addressing today—surveillance by the government—concerns all of us as citizens in a democratic society.

Let me start by asking a few questions. In the past several years, have you made a phone call or sent an email overseas? Have you walked the streets of Washington, D.C., Baltimore, Maryland, or Chicago, Illinois? Have you patronized a bank, paid a phone bill, used a credit card, or bought an airplane ticket? If you have done any of these things, and I assume virtually all of you have, then the chances are good that you have been under surveillance by the government, that you have been

† Milton Underwood Professor of Law, Vanderbilt University Law School. A.B., 1973, Princeton University; J.D., 1977, University of Virginia Law School; L.L.M., 1979, University of Virginia Law School. This Article is a slightly revised version of a Distinguished Lecture delivered at Wayne State University Law School on Feb. 26, 2009.

overheard, observed, or had your records accessed by the FBI, the National Security Agency (NSA), or some other federal or state law enforcement authority.

Today I want to talk about the extent of this surveillance and why it is so easy for the government to carry it out. I will also talk about why government surveillance should be more heavily regulated. Finally, I will briefly discuss what a new regulatory regime might look like. My focus will be on the extent to which the Constitution limits government surveillance activities. The details of regulation should be statutory, but the basis for that statutory regulation must be founded on constitutional principles to ensure that it cannot be legislatively nullified during the next moral panic, the next terrorist attack, or not to put too fine a point on it, the next time a Dick Cheney comes into power.

The primary source of that constitutional regulation is the Fourth Amendment. The Fourth Amendment prohibits unreasonable searches and seizures and requires that warrants for searches and seizures be based on probable cause and describe the object of the search.[1] This is the amendment that places limitations on government efforts to conduct searches of homes and cars, and make stops and arrests.

Although this amendment is the fourth in line, it has been called the most important part of the Bill of Rights, even more important than the First Amendment's guarantee of free speech, association, and press,[2] because without security from government intrusions and monitoring, speech and association are chilled and perhaps even silenced, and sources for the media can be choked off. As Monrad Paulsen observed:

> The basic . . . problem of a free society is the problem of controlling the public monopoly of force. All the other freedoms, freedom of speech, of assembly, of religion, of political action, presuppose that arbitrary and capricious police action has been restrained. Security in one's home and person is the fundamental right without which there can be no liberty.[3]

Unfortunately, even with President Obama and a more civil liberties-oriented crowd in power, these days it's hard to find a reason to celebrate the Fourth Amendment. A much more apt ceremony would be a funeral service. Some obvious examples of why we should mourn the Fourth Amendment are the Supreme Court's two recent cases strongly

1. U.S. CONST. amend. IV.

2. U.S. CONST. amend. I.

3. Monrad G. Paulsen, *The Exclusionary Rule and Misconduct by the Police*, *in* POLICE POWER AND INDIVIDUAL FREEDOM 87, 97 (Claude R. Sowle ed., 1962).

suggesting that the exclusionary rule—the primary means of enforcing the Fourth Amendment—is on its way out.[4] But my focus will not be on the remedy for Fourth Amendment violations, which involves the back-end of the analysis, but rather on the analysis at the front-end: when is the Fourth Amendment implicated in the first instance? Here too Fourth Amendment jurisprudence is in bad shape, and nothing illustrates that conclusion better than a look at the minimal impact that this jurisprudence has on government surveillance techniques.

Over the past couple of years there has been a vast uptick in surveillance programs, ranging from mass interception of overseas phone calls by the NSA to the establishment of elaborate video camera systems in our major cities, from the use of satellite technology to the well-known Total Information Awareness initiative sponsored by Admiral Poindexter. All of these programs, about which I will say more later, involve searches for information and often result in seizures of tangible items. But according to the U.S. Supreme Court, none of them trigger the Fourth Amendment. Most of the relevant Supreme Court case law pre-existed 9/11. But with the events of that day any chance of reversing it has diminished significantly, given the concern that such a reversal would handcuff government efforts to nab terrorists.

My key point is that, despite our justifiable fear of terrorism and crime more generally, we should be concerned about these legal developments. Although many of you may believe that the types of surveillance I just described do not affect you or do not have significant adverse effects on the country, in fact they can have real negative consequences. Congress and the executive branch, if not the courts, need to be made more aware of these consequences. If we can succeed at that goal, the spirit of the Fourth Amendment can remain alive even if the Supreme Court continues to affirm its precedents.

I will start by describing in more detail some of the surveillance programs and techniques in existence today and how the Fourth Amendment applies to them. I am going to divide these techniques into three different types of surveillance. The first category is surveillance of our communications, whether they occur over the phone or via email (sometimes called electronic surveillance). The second category is surveillance of our physical activities as we go about our daily lives, using video cameras, spy satellites, see-through technology that can penetrate walls and clothing, tracking devices and the like. Finally, there is surveillance of our transactions, carried out by accessing our credit

4. *See* Herring v. United States, 129 S. Ct. 695 (2009); Hudson v. Michigan, 547 U.S. 586 (2006).

card histories, bank, medical and school records, and other documentations of what we have done in the past. I will describe each type of surveillance and its current constitutional and statutory regulation, which in most cases turns out to be minimal. Then I will talk about why this minimal regulation is a bad thing and how we can rectify it.

II. COMMUNICATIONS SURVEILLANCE

Let's begin with communications surveillance. The government has been wiretapping and bugging conversations since early in the twentieth century.[5] In recent years, this communications surveillance technology has become very sophisticated. Not only can phones be tapped and email messages be intercepted, but face-to-face conversations can be monitored from a long distance away, and even through walls, using vibrations off of windowpanes.[6]

Normally, under the Fourth Amendment and Title III of the United States Code, this type of communications surveillance cannot take place unless a judge has issued a warrant based on a finding of "probable cause;" in other words, a finding that it is more likely than not that evidence of crime will be discovered.[7] The idea behind the warrant requirement is to ensure that an independent agent, "a judicial officer," double checks the law enforcement officer's opinion, and that there is a credible basis for that opinion, not merely a hunch or speculation. Otherwise the fear is that law enforcement officers, in their enthusiasm to catch criminals, will use their considerable powers to harass people who turn out to be innocent, and perhaps even people they *know* to be innocent but whom they target because of their skin color, ethnicity, or some other inappropriate characteristic. As Justice Jackson said:

> The point of the Fourth Amendment is not that it denies law enforcement the support of the usual inferences reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.[8]

5. *See* Berger v. New York, 388 U.S. 41 (1967).
6. *Id.*
7. *Id.*; *see also* 18 U.S.C.A. § 2518 (West 2009).
8. Johnson v. United States, 333 U.S. 10, 13-14 (1948).

Research conducted by the National Center for State Courts shows that even when magistrates do no more than look over the warrant application and ask a few questions, the warrant requirement makes police think twice before acting and curbs their natural tendency to be suspicious about everything and everybody.[9]

That is why the most recent developments in connection with national security surveillance have occasioned so much controversy. National security surveillance has always been treated differently than ordinary law enforcement surveillance. For some time, it was essentially unregulated. Even after Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978,[10] national security surveillance warrants could be issued by a secret court, called the FISA court, which only had to find that acquisition of foreign intelligence was a primary purpose of the surveillance, not that there was probable cause to believe such intelligence would be intercepted.[11] And in 2001, the Patriot Act amended the probable cause requirement so that foreign intelligence only had to be a "significant" purpose of the surveillance.[12] But at least the basic warrant structure was preserved.

