2002

Foreword--Privacy and Secrecy after September 11

Marc Rotenberg

Foreword

Privacy and Secrecy After September 11

Marc Rotenberg†

It is difficult to speak about privacy in the United States today without considering the significance of September 11. That day has had a profound impact on the public perception of privacy, the actions of Congress, the development of new technologies, and most likely even the decisions of courts. Polls indicate increased public support for new forms of surveillance.[1] Congress has moved swiftly to expand the surveillance authority of the state.[2] New technologically advanced means of surveillance, such as biometric identifiers and a National ID card,

---

† Executive Director, Electronic Privacy Information Center (EPIC), and Adjunct Professor, Georgetown University Law Center. Former Counsel, Senate Judiciary Committee (Senator Patrick Leahy). Thanks to Mikal J. Condon for research assistance, and to Matthew Wegner and the *Minnesota Law Review* for organizing this symposium. Thanks also to Professor Paul Schwartz for his encouragement and Professor Daniel Solove for his dedication.

1. *See, e.g.*, *ABC News/Washington Post Terrorist Attack Poll #3*, ABC NEWS/WASH. POST, Sept. 29, 2001 (indicating high levels of public support for expanded government surveillance, use of wiretap authority, and ID cards in the wake of the September 11 attacks); Robert O'Harrow Jr. & Jonathon Krim, *A Changing America: National ID Cards Gaining Support*, WASH. POST, Dec. 17, 2001, at A1 (indicating nearly 70% support for some form of National ID). *But see E-Government Poll*, WASH. POST, Feb. 27, 2002, at A21 (finding that Americans are sharply divided on the issue of national ID cards, with only 47% in support of a national ID, and 44% viewing it as "an invasion of people's civil liberties and privacy"); ROPER CTR. FOR PUB. OPINION RESEARCH, Bureau of Justice Sourcebook of Criminal Justice Statistics (1994) (illustrating longstanding public opposition (by three to one) to use of electronic surveillance as an acceptable investigative technique).

2. *See, e.g.*, National Defense Authorization Act for Fiscal Year 2002, Pub. L. No. 107-107, 115 Stat. 1654 (2001); Defense Appropriations Act, 2002, Pub. L. No. 107-117, 115 Stat. 2230 (2002); Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 2002, Pub. L. No. 107-77, 115 Stat. 748 (2001); Uniting And Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 15 Stat. 272 (2001).

are now under serious consideration.[3] Even the courts have shown a new deference to claims of national security.[4]

During such periods in history it is appropriate to reexamine core values and consider the structure and purpose of principles in law that today are constantly under attack. This is only partly to reaffirm critical political goals; it is also to explore and clarify the relationship and significance of critical concepts that are too easily misunderstood.

In this Article I will examine two critical concepts in the world of privacy—privacy and secrecy—and discuss what the developments since September 11 tell us about the relationship between these two key legal categories . I will argue that they are very different ideas, reflecting very different political values, and that they are fundamentally at odds in the structure of privacy law in the United States. But it is fair to note at the outset that the terms are often used interchangeably. We speak of meeting "in secret" and meeting "in private." We communicate secretly and we communicate privately. There are aspects of our lives that we wish to keep secret, or private. These terms require more careful examination, particularly after the events of September 11.

I. DIMINISHMENT OF PRIVACY BY LEGAL MEANS

One clear impact of September 11 has been the reduction in privacy protection under U.S. law. The USA PATRIOT Act is the most sweeping expansion of government surveillance authority since the passage of the Communications Assistance for Law Enforcement Act (CALEA) of 1994.[5] Where CALEA established for the first time the premise that the government had the authority to require by law that new communication services be designed to enable surveillance by the state, the USA Patriot Act limited in multiple ways the scope, impact, and effect of many privacy laws previously in force in the United States.

---

3. *See* Barnaby J. Feder, *A Surge in Demand to Use Biometrics*, N.Y. TIMES, Dec. 17, 2001, at C21, *available at* http://www.nytimes.com/2001/12/17/technology/17IRIS.html; O'Harrow & Krim, *supra* note 1, at A1.

4. *See* United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001) (upholding the use of the Classified Information Procedures Act in a case involving a low-level mobster).