However, in 2007 Congress passed the Protect America Act,[13] a law that eliminated *entirely* the warrant requirement for national security surveillance, if and when the Director of National Intelligence and the Attorney General certified that the surveillance is "directed at a person reasonably believed to be located outside of the United States" and that gathering foreign intelligence is a "significant" purpose of surveillance.[14] Under this statute, not even the secret intelligence court, much less a regular one, had a role in individual cases; rather it was relegated to determining whether the general procedures adopted by the Attorney General and the Director were "reasonably designed to ensure" that the surveillance targeted persons located outside the United States.[15] Thus, all calls or emails to someone or from someone outside the United States—note it did not have to be a member of Al Qaeda or a foreign power, just someone outside the United States—could be intercepted whenever the executive branch decided that gathering foreign intelligence was a significant purpose of the surveillance.

---

9. RICHARD VAN DUIZEND, ET AL., THE SEARCH WARRANT PROCESS: PRECONCEPTIONS, PERCEPTIONS AND PRACTICES 148-49 (1985).

10. 50 U.S.C.A. §§ 1801-1871 (West 2009).

11. Foreign Intelligence Surveillance Act, 50 U.S.C. § 1804 (1978).

12. 50 U.S.C.A §1804(a)(6)(B) (West 2009).

13. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007).

14. *Id.* § 105(B)(a)(1).

15. *Id.* § 105(c)(b).

Last year the Democrats, among them Senator Obama, amended this statute to provide a bit more protection.[16] Now the executive branch must get a FISA court warrant if the target is a United States person inside the United States and provide more information to the court and Congress about its warrantless searches.[17] But the amendments—misleadingly initially called the RESTORE Act[18]—still do not require even FISA warrants for most overseas interceptions and when they do require such warrants the law still provides that intelligence gathering only need be a "significant", not a "primary," purpose of the interception.[19]

Do these changes matter, in terms of the number or type of interceptions that will occur? Almost certainly. Even though the foreign intelligence court rarely refused a warrant outright, in 2003 and 2004 before the Protect America Act obliterated its role, the court either rejected, modified or requested more information in connection with 173 warrant applications, or about five percent of all applications.[20] What this suggests is that, without the court's supervision or the minimal supervision now required, the executive branch will *really* push the envelope on this type of surveillance.

But is the new law unconstitutional or merely controversial? The Supreme Court, back in 1972, made clear that surveillance that involves intercepting communications between purely domestic subversive persons or groups implicates the Fourth Amendment.[21] But it refused to address the reach of the Fourth Amendment when the surveillance is directed at an agent of a foreign power and also stated that Fourth Amendment strictures could be relaxed if domestic activities directly implicated national security. On the government's side, there is also the argument, likely to be accepted by many members of the Supreme Court, that we are at war with terrorists, and thus the Fourth Amendment is inapplicable, or significantly diminished in power, when the target is people overseas. So as of right now, it is unclear at best as to whether the Supreme Court would find the Protect America Act as amended unconstitutional.

At least interception of communications between citizens within the United States still requires a warrant, right? No, not quite. Not if what is

16. *See* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

17. *Id.*

18. H.R. 3773, 110th Cong., 1st Sess. (2007), *available at* http://thomas.loc.gov-/home/gpoxmlc110/h3773_eh.xml (last visited Oct. 21, 2009).

19. *See* Pub. L. No. 110-261, 122 Stat. 2436 (2008).

20. Stewart M. Powell, *Secret Court Modified Wiretap Requests: Intervention May Have Led Bush to Bypass Panel*, SEATTLE POST-INTELLIGENCER, Dec. 24, 2005, *available at* http://seattlepi.com/national/253334_nsaspying24.html?source=mypi.

21. United States v. United States District Court, 407 U.S. 297, 320 (1972).

being intercepted is what is usually called "envelope" information—the phone number or email addresses connected with the communication—rather than its content. In this situation, the government does have to go to court, but the court *must* issue an order permitting the interception if a government agent certifies the information is relevant to an ongoing investigation.[22] In other words, this is a rubberstamp order; if the papers are correctly filled out the court is not permitted to exercise any independent judgment. So this type of court order is quite different from a warrant. This action was authorized under a statute called the Electronic Communications Privacy Act, passed back in 1986.[23]

Is this statute constitutional? Those of you who have taken criminal procedure know that it is. Back in 1967 one might not have thought so. That was the year the Supreme Court decided a very important case, *Katz v. United States*.[24] Up until *Katz*, the Fourth Amendment was thought to protect only property interests, so while a microphone planted inside someone's house was a Fourth Amendment search, a wiretap set up on phone lines outside the person's house was not—no trespass was involved in the latter situation.[25] In *Katz* and subsequent cases, however, the Warren Court held that the Fourth Amendment is implicated whenever a government action infringes on an "expectation of privacy . . . that society is prepared to recognize as reasonable."[26] At the time, commentators believed this formulation would expand the scope of the Fourth Amendment, because in *Katz* itself the Court held that police efforts to bug a public phone booth, which did not involve a trespass on private property, required a warrant based on probable cause.[27]

The Warren Court era ended in the late 1960s, however. In the hands of the post-Warren Supreme Court, the expectation of privacy test has not been interpreted in a very expansive manner, as illustrated by how the Court handled interception of envelope information. In 1979 the Court held that people either know or should know that the phone company keeps a record of the phone numbers they dial and thus assume the risk that those phone numbers will end up in the hands of the government.[28] So, the Court said, we should not expect privacy in the phone numbers we dial or, to put it another way, any expectation of

22. 18 U.S.C.A. § 3123(a)(1) (West 2009).

23. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

24. 389 U.S. 347 (1967).

25. *Katz*, 389 U.S. at 352-53.

26. For a subsequent case so holding, see Bond v. United States, 529 U.S. 334, 338 (2000) (internal quotation marks omitted).

27. *Katz*, 389 U.S. at 352.

28. Smith v. Maryland, 442 U.S. 735, 742 (1979).

privacy we have with respect to our phone numbers is unreasonable.[29] The lower courts have said the same thing about email and website addresses that we use.[30] We assume the risk that Internet Service Providers like America Online and Google will retain this information and hand it over to the government. That means the government does not need a warrant to intercept the information. This assumption of risk gloss on the expectation of privacy test, adopted in the 1970s, prevails to this day, as we will see in other contexts.

III. PHYSICAL SURVEILLANCE

So what about physical surveillance? In Washington, D.C., in the wake of the terrorist attacks of September 11, hundreds of government cameras were positioned on streets, subways, school hallways, and federal facilities, in a project that "[made] Washington the first U.S. city to be able to peer across wide stretches of the city and to create a digital record of images."[31] State-of-the-art cameras allow operators to take advantage of "satellite-based optics" that enable them to see in the dark, capture words on a printed page from hundreds of feet away, and peer into buildings.[32] Numerous private cameras are also added into the mix. The head of the project has stated "I don't think there's really a limit on the feeds [the system] can take."[33] Further, he noted the system has "the capability to tap into not only video but databases and systems across the region," and can move into schools, businesses and suburban neighborhoods.[34] All of this is accomplished through a $7,000,000 control facility, which can then relay the feeds to nearly 1000 squad cars.[35]

Washington's cameras are supposedly only activated during major events and emergencies, and recordings are kept for only ten days. But pressure is building to operate the system twenty-four/seven. And other cities, bolstered by tens of millions of federal dollars, are not so reticent

---

29. *Id.* at 745.

30. *See, e.g.,* Thygeson v. United States Bancroft, 2004 WL 2066746, at *22 (distinguishing between website addresses and content of websites); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan 2000) (holding that the defendant did not have a Fourth Amendment privacy interest regarding information connected to his IP address).

31. Spencer S. Hsu, *D.C. Forms Network of Surveillance*, WASH. POST, Feb. 17, 2002, at C01.

32. *Id.*

33. *Id.*

34. *Id.*

35. *Id.*

about using their cameras. By the end of 2006, Chicago had networked over 2200 videos, at a cost of over $8 million of federal and municipal funds, that are turned on night and day, every day of the week.[36] Many of the cameras are hidden, and all are patched into the city's $43 million operations center, so that a dispatcher can send video images from the camera located most proximately to the scene of a reported incident.[37] Baltimore's system is also running continuously, and is linked to cameras in four surrounding counties.[38] San Francisco, even knee-jerk liberal San Francisco, now has a $700,000 camera system aimed at some of the city's streets.[39]

Many smaller cities and towns are following suit in one way or another. A 2001 study by the International Association of Chiefs of Police found that eighty percent of the 207 responding American law enforcement agencies have deployed some sort of closed-circuit television and that another ten percent will soon do so.[40] About half the agencies surveyed in the study use cameras in "high crime areas," twenty-five percent use them on "streets" and fifteen percent use them in "parks."[41]

These cameras can be used to focus on individuals for long periods of time, even hours, as they walk around public streets. Operators can zoom in on the faces of targets and read the titles on books they are carrying, and in some locales can do so at night as well as in the daytime. They do this without a warrant or probable cause, and, according to research, often just out of curiosity; in other words, with no cause at all.[42]

Is this type of camera surveillance constitutional? Yes, according to the Supreme Court. In 1983, the Supreme Court held that police use of a beeper to track a car for over an hour did not implicate the Fourth Amendment because we do not have a reasonable expectation of privacy on the public thoroughfares.[43] Put another way, we assume the risk that

---

36. Fran Spielman, *Hey Bad Guys, Try Finding These New Police Cameras,* CHI. SUN-TIMES, Oct. 4, 2006, at 8.

37. *Id.*

38. Doug Donovan, *24-Hour Camera Surveillance in City is Part of Bigger Plan,* BALT. SUN, June 10, 3004, at 1A.

39. Robert Selna & Demian Bulwa, *S.F. Spy Cameras No Help in Violent Crime,* SAN FRAN. CHRON., Jan. 12, 2009, at A-1.

40. Int'l Ass'n Chiefs of Police, *Cutting Edge of Technology: The Use of CTV/Video Cameras in Law Enforcement, Executive Brief,* Mar. 2001, at 4, *available at* http://www3.cutr.usf.edu/security/documents%5CIACP%5CIACP%20Guide%20for%20the%20Use%20of%20CCTV.pdf (last visited Sept. 17, 2009).

41. *Id.*

42. CLIVE NORRIS & GARY ARMSTRONG, THE MAXIMUM SURVEILLANCE SOCIETY 150 (1999).

43. United States v. Knotts, 460 U.S. 276, 281 (1983).

whatever we do in public will be observed by others, and therefore have no Fourth Amendment protection. This holding would probably also apply to the use of satellite imagery in the new Department of Defense program I mentioned earlier, a program that is meant to give the federal government the capacity to track all people or cars that are out-of-doors. The Department of Homeland Security has said the program "complies with all existing laws."[44] That's easy to do, since there are none.

But certainly, if the government conducts physical surveillance of the interior of our home, then the Fourth Amendment is implicated? Yes and no. If the government uses sophisticated technology such as a thermal imager that can detect heat differentials inside the house to see what a police officer could not see from the sidewalk with the naked eye, then a warrant is required, the Court held in 2001.[45] But the same case indicated that if the government's technology is generally available to the public, or "in general public use," then it can be used to look inside the home without worrying about the Fourth Amendment.[46] Lower courts have held that binoculars and cameras with zoom lenses fit in this general public use category, and presumably telescopes, which can be bought at Wal-Mart for under $100, would fit as well.[47] Furthermore, the Court said, even very sophisticated technology can be used to look into the home without triggering the Fourth Amendment if the government can show that what is viewed could have been seen with the naked eye from a public vantage point.[48]

IV. TRANSACTION SURVEILLANCE

Finally, let's talk about transaction surveillance, which is by far the most prevalent type of surveillance carried out by the government today. It is virtually impossible to exist in modern society without creating a record of our purchases, our use of banks and hospitals, our visits to the library and the video rental shop, and our performance in school and at

---

44. Sibhan Gorman, *Satellite-Surveillance Program to Begin Despite Privacy Concerns*, WALL ST. J., Oct. 1, 2008, at A10. As this article was going to press, the government announced the satellite program would be canceled, not out of privacy concerns but because law enforcement wants the federal government to focus on "fusion centers" (discussed further below) that will create "a national suspicious activity reporting system." Spencer S. Hsu, *Napolitano Announced End to Domestic Spy Satellite Program*, WASH. POST, June 23, 2009.

45. Kyllo v. United States, 533 U.S. 27, 40 (2001).

46. *Id.*

47. *See, e.g.*, United States v. Van Damme, 48 F.3d 461, 463 (9th Cir. 1995); Dean v. Duckworth, 99 Fed. Appx. 760 (8th Cir. 2004).

48. *Kyllo*, 533 U.S. at 34, 40.

work. All of this information is typically stored these days in computers. Yet, believe it or not, all the government needs to obtain any of this information is, at most, a subpoena. A subpoena is not a warrant. It is not based on probable cause; rather all the prosecutor or law enforcement officer has to show is that the information sought is relevant to an investigation, a standard the Supreme Court has held is extremely easy to meet.[49] Indeed, in one decision the Supreme Court explained that a subpoena is valid even if it's designed merely to satisfy "official curiosity."[50] And in many cases, the subpoena can be ex parte, meaning that the target of the surveillance—that is, you—need not even be told about it.