5. Communications Assistance for Law Enforcement Act (CALEA) of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001-1010 (1995)).

To understand the impact of the USA PATRIOT Act on privacy law in the United States you must understand that the protection of privacy by statutory means typically incorporates a wide range of Fourth Amendment values, such as an articulated probable cause standard, a notification requirement, a nexus between the authority granted and the area searched, and means of judicial oversight.[6] Taken separately and as a whole, these provisions limit the state's ability to conduct searches, thereby seeking to safeguard certain aspects of private life that may be recorded in paper or electronic records.

Broadly stated, these provisions develop from two lines of cases that provide the twin cornerstones for information privacy law in the United States. The first is the *Olmstead v. United States* and *Katz v. United States* line, which gave way to enactment of the federal wiretap act in 1968.[7] The second is the *United States v. Miller*[8] and *California Bankers Ass'n v. Schultz*[9] line, which led Congress to recognize that if there were to be constitutional safeguards for the disclosure of personal information to police held by third parties, Congressional action would be required.[10]

---

6. The law enforcement provision in the Subscriber Privacy provision in the Cable Communications Policy Act of 1984 (the Cable Act) provides a good example:

> Except as provided in subsection (c)(2)(D) of this section, a governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order—
> (1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and
> (2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

Pub. L. No. 98-549, 98 Stat. 2779 (1984) (codified as amended at 47 U.S.C. § 551(h) (2002)).

7. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (1994)); Olmstead v. United States, 277 U.S. 438 (1928); Katz v. United States, 389 U.S. 347 (1967).

8. 425 U.S. 435 (1976).

9. 416 U.S. 21 (1974).

10. The Cable Act, 47 U.S.C. § 551(h) (2002). *See also* Right to Financial Privacy Act, Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified at 12 U.S.C. § 3401 (1994)); Electronic Communications Privacy Act (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510-2522 (1994)); Privacy Protection Act, Pub. L. No. 96-440, 94 Stat. 1879 (1980) (codified as amended at 42 U.S.C. § 2000aa-2000aa-12 (1994)).

Since the mid-1970s a range of privacy laws in the United States has been enacted to limit government access to a wide range of record systems, including government records, financial records, medical records, cable subscriber records, electronic mail records, video rental records, and more.[11] In just the last few years, Congress extended new safeguards to medical information,[12] financial information,[13] and records on students.[14]

The USA PATRIOT Act did not destroy the edifice of U.S. privacy law, but it did significantly weaken the structure and limit the coverage of many key statutes. The Act limits safeguards created by fifteen statutes.[15] It reduces probable cause standards in key laws.[16] It significantly expands the authority of the Foreign Intelligence Surveillance Act. It limits judicial review.[17] It creates a new "sneak and peak provision" for police to undertake searches without the customary notification requirement.[18]

Still, the USA PATRIOT Act is not the only means by which privacy provisions in the United States have been diminished since September 11. The Attorney General has also indicated that attorney-client privilege, one of the oldest privileges

---

11. *See supra* note 10; *see also* Video Privacy Protection Act, Pub. L. 100-618, 102 Stat. 3195 (1988) (codified as amended at 18 U.S.C. §§ 2710-2711 (2000)); Family Educational Rights & Privacy Act (FERPA), Pub. L. No. 93-380, 88 Stat. 571 (1974) (codified as amended in scattered sections of 47 U.S.C.).

12. *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in various provisions in 42 U.S.C. and 29 U.S.C.).

13. *See* Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

14. Elementary and Secondary Education Act Authorization Bill, Pub. L. No. 107-110 § 1061, 115 Stat. 1425 (2002).

15. Among the statutes amended by the USA PATRIOT Act are The Right to Financial Privacy, 12 U.S.C. § 3414; Consumer Credit Protection Act, 15 U.S.C. § 1681u; The Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Additional Grounds for Issuing Warrant under Title II, 18 U.S.C. §3103; ECPA, 18 U.S.C. §§ 2510, 2511, 2516, 2517, 2520, 2702, 2703, 2707, 2709, 2711, 3056, 3121, 3124, 3127; FERPA, 20 U.S.C. §§ 1232g, 9007; The Cable Act, 47 U.S.C. § 551; The Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1803, 1804, 1805, 1806, 1823, 1824, 1842, 1843, 1861-1863 (1994 & Supp. 1998). *See generally* USA PATRIOT Act, Pub. L. No. 107-56, 15 Stat. 272 (various provisions amending language in each of the aforementioned statutes).

16. USA PATRIOT Act, Pub. L. No.107-56, §§ 206, 216, 218, 115 Stat. 272 (2001).

17. *Id.* §§ 206-208, 214-215, 218, 225.

18. *Id.* § 213.

in common law, may be violated by police.[19] And proposals currently pending in Congress would enable access by state police to records previously restricted under the Foreign Intelligence Surveillance Act.[20]

Apparently the only area that the Attorney General believes should not be subject to reduced protection following September 11 are the records provided by individuals seeking the right to carry personal firearms. There the Attorney General has said that, because there is no current legal authority, investigators seeking access to this information should be restricted.[21] The Attorney General had not made a similar argument during the debate over the USA PATRIOT Act with regard to the information that might be sought in telephone records, banking records, voicemail records, educational records, library records, or business records.

II. LOSS OF PRIVACY BY TECHNOLOGICAL MEANS

The expansion of state surveillance authority under the USA PATRIOT Act is only one way that personal privacy has been diminished after September 11. The government has also sought by technical means to expand monitoring and profiling of individuals. At the moment, the three proposals that have received the most attention are a National ID Card, new face recognition technology, and systems for border control.[22]

A. NATIONAL ID CARD

The proposal for the National ID Card reflects, perhaps more than any other example, the great ambivalence of the American people about the appropriate response to the events of September 11. In the days following that event, public opin-

19. *See* U.S. Bureau of Prisons Special Administrative Measure for the Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. 55,062 (2001) (to be codified at 28 C.F.R. pts. 500-501).

20. *See* Federal-Local Information Sharing Partnership Act of 2001, S. 1615, 107th Cong. (2001).

21. Peter Slevin, *Ashcroft Blocks FBI Access to Gun Records; Critics Call Attorney General's Decision Contradictory in Light of Terror Probe Tactics*, WASH. POST, Dec. 7, 2001, at A26.

22. *See, e.g.*, *E-Government Poll*, *supra* note 1, at A21; Bill Miller, *Ridge to Brief Senators About Border Security; Session Conflicts With Byrd Hearing*, WASH. POST, May 2, 2002, at A2; O'Harrow & Krim, *supra* note 1, at A1; Robert O'Harrow, Jr., *Facial Recognition System Considered for U.S. Airports, Reagan National May Get Scanning Device*, WASH. POST, Sept. 24, 2001, at A14.

ion polls showed sharp increases for support of a National ID.[23] Prominent American businessmen, law professors, and political leaders also expressed support for the idea.[24] A congressional hearing in the late fall suggested that a National ID Card, defined as one issued by the federal government that individuals in the United States would be required to carry, would still face strong political opposition.[25] Technical experts also noted the significant privacy and security risks in the development of a true National ID.[26] And subsequent polls indicated that the initial wave of support for a National ID Card had diminished.[27] Thereafter, the focus shifted to a proposal put forward by the American Association of Motor Vehicle Administrators (AAMVA) to build upon the current state-issued drivers license and to create a document that was both more secure, by means

23. *See* Harris Poll, *Overwhelming Public Support for Increasing Surveillance Powers and, Despite Concerns about Potential Abuse, Confidence that the Powers Will be Used Properly*, *at* http://www.harrisinteractive.com/news/allnewsbydate.asp?NewsID=370 (Oct. 3, 2001) (indicating that 68 % of the public polled supports national identification cards).

24. Elise Ackerman & Paul Rogers, *ID Card Idea Attracts High-level Support: Top executives, lawmakers back national identification card proposal*, SAN JOSE MERCURY NEWS, Oct. 16, 2001, at 1A; Alan M. Dershowitz, *Why Fear National ID Cards?*, N.Y. TIMES, Oct. 13, 2001, at A23; Press Release, Senator Feinstein Identifies Weaknesses of U.S. Visa System, Oct. 12, 2001, http:// feinstein.senate.gov/releases01/s-visas.htm.