By now, you can probably guess why this type of surveillance is not governed by the Fourth Amendment. In 1976 the Supreme Court used the assumption of risk rationale to declare that information we "voluntarily surrender" to a bank is not protected by the Fourth Amendment, because we assume the risk that banks will give it to the government, and thus cannot claim a reasonable expectation of privacy in it.[51] This is so, the Court stated, even when the information is provided on a guarantee that the information will remain confidential.[52] In effect, this decision made banks an institutional undercover agent. Lower courts have applied the same reasoning in authorizing government efforts to obtain records from all sorts of other institutions, ranging from accounting firms to loan companies, and some have even applied it to medical facilities.[53]

So consider another provision of the Electronic Communications Privacy Act, the 1986 law I mentioned earlier.[54] Under that Act, if e-mail sits on a server for longer than 180 days without being opened *or* the recipient of e-mail opens it and stores it on an outside server for any length of time, then an ex parte subpoena is sufficient authorization to obtain the communication.[55] Even though now we're talking about the contents of messages rather than envelope information, most courts have held this latter provision does not violate the Fourth Amendment

---

49. United States v. Morton Salt Co., 338 U.S. 632, 652 (1950).

50. *Id.*

51. United States v. Miller, 425 U.S. 435, 443 (1976).

52. *Id.*

53. *See, e.g.*, Webb v. Goldstein, 117 F. Supp. 2d (E.D.N.Y. 2000) (discussing medical institutions); Wang v. United States, 947 F.2d 1400, 1403 (9th Cir. 1991) (discussing accountant records); *In re* Lufkin, 255 B.R. 204, 211 (E.D. Tenn. 2000) (discussing trustees in bankruptcy); Doe v. DiGenova, 642 F. Supp. 624 (D. D.C. 1986) (discussing V.A. records).

54. 18 U.S.C.A. § 2703 (West 2009).

55. *Id.*

because, you guessed it, we assume the risk the server operators will turn these types of emails over to the government.[56] One lone court held that a warrant is required in this situation, but its decision was nullified within a year.[57] As a result, email that government could not obtain in real time without a warrant can be obtained with a mere subpoena if it is stored. As amended by the Patriot Act, ECPA now also provides that an ex parte subpoena is sufficient to obtain basic subscriber information, defined as name, address, session times and durations, source of payment, including credit card numbers, and the identity of those who use a pseudonym.[58]

The Patriot Act also provided easier access to certain types of records in connection with national security investigations. When the FBI or another government investigative agency seeks electronic or communication billing records, financial records of any kind, or credit records in connection with a national security investigation, all it must do is issue a form of administrative subpoena known as a National Security Letter (NSL), in which a special agent in charge (in other words, a field agent) certifies that the information sought is relevant to an investigation designed to protect against international terrorism or clandestine intelligence activities and does not focus on activities protected by the First Amendment.[59] If this certification is in order, the court is *required* to affirm the letter; in other words, this is another version of the rubberstamp order I mentioned earlier.[60] Recent reports make clear that NSLs have been issued not just for targets but for "persons of interest" who are in any way connected with the target. As one FBI agent put, NSLs often seek people and phone records "once removed" from the target.[61] Thus, NSLs are used quite frequently. The FBI alone issues roughly 30,000 to 50,000 NSLs a year and maintains all the records thereby obtained (even when they are not linked to terrorism).[62]

A related development has been the advent of "data mining," involving the computerized search of databanks for information valuable

---

56. *See, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996).

57. Warshak v. United States, 490 F.3d 455 (6th Cir. 2007), vacated No. 06-4092, 2007 U.S App. LEXIS 23741, *1 (6th Cir., October 9, 2007), *held not ripe for decision*, Warshak v. United States, 532 F.3d 521 (6th Cir. 2008) (en banc).

58. 18 U.S.C.A. § 2703(c)(1)-(2) (West 2009).

59. 18 U.S.C.A. § 2709(b) (West 2009).

60. *See* 18 U.S.C. § 2709(c)(1).

61. Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES, Sept. 9, 2007, at A1.

62. Ann Broache, *House Questions "Overreaching" FBI Spy Powers*, CNET NEWS, Mar. 20, 2007, *available at* www.news.com.com/House+questions+overreaching-+FBI+spy+powers/-2100o-1-28_36168922.html (last visited Sept. 17, 2009).

to anti-terrorism and crime control efforts. According to a General Accountability Office report issued in 2004, 52 federal agencies were using or were planning to use data mining, for a total of 199 data mining efforts, 68 planned and 131 operational.[63] Of these programs, at least 122 are designed to access "personal" data.[64] These data mining efforts can be categorized as either target-driven, match-driven, or event-driven.[65]

Target-driven data mining is a search of records to obtain information about an identified target. Computerized databases have vastly increased the ability to carry out this type of investigation. For instance, in 2002, the IRS and the Social Security Administration made more than 12,000 "emergency disclosures" of personal data to federal intelligence and law enforcement agencies, and thousands more such disclosures have been made each year since then, often via a data mining program with the telling acronym REVEAL that combines sixteen government databases with databases maintained by private companies.[66] Similarly, the Department of Justice, through the FBI, has been collecting telephone logs, banking records, and other personal information regarding thousands of Americans not only in connection with counter-terrorism efforts but also in furtherance of ordinary law enforcement.[67] These two programs sift through records, tax records, bank records, and phone and ISP logs in an effort to find out more about particular individuals who are suspected of engaging in illegal activity.

Match-driven data mining is designed to determine whether a particular individual is someone who has already been identified as a suspect. In other words, the goal here is not to find out more about a person, but rather to determine whether a particular person is a known suspect. An example of match-driven data mining is the program once known as the Computer-Assisted Passenger Pre-Screening System (CAPPS II), and then as Secure Flight, a "no-fly list" that compares

63. General Accountability Office, *Data Mining: Federal Efforts Cover a Wide Range of Uses*, GAO-04-548, May 2004, at 2, *available at* http://www.gao.gov/new.items/d04548.pdf (last visited Sept. 17, 2009).

64. *Id.* at 3.

65. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 322-32 (2008).

66. Dalia Naamani-Goldman, *Anti-Terrorism Program Mines IRS' Records: Privacy Advocates Are Concerned that Tax Data and Other Information May Be Used Improperly*, L.A. TIMES, Jan. 15, 1007, at 1.

67. David Johnston & Eric Lipton, *U.S. Report to Fault Wide Use of Special Subpoenas by F.B.I.*, N.Y. TIMES, March 9, 2007, at A1.

airline passengers to lists of known or suspected terrorists and produces a particular risk level with respect to each passenger.[68]

Event-driven data mining is the most insidious form of data mining because it is conducted in the absence of a particular suspect; rather it is designed to discover the perpetrator of a past or future event using profiles or algorithms that purport to describe general characteristics of such a perpetrator. The best-known example of event-driven data mining is the federal program first known as Total Information Awareness, and then, when that name ended up being too scary for public consumption, as Terrorism Information Awareness (TIA). TIA had one major goal: to increase access to counter-terrorism information "by an order of magnitude."[69] The intent of the program was to extract information from a wide array of sources, including schools, hospital, travel agencies, and even veterinarians! Spurred by rumors that the Total Information Program would involve the accumulation and analysis of vast amounts of data about the everyday transactions of American citizens, and probably influenced as well by TIA's icon—an eye on top of a pyramid looking over the globe, accompanied by the Latin slogan for "Knowledge is power"—Congress decided to cut off funding for it in 2003, and it supposedly died at that time.[70]

However, the legislation that limited TIA's reach still permitted the Defense Department and other agencies, after "appropriate consultation with Congress," to pursue data mining of records, on American as well as foreign citizens, for the purpose of gathering information relevant to "law enforcement activities" as well as foreign intelligence.[71] The government has taken full advantage of this authority, as evidenced by the disclosure since the passing of TIA that it developed a program called ADVISE (for Analysis, Dissemination, Visualization, Insight and Semantic Enhancement), designed to "troll a vast sea of information, including audio and visual, and extract suspicious people, places and other elements based on their links and behavioral patterns" (although recent reports suggest that this program too has been discontinued for

68. Jeffery W. Seifert, *Data Mining and Homeland Security: An Overview*, CONGRESSIONAL RESEARCH SERVICE, Jan. 18, 2007, at 9, 11, *available at* http://www.fas.org/sgp/crs/homesec/-RL31798.pdf (last visited Sept. 17, 2009).