25. *See Oversight Hearing on "National Identification Card" Before the Subcomm. on Government Efficiency, Financial Management, and Intergovernmental Relations of the House Comm. on Gov't Reform*, 107th Cong. (2001) [hereinafter *Oversight Hearing*] (statement of Rep. Horn, Chairman, House Comm. on Gov't Reform); *see also* O'Harrow & Krim, *supra* note 1, at A1 ("[T]he political hurdles to a national ID card remain huge. President Bush has publicly downplayed their benefits, saying they're unnecessary to improve security. Bush's new cyberspace security chief, Richard Clarke, recently said he does 'not think it's a very smart idea.'").

26. *See Oversight Hearing*, *supra* note 25, (statement of Ben Schneiderman, Professor of Computer Science, University of Maryland) ("We must ask whether there is now a secure data base that consists of 300 million individual records that can be accessed in real time? The government agencies which come close are the Internal Revenue Service and the Social Security Administration, neither or which are capable of maintaining a network that is widely accessible and responsive to voluminous queries on a 24 hour by 7 days a week basis."); Peter G. Neumann and Lauren Weinstein, *Risks of National Identity Cards*, 44 COMM. OF THE ACM 176 (2001); Bruce Schneier, *National ID Cards*, CRYPTO-GRAM NEWSLETTER, *at* http://www.counterpane.com/crypto-gram-0112.html#1 (Dec. 15, 2001);.

27. *See* Donna Leinwand, *National ID in Development, But Enthusiasm for the System Appears to be Fading, Poll Says*, USA TODAY, Jan. 22, 2002, at 2A; Julia Scheeres, *Support for ID Cards Waning*, WIRED NEWS, Mar. 13, 2002, *at* http://www.wired.com/news/business/0,136,51000, 00.html.

of a biometric identifier, and more easily integrated with a variety of record systems.[28] At present, it remains unclear whether the AAMVA proposal to create a de facto National ID Card will go forward. There are both legislative and budgetary obstacles, and Americans still appear deeply divided.[29]

B. FACE RECOGNITION

A second proposal to significantly expand surveillance is the idea of putting in place new "smart cameras" that have the ability to match in realtime the images of individuals viewed in public and private places against a stored database of facial images, which could be either those of suspected terrorists, licensed drivers, gamblers in Las Vegas casinos, or children in the Washington, DC public school system.[30] Joseph Attick, CEO of the company Visionics, has argued that his system for face recognition would reduce the risk of terrorist threat, and several pilot projects are underway.[31] However, independent studies have also raised questions about the reliability of face recognition systems, and at least one airport has decided not to go forward with the system after the chief of security determined that it might actually diminish the effectiveness of cur-

28. *See* AM. ASS'N OF MOTOR VEHICLE ADMINS., SPECIAL TASK FORCE ON IDENTIFICATION SECURITY REPORT TO THE AAMVA BOARD, *at* http://www.aamva.org/documents/private/idsecuritytaskforce/drvidsecuritytaskforcerecommendations.pdf (Jan. 2002); *see also* Robert O'Harrow Jr., *States Devising Plan for High-Tech National Identification Cards*, WASH. POST, Nov. 3, 2001, at A10.

29. *See E-Government Poll*, *supra* note 1, at A21; EPIC, *Your Papers, Please: From the State Drivers License to a National Identification System*, *at* http://www.epic.org/privacy/id_cards/yourpapersplease.pdf (opposing the AAMVA plan); Shane Ham & Robert D. Atkinson, *Progressive Policy Institute Report: Modernizing the State Identification System*, *at* http://www.ppionline.org/documents/Smart_Ids_Feb_02.pdf (Feb. 7, 2002).

30. *See* Robert O'Harrow Jr., *Facial Recognition System Considered for U.S. Airports*, WASH. POST, Sept. 23, 2001, at A14; Robert O'Harrow Jr., *D.C. Plans ID Card for Students; Aim of DMV Database is Missing Children*, WASH. POST, Aug. 15, 2001, at A1; Bob Hirschfeld, *Security is Watching*, TECH TV, *at* http://www.techtv.com/news/culture/story/0,24195,3367924,00.html (Jan. 11, 2002).

31. *See* Karen Alexander, *Airport to Get Facial Recognition Technology Oakland*, L.A. TIMES, Oct. 29, 2001, at B1; O'Harrow, *Facial Recognition System Considered for U.S. Airports*, *supra* note 30, at A14; *see also Interest in face scanning grows: Makers of technology struggle to meet demand since attacks*, REUTERS, *at* http://www.msnbc.com/news/630735.asp (Sept. 18, 2001) ("'Right now what we need to do is build our defenses, as we need to protect innocent lives and prevent this from happening again,' said Visionics CEO Joseph Attick.").

rent security procedures.[32]

C. BORDER CONTROL

A third area of significant focus is the effort to improve the tracking of non-U.S. citizens in the United States. It is clear that many people in the United States who receive visas often do not comply with the reporting requirements.[33] It is also clear that current means to track those individuals are not particularly effective.[34] But it is less clear what role technology would play in solving this problem. While it may be possible to integrate databases to enable more detailed monitoring of individuals in the United States on visas, the idea of real-time tracking, as has been proposed by some political leaders, would require extraordinarily intrusive surveillance techniques and also be extraordinarily expensive. It might also be fair to ask whether U.S. citizens traveling abroad would accept a system that would track their activities and their meetings with others.

Some systems for real-time tracking of individuals are currently being pursued for parolees and those serving in-home detention.[35] These systems enable remote tracking of a person's location and are designed to ensure that an individual stays within a circumscribed geographic region.[36] Similar technologies widely available for pets administer a small shock to the animal if the animal strays beyond the prescribed region.

We can briefly summarize this Part by noting that since September 11 there has been a dramatic reduction in privacy in the United States and that further proposals are under consideration. Some of this may be ascribed to specific changes in federal statutes; some to new technologies that enable greater surveillance and tracking. The interesting question now is whether we can say that there has been a similar decrease in secrecy.

---

32. *See* Liz Anderson, *At the Assembly–About Face*, PROVIDENCE J., Jan. 17, 2002, at B1 (reporting that T.F. Green International Airport in Providence, Rhode Island, one of the first airports to consider facial recognition technology, decided in January 2002 that they would not install it after all, citing the possibility of false matches and other technological shortcomings of facial recognition systems).

33. AMITAI ETZIONI, THE LIMITS OF PRIVACY 107 (1999).

34. *Id.*

35. Jennifer Lee, *Putting Parolees on a Tighter Leash*, N.Y. TIMES, Jan. 31, 2002, at G1.

36. *Id.*

III. EXPANSION IN GOVERNMENT SECRECY

There are two ways to understand the expansion of government authority resulting from passage of the USA PATRIOT Act on October 26, 2001. One way is to assess the variety of ways in which personal information may be made more readily available to police in the course of a criminal or national security investigation. This is apparent in the diminished probable cause standard in several key statutes.[37] We can reasonably say that these changes result in a diminished privacy protection for the person whose information is now more readily available to government agents.

The second way to assess the means of expansion of government authority is the various ways in which the conduct of government is more difficult to detect, is more readily concealed, or fails to follow the requirements that might otherwise apply. It is to this change—the increase in secrecy—that we now turn.

Central to this analysis is the expanded role of the Foreign Intelligence Surveillance Act (FISA) in the post USA PATRIOT Act world. The FISA was originally enacted in 1978 to address a problem raised in the *Katz* decision and left open by the enactment of the federal wiretap statute in 1968.[38] That is what would be the statutory standard for a search undertaken in matters of national security. The *Katz* Court suggested that all forms of electronic surveillance that violated a reasonable expectation of privacy would be subject to a Fourth Amendment standard.[39] But clearly there was concern that the standard appropriate for the investigation of a person engaged in an illegal gambling operation may not be the same as an agent of a foreign power, not a U.S. citizen, who intended harm against the United States.[40]

In 1978 Congress adopted the FISA with the narrow goal of

37. USA PATRIOT Act, Pub. L. No.107-56, §§ 206, 216, 218, 115 Stat. 272 (2001).

38. Katz v. United States, 389 U.S. 347, 363-64 (1967) (White, J., concurring) (noting that the *Katz* holding does not preclude a national security exception to the warrant requirement for wiretapping). *But see id.* at 359 (Douglas and Brennan, JJ., concurring) (objecting to Justice White giving a "green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security' matters").