69. Defense Advanced Research Projects Agency (DARPA), *Report to Congress Regarding the Terrorism Information Awareness Program*, May 20, 2003 at 3-9, *available at* http://www.eff.org/Privacy/TIA/TIA-report.pdf (last visited Sept. 17, 2009).

70. *Senate Rebuffs Domestic Spy Plan*, REUTERS, Jan. 23, 2003, *available at* http://www.wired.com/politics/law/news/2003/01/57386 (last visited Sept. 17, 2009).

71. Consolidated Appropriations Resolution, 2003, Pub. L. No. 108-7, 117 Stat. 11.

reasons I will note in a minute).[72] The NSA program that I described earlier, in which literally millions of phone records of American citizens were acquired from telecom providers so that they could be sifted through for suspicious-looking patterns, is another example of post-TIA data mining. And recently the government has been busy creating so-called "fusion centers," described by one commentator as "an amalgamation of commercial and public sector resources for the purpose of optimizing the collection, analysis, and sharing of information on individuals," using data about banking and finance, real estate, education, retail sales, social services, transportation, postal and shipping, and hospitality and lodging transactions.[73] I do not know about you, but to me that sounds an awful lot like TIA all over again.

Again, all of this, subpoenas, National Security Letters, and data mining, can take place outside the strictures of the Fourth Amendment. All of the information is obtained from third parties to whom we have voluntarily surrendered information or whom we have allowed to collect it. So we do not have any reasonable expectation of privacy in it.

To summarize what I have said with respect to all three types of surveillance, according to the United States Supreme Court we do not have a reasonable expectation of privacy in many of our overseas communications, intercepted envelope information, our public activities, activities in our homes if they can be seen with technology in general public use or with the naked eye, or in records of our transactions with third parties. So the Fourth Amendment—the Constitution—is a dead letter in these situations.

V. WHY WE SHOULD BE CONCERNED

Is any of this reason for concern? Has the Constitution, and specifically the Fourth Amendment been misinterpreted, or is this state of the law a reasonable one? I want to answer these questions by looking at the language of the Fourth Amendment, its history, and then, for lack of a better word, policy considerations.

---

72. Ellen Nakashima & Alec Klein, *New Profiling Program Raises Privacy Concerns*, WASH. POST, Feb. 28, 2007, at DO3.

73. Lille Coney, *Statement to the Dep't of Homeland Security: Data Privacy and Integrity Advisory Committee*, Sept. 19 2007 at 1, 4 *available at* http://epic.org/privacy/fusion/fusion-dhs.pdf (last visited Sept. 17, 2009).

A. The Language and History of the Fourth Amendment

First, look again at the language of the Fourth Amendment. It states that the people shall be "secure" from unreasonable "searches."[74] So a key issue in determining the protection the Fourth Amendment affords is whether a search has occurred. A "search," back in colonial times as well as today, is an effort to look for something. As Justice Scalia has said, quoting from a dictionary published in 1828, when the Fourth Amendment was adopted, as now, to "search" meant "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to search the house for a book; to search the wood for a thief."[75] Surveillance—whether it's communications surveillance, physical surveillance, or transaction surveillance—definitely meets that definition. (Indeed, my research suggests that many believe that even under the modern Court's more restrictive expectation-of-privacy rubric, interception of our phone and email communications, technological observation of indoor (and at least some outdoor) activities, and accessing our financial and other transactional information is a search.[76]

That does not mean, of course, that the government is prohibited from engaging in surveillance. It only means that it cannot engage in unreasonable surveillance that makes people insecure. The Amendment indicates that one way of ensuring that a search is reasonable is by pursuing it via a warrant. But the language does not say a warrant is required to make a search reasonable. And unfortunately, the language of the Amendment says nothing else about when searches might be unreasonable, or what might make people insecure about their government.

So how can we figure out what is unreasonable surveillance? In answering this type of question courts, as you know, often look to history, particularly what was going on at the time the Constitution was drafted. Of course, most of the surveillance I have described—wiretapping, satellite spying, computerized data mining—did not exist in the late eighteenth century. But there are analogues to those practices.

---

74. U.S. CONST. amend. IV.

75. *Kyllo*, 532 U.S. at 33 n.1.

76. *See* Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 742-51 (1993); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L. J. 213, 275-80 (2002); Slobogin, *supra* note 65, at 333-36. These articles describe three separate surveys of diverse groups of lay people indicating that, on average, these types of police actions were viewed as more intrusive than roadblocks and, in some instances, as intrusive as search of a bedroom.

The Framers were clearly very worried about what have been called "general warrant" searches.[77] These were random searches for evidence of uncustomed goods or sedition, based on so-called "writs of assistance" that did not list any person or place in particular, but rather enabled a lowly field officer to search any house, boat or cart he thought might hide such evidence. The similarities to practices like city-wide camera surveillance, National Security Letters, and event-driven data mining in search of subversives and ordinary criminals are not far-fetched.

And the Framers were also worried about practices that come even closer to modern-day surveillance. Even before the Constitution was drafted people were bringing law suits against peeping toms and eavesdroppers.[78] And there is no doubt that the oppressive presence of British soldiers deployed throughout Boston and other towns, ordered to keep watch on the uppity colonists, was a significant reason for American discontent.[79]

So the Framers, if they had survived through to today, would probably be concerned about the types of surveillance I have been describing. But would they have wanted the government to always obtain a warrant before it takes place? Unfortunately, we do not know. We do know that the Framers did not contemplate that a warrant would be required before *every* search or seizure, since in colonial times the usual search of a house occurred when constables were in hot pursuit of a felon, when there was no time to go to a magistrate. We also have strong evidence to believe that, outside of the hot pursuit situation, they thought warrants should be required for entries in the home.[80] But what would they have thought about other situations—public surveillance, records searches, and so on? Unfortunately, answering that question ultimately requires far too much speculation.

---

77. *See generally* TELFORD TAYLOR, TWO STUDIES OF CONSTITUTIONAL INTERPRETATION: SEARCH, SEIZURE AND SURVEILLANCE AND FAIR TRIAL AND FREE PRESS 41 (1969).

78. *See* DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 89 (1972) (describing Peeping Tom lawsuits).

79. Don B. Kates, *The Second Amendment and the Ideology of Self-Protection*, 9 CONSTITUTIONAL COMMENTARY 87, 103 (1992) (stating that for the Founders, "the very idea of empowering government to place an armed force in constant watch over the populace was vehemently rejected as a paradigm of abhorrent French despotism," and noting that organized police forces were resisted in colonial times).

80. See account of common law history in *Payton v. New York*, 445 U.S. 573, 591-98 (1980).

B. Policy Considerations—National Security and Other Emergencies

Thus, as is often the case with constitutional analysis, neither language nor history definitively answers the modern-day question of whether leaving surveillance decisions up to the executive branch is reasonable. Fortunately, as the Supreme Court has said on many occasions, the Constitution is a "living document," that permits interpretations in light of political and social change.[81] This leads us to policy analysis, which requires construing the Fourth Amendment in light of the eventualities of the day.

One such eventuality is our current conflict with terrorists. Although the Obama administration is apparently going to drop the nomenclature, the Bush Administration insisted on calling this conflict a war. One reason for doing so is that, under the Constitution, that perilous condition enhances the power of the executive branch. There is considerable debate over whether the United States can be at war if Congress has not declared one, but the fact is that we have gone to war on several occasions without a congressional declaration,[82] and I am not going to enter into that debate today. More relevant for present purposes is the issue of whether, if we are at war, the Fourth Amendment no longer applies or applies differently. As I mentioned before in talking about the Protect America Act, that was the position of the Bush Administration: to wit, that we are in a special situation that justifies suspending the usual warrant and probable cause requirements.[83] The Administration bolstered that argument by pointing to Congress' resolution, passed shortly after 9/11, authorizing the president to use military force against those thought to be behind the terrorist attacks that took place on that day.[84] The Administration argued that rational implementation of that force requires the type of surveillance that I have been describing, and that the usual Fourth Amendment restrictions should not govern such surveillance.[85]

Many people who hear this debate are inevitably drawn into thinking about the TV show, *24*. For those of you who have seen it, you know that on *24* the country is always on the verge of being blown up, and if Jack Bauer or Chloe had to go to a magistrate to authorize their eavesdropping, camera surveillance or data mining we would all be dead.

---

81. Youngstown Tube & Sheet Co. v. Sawyer, 343 U.S. 579, 682 (1952).

82. Saikrishna Bangalore Prakash, *Exhuming the Seemingly Moribund Declaration of War*, 77 GEO. WASH. L. REV. 89 (2008).

83. *See generally* John Yoo, *The Terrorist Surveillance Program and the Constitution*, 14 GEO. MASON. L. REV. 565, 566 (2007).

84. Authorization for Use of Military Force (AUMF), Pub. L. No. 107-40, 115 Stat. 224 (2001).

85. Yoo, *supra* note 83, at 566.

Of course, as usual, Hollywood vastly exaggerates the need for this type of emergency surveillance. But more important, if such a need did arise there is nothing in the Fourth Amendment that prevents quick action in the face of imminent danger. The Fourth Amendment only prohibits unreasonable searches, and no one could call *24*-type of surveillance unreasonable in light of the danger. Indeed, as I mentioned before, the Framers were quite comfortable with hot pursuit searches conducted without a warrant.[86]

Most of the national security surveillance I am talking about, however, does not take place in Jack Bauer-type emergency situations. It is intelligence gathering in the real sense of the words, sifting through information, trying to figure out whether anything useful is there. Would it be unreasonable to require the executive branch to justify its non-emergency wiretapping, camera surveillance or data mining programs to some outside authority? More specifically, would it be unreasonable to require the executive branch to explain to a judge why a particular overseas person is thought to be associated with Al Qaeda and thus why phone calls made to that person should be monitored? Or to require the government to justify why cameras with zoom capacity and night vision need to be trained on particular parts of town or particular persons? Or to require the government to describe how the profiles it uses in data mining transactional information will help nab terrorists or other criminals?

There is not only a potential constitutional rationale for such requirements. There is also a practical benefit. The tendency of the government is to collect any and all information it can, with the result that it can be very hard to find the proverbial needle in the haystack. Indeed, from what we know, none of the government programs that I have been describing have produced much actionable intelligence.[87] The government is not telling us what kind of information it has obtained from its surveillance of overseas communications. But presumably most terrorists know not to talk too freely on their cell phones, or at least to use very elaborate code. And with a few notable exceptions, such as the leads provided in the July 7, 2005 bombing in London, public camera surveillance has also been surprisingly unsuccessful at reducing or solving crime, with the most recent meta-review finding that crime in the

86. *See generally Payton*, 445 U.S. at 591-98.

87. *See* John Diamond and David Jackson, *Surveillance Program Protects Country, Bush Says*, USA TODAY, Jan 23, 2006, *available at* http://www.usatoday.com-/news/washington/2006-01-23-bush_x.htm (last visited Sept. 17, 2009).

surveilled areas goes down by an average of about four percent.[88] Washington's multi-million system generated precisely one arrest in six years, Baltimore's cameras capture "mostly people drinking beer in public, or popping pills" according to one camera monitor, and San Francisco's system reduced violent crime not at all, although it did reduce property crime twenty percent.[89] Data mining has also not been particularly useful to date either. According to the *New York Times,* for instance, the NSA program that used algorithms to profile hundreds of thousands of phone records generated thousands of tips in the months following 9/11, but not one lead panned out.[90] ADVISE—the program that replaced TIA—appears to have been discontinued in part because preliminary tests indicate it is useless as a way of discovering terrorists.[91] The bottom line is that requiring the government to think through why it needs what it wants is more efficient than a blunderbuss approach.

C. Policy Considerations—Profiling and Chilling

But one often hears another argument in favor of unrestricted, or relatively less restricted, surveillance. It is simply this: if a person has nothing to hide, why should he or she be bothered about all of this eavesdropping, technological observation, and data mining? Only the bad guys will ever be really affected by it, when the government finds out what they're up to and zeroes in on them.

This is an important and plausible consideration. But it is not convincing if one takes the Fourth Amendment seriously.

Consider first these responses, collected by Daniel Solove on his website, to the "I've got nothing to hide" argument: "If you've got nothing to hide, why do you have curtains?" "Can I see your credit card bills for the last year?" "I don't have anything to hide. But I don't have anything I feel like showing you either." "If you have nothing to hide,

---

88. BRANDON C. WELSH & DAVID P. FARRINGTON, CRIME PREVENTION EFFECTS OF CLOSED CIRCUIT TELEVISION: A SYSTEMATIC REVIEW 41 (Home Office Research Study 252) (2002).

89. David Farenthold, *Federal Grants Bring Surveillance Cameras to Small Towns*, WASH. POST, Jan. 29, 2006 at A01; Stephen Janis, *Blue Light Special: Life in a City Under Surveillance*, BALT. CITY PAPER, Aug. 17, 2005, *available at* http://www.citypaper.com/news/story.asp?id=10405 (last visited Sept. 17, 2009); JENNIFER KING ET AL., CITRIS REPORT: THE SAN FRAN. COMMUNITY SAFETY CAMERA PROGRAM: AN EVALUATION OF THE EFFECTIVENESS OF SAN FRANCISCO'S COMMUNITY SAFETY CAMERAS (2008).

90. Lowell Bergman et al., *Domestic Surveillance: Spy Agency Data After Sept 22 Led F.B.I. to Dead Ends*, N.Y. TIMES, Jan. 17, 2006, at A1.

91. Ellen Nakashima & Alec Klein, *New Profiling Program Raises Privacy Concerns*, WASH. POST, Feb. 28, 2007, at B1.

then you don't have a life;" and "[b]ottom line: Joe Stalin would have loved it. Why should anyone have to say more?"[92]

But, one might counter, the Soviet state made it a crime to be anti-soviet, a condition that was defined by Joe Stalin and his minions, and included saying anything negative about the communism or doing anything out of the ordinary. That kind of 1984-style police state is not the kind of country we live in.

Not for us, perhaps. But consider the following facts: Shortly after 9/11 scores of Muslim men, most of middle-eastern descent and many of them American citizens, were picked up as "material witnesses." No charges were filed initially, and most of these individuals never appeared as witnesses in any proceeding, but all were detained for weeks, months or, in one case, over a year; most have since been released, although nine were eventually charged with some type of crime.[93] This spate of detentions was not on the scale practiced in cold war Russia. But that fact is small comfort to the people who the government has decided are material witnesses. And right after 9/11 here in the Detroit area, over 4800 Arab-Americans were interviewed by the FBI, selected, according to Attorney General John Ashcroft, according to "generic factors" that suggested they might know terrorists.[94] No terrorism-related arrests resulted from this program.[95] Another fact: Around the country, over 15,000 other men and women, most of middle-eastern descent, have been subject to FBI interviews in their homes and offices to determine if they are in league with terrorists.[96] While almost 3000 of these people have been convicted of crime, most of these convictions were for relatively minor offenses such as marriage fraud, misuse of visas, or smuggling small amounts of drugs (the average sentence has been twenty-seven months).[97] For the 12,000 others, there was not only the inconvenience

92. Daniel Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 750 (2007).

93. *Witness to Abuse: Human Rights Abuses Under the Material Witness Law Since September 11*, HUM. RTS. WATCH, June 2005, at 1. *See generally* Ricardo J. Bascuas, *The Unconstitutionality of "Hold Until Cleared:" Reexamining Material Witness Detentions in the Wake of the September 11th Dragnet*, 58 VAND. L. REV. 677, 686-92 (2005).

94. Memorandum from Attorney Gen. John Ashcroft to United States Attorneys and Members of the Anti-Terrorism Task Forces (Nov. 9, 2001).

95. *Homeland Security: Justice Department's Project to Interview Aliens after September 11, 2001*, GAO-03-459, Apr. 2003, at 16, *available at* http://www.gao.gov/htext/d03459.html (last visited Sept. 17, 2009).

96. Dep't of Justice, Office of the Inspector General, *The September 11 Detainees: A Review of the Treatment of Aliens Held on Immigration Charges in Connection with the Investigation of the September 11 Attacks* 12, 17 (April 2003), available at http://purl.access.gpo.gov/GPO/LPS31588 (last visited Sept. 17, 2009).

97. *Id.*

but the stigma and embarrassment of being confronted by government officials in front of friends, neighbors and strangers.[98]

Why were these people targeted? We don't know for sure. But probably many of them were picked because of their ethnicity and other innocuous facts: they made phone calls to Pakistan, bought plane tickets to Turkey, were observed on video attending mosques, or used credit cards to purchase guns or fundamentalist Islam texts. The vast majority had done nothing criminal or had only small transgressions to hide, yet they all experienced tangible negative consequences as a result of the government surveillance.[99]

Thousands of others, many of them not of middle-eastern descent, have had their travel plans rudely interrupted because of the government's match-driven data mining efforts. There are now close to three-quarters of a million people on the No-Fly List, which results in enhanced scrutiny at airports and often being barred from flying.[100] Senator Ted Kennedy and the former head of the Department of Justice's criminal division, Assistant U.S. Attorney General Jim Robinson, were two of the tens of thousands of innocent flyers who have been affected by this program.[101]

And many others, most of them not of middle-eastern descent, have been singled out for surveillance because they have disagreed with the government. Here are some representative headlines: "US Accused of Spying on Those Who Disagree with Bush Policies,"[102] "NSA Used City Police as Trackers;"[103] "Md. Police Put Activists' Names on Terror Lists;"[104] "Spying on Pacifists, Environmentalists and Nuns."[105] Russell Tice, who used to work at the NSA, has said that the NSA collected

98. *Id.*

99. *Id.*

100. Timothy B. Lee, *Bloated Terrorist List May Contribute to Security Problems*, Oct. 26, 2007, *available at* http://arstechnica.com/security/news/2007/10/report-terrorist-watch-list-swells.ars (last visited Sept. 17, 2009).

101. Sindh Today, *Canadian Changes Name to Dodge U.S. No-Fly List*, Sept. 13, 2008, *available at* http://www.sindhtoday.net/world/20207.htm (stating that 32,000 Americans have applied to have their names removed from the list) (last visited Sept. 17, 2009).

102. William E. Gibson, *U.S. Accused of Spying on Those Who Disagree With Bush Policies*, S. FLA. SUN-SENTINEL, Jan. 20, 2006, *available at* http://www.oldamericancentury.org/bb/index.php?showtopic=6501 (last visited Sept. 17, 2009).

103. Douglas Birch, *NSA Used City Police as Trackers*, THE BALT. SUN, Jan. 13, 2006, at 1B.

104. Lisa Rein, *Md. Police Put Activists' Names On Terror Lists*, THE WASH. POST, Oct. 8, 2008, at A01.

105. Bob Drogin, *Spying on Pacifists, Greens and Nuns*, L.A. TIMES, Dec. 7, 2008, at A18.

information about journalists round-the-clock, year-round, supposedly with the intent of figuring out who merited further attention. But in the meantime, he says, "They sucked in everybody."[106] The negative consequences in these cases are less tangible than the round-ups of Arab-Americans, but are still noteworthy because they involve intimidation of activists and the press engaging in political speech. Indeed, New York Times reporter James Risen, who co-authored articles about the NSA's wiretapping program, has alleged that the purpose of the NSA's journalist-monitoring was "to have a chilling effect on potential whistleblowers in the government to make them realize that there's a Big Brother out there that will get them if they step out of line."[107] Remember Monrad Paulsen's comments that I quoted at the beginning of this talk: the Fourth Amendment is needed to protect the First Amendment.

D. Policy Considerations—The Effect on the Rest of Us

But perhaps all of this—detaining or interviewing a few thousand innocent people of Arabic descent, disrupting the travel plans of a few thousand others who use airplanes, intimidating a few hundred protesters and journalists—is still a small price to pay for being extra cautious? Even if you think so, consider whether that is the only price we pay. Former National Security Director Mitch McConnell insisted that there is no spying on Americans. But Russell Tice, the NSA worker I've already mentioned, has alleged the NSA vacuumed in the fax, phone, ISP credit card and financial records of tens of thousands of U.S. citizens who had no discernible links to terrorist organizations; as Tice eloquently put it, "They sucked in everybody."[108]

It is true that those whose records are accessed through this process usually don't know it is happening and that, if nothing incriminating is found, they may never find out, at least about the data mining itself. But there are, nonetheless, at least two ways data mining can hurt all of us.

First, the desire for efficient data mining creates tremendous pressure to accumulate all information in one central repository, and that makes personal data all that more vulnerable to misuse. As Larry Ellison, the head of Oracle stated, "The biggest problem today is that we have too many [databases]. The single thing we could do to make life tougher for terrorists would be to ensure that all the information in myriad

106. Kim Zetter, *NSA Whistleblower: Wiretaps Were Combined with Credit Card Records of US Citizens*, WIRED, Jan. 23, 2009, *available at* http://www.wired.com/threatlevel/2009/01/nsa-whistlebl-1/ (last visited Oct. 21, 2009).

107. *Id.*

108. Zetter, *supra* note 106.

government databases was integrated into a single national file."[109] That may be true. But a single data base makes it all that much easier for identity thieves and hackers to do their dirty work. USA Today recently reported that cyber attacks on U.S. government computer networks, most of which were designed to "control or steal sensitive data," climbed 40% last year.[110]

Second, data mining allows the government to accumulate and analyze vast amounts of information about us, sufficient to create what some have called personality or psychological "mosaics" of its subjects.[111] How many of you are on Facebook? In February 2009, thousands of Facebook users were up in arms over reports that Facebook was planning on maintaining control of their page content even if users canceled their accounts.[112] But what Facebook can do is nothing compared to what the government is capable of. One result of government's entry into the information age is that faceless bureaucrats will be able to compile dossiers on each of us, for any reason or for no reason at all. There are many reports of government officials misusing data in bad faith or for ends they believed were justified, albeit not explicitly authorized (the latter a phenomenon known as "mission creep").[113] Moreover, this dossier-building power extends well beyond what government officials can do, as evidenced by reports that the federal government is going to pay private contractors up to $1 billion to conduct core intelligence tasks of analysis and collection over the next five years.[114] It may have been some vague sense of this possibility that led Congress, however ineffectually, to declare its opposition to the

109. Larry Ellison, *Digital IDs Can Help Prevent Terrorism*, WALL ST. J., Oct. 18, 2001, at A26.

110. Peter Eisler, *Raids on Federal Computer Data Soar*, USA TODAY, Feb. 17, 2009, at 1A.

111. Anthony Paul Miller, *Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age*, 20 COL. J. L. & SOC. PROBS. 89, 111 (1986).

112. Barbara Ortutay, *Facebook Backs Off User Policy Changes*, ASSOCIATED PRESS, Feb. 19, 2009, *available at* http://fullcircle-adminservices.blogspot.com/2009/02/fyi-facebook-backs-off-user-policy.html (last visited Sept. 17, 2009).

113. *See generally* Peter P. Swire, *Financial Privacy and the Theory of High Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 493-500 (1999) (recounting misuse of data for financial gain, political gain, satisfaction of prurient interest, and as a result of mission creep such as using tax records to detect welfare fraud). For a more recent example, see Brad Schrade, *Trooper Begs to Keep Job*, THE TENNESSEAN, Oct. 10, 2008, at B1 (describing highway patrol officer who ran unauthorized background checks on as many as 182 people).

114. Richard Willing, *Defense Department Pays 1 Billion to Outside Contractors*, USA TODAY, Aug. 30, 2007, *available at* http://www.c4isrjournal.-com/story.php?F=3003724 (last visited Sept. 17, 2009).

concept of Total Information Awareness, with its epithet "Knowledge is Power."

But, one might say again, that knowledge will never be used against me. Consider these two statements, one from Justice Jackson, and the second from Monroe Freedman: "With the law books filled with a great assortment of crimes, a prosecutor stands a fair chance of finding at least a technical violation of some act on the part of almost anyone."[115] And "[t]here are few of us who have led such unblemished lives as to prevent a determined prosecutor from some basis for an indictment or information."[116] Bank records can reveal financial irregularities, intentional or not, that might lead to tax prosecutions. Internet Service Provider logs can indicate the websites we have visited, innocently or not, that might lead to pornography charges. Cameras can track one's visits to drug alleys, psychiatrist offices, or lovers' apartments, which can lead to trouble with the law or, perhaps worse, with one's spouse or friends. As Jack Balkin has written, the surveillance state emphasizes *ex ante* prevention rather than *ex post* apprehension and prosecution, so that law enforcement becomes increasingly preventive in orientation, which widens the net considerably, wide enough to include many of us.[117]

And even if you never find out about this surveillance because the government chooses not to act: Are you comfortable knowing that your conversations are likely to be overheard because you have a friend overseas, that your public meanderings are likely to be constantly monitored on cameras because you are sexy or strange-looking, or that you are routinely tracked because your name is Mohammed or because of your unusual travel habits?

VI. THE NEED FOR, AND SCOPE OF, MORE REGULATION

These potential costs of surveillance do not necessarily outweigh its benefits. But they at least suggest that surveillance by the government should be subject to some regulation. And it should be regulation by entities outside the executive branch. Last year, the FBI reported that, for the fourth year in a row, it violated the minimal restrictions on the issuance of NSL letters in obtaining American's phone records, credit

115. Robert Jackson, *The Federal Prosecutor, Address Delivered at the Second Annual Conference of United States Attorneys*, April 1, 1940 (quoted in Morrison v. Olson, 487 U.S. 654, 728 (1988)).

116. Monroe H. Freedman, *The Professional Responsibility of the Prosecuting Attorney*, 55 GEO. L.J. 1030, 1034-35 (1967).

117. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 15 (2008).

reports and Internet traffic, which led even one former FBI official to state "The credibility factor shows there needs to be outside oversight . . . The idea that new guidelines [administered by the FBI] would make a difference . . . cuts against rationality."[118] However, I do not think this outside regulation should always require a warrant based on probable cause. In addition to the emergency exception I mentioned earlier, I think that surveillance that is relatively less intrusive—for instance camera surveillance and some forms of data mining—should be permissible on far less than probable cause, and perhaps could even be authorized by an entity within the executive branch. Unfortunately, I do not have sufficient time to describe in detail how I think the Fourth Amendment should be construed so as provide this regulation. My book, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment*,[119] does so at great length and, if you are interested in this topic, I hope you will read it. In the meantime, I hope you agree with me that surveillance poses a grave challenge to our individual and collective security, and that a rejuvenated Fourth Amendment is necessary to ensure that the challenge is met.

118. Daniel Solove, *The FBI Does it Again*, Mar. 2, 2008, *available at* http://www.concurringopinions.com/archives/2008/03/the_FBI_does_it.html (last visited Sept. 17, 2009).

119. University of Chicago Press (2007).