39. *Id.* at 359.

40. *Id.*

enabling electronic surveillance of foreign agents in the United States pursuant to federal statutory authority.[41] The Act also established the Foreign Intelligence Court, which, unlike a traditional Title III court, issued orders authorizing wiretaps without indicating the jurisdiction, purpose, or duration of the order.[42] The FISA court met within the Department of Justice office building in Washington, DC and was in physical orientation as well as statutory structure more closely aligned with the interests of the executive branch of government than other courts.[43]

A. DIMINISHED ACCESS TO PUBLIC RECORDS

Not only has the prosecution of crime been made more secretive since September 11, but so too have the routine activities of government. The Attorney General indicated in a memo published on October 11 that federal agencies would be encouraged to withhold public records that are subject to the Freedom of Information Act if there was a "reasonable basis" for the application of a statutory exemption.[44] This standard is in contrast to the one under which the federal agencies operated when Janet Reno served as Attorney General. As President Clinton's Attorney General, Reno had required that agencies adopt a "foreseeable harm" test, similar to the standard that Attorney General Levy had adopted in the 1970s.[45]

The new standard for litigating FOIA cases is a clear indication that the Department of Justice is less committed to open government since September 11.[46] On several occasions the At-

---

41. FISA, 50 U.S.C. §§ 1801-1829, 1841-1846 (2002).

42. *Compare* 18 U.S.C. § 2518 *with* 50 U.S.C. § 1803.

43. *See generally* Patrick S. Poole, *Inside America's Secret Court: The Foreign Intelligence Surveillance Court*, *at* http://fly.hiwaay.net/~pspoole/fiscshort.html (last visited May 13, 2002).

44. Memorandum from John Ashcroft, Attorney General, to Heads of all Federal Departments and Agencies re: The Freedom of Information Act (Oct. 12, 2001) [hereinafter Ashcroft FOIA Memorandum], *available at* http://www.usdoj.gov/04foia/011012.htm.

45. *See* Memorandum from Janet Reno, Attorney General, to Heads of all Federal Departments and Agencies re: The Freedom of Information Act 3 (Oct. 4, 1993), *available at* http://www.usdoj.gov/oip/foia_updates/Vol_XIV_3/page3.htm (urging agencies toward greater openness under FOIA, with an overall "presumption of disclosure," establishing a new "foreseeable harm" standard governing the application of FOIA exemptions, and promoting "discretionary" FOIA disclosures as a means of achieving the goal of "maximum responsible disclosure" under the Act).

46. *See* Tom Beierle & Ruth Greenspan Bell, *Don't let 'right to know' be a*

torney General has expressed his opinion that the U.S. federal government cannot make information publicly available that may be a threat to the country.[47] This policy has extended to decisions to severely limit the availably of public information that was previously available over the Internet prior to September 11.

B. CLOSED HEARINGS

Government secrecy has also become apparent in the reluctance of the President and the Congress to pursue public hearings in what many have described as a "massive intelligence failure."[48] While CIA Director George Tenant appeared in an open hearing to discuss the annual CIA budget request, subsequent hearings on the adequacy of intelligence gathering prior to September 11, the current status of the Anthrax investigation, the justification for significantly expanding certain CIA programs, as well as a range of questions related to the effectiveness of the CIA have been kept from public review.

C. CONSEQUENCES OF GOVERNMENT SECRECY

One of the consequences of the expanded secrecy is clearly that public accountability is diminished. This has consequences both large and small. In the context of electronic surveillance undertaken pursuant to the new powers created by the USA PATRIOT Act, it means that targets of government searches who might previously have been notified that they were subject to government surveillance will not be so told.[49] It

---

war casualty, THE CHRISTIAN SCI. MONITOR, Dec. 20, 2001, at 9; Editorial, *On the Public's Right to Know; The Day Ashcroft Censored Freedom of Information*, S. F. CHRON., Jan. 6, 2002, at D4; Editorial, *Ashcroft sends a chilling message FOIA: Memo urging caution over freedom of information requests needs to be reviewed*, VENTURA CTY. STAR, Jan. 11, 2002, at B6; Helen Thomas, *President Bush and John Ashcroft Trample the Bill of Rights*, SEATTLE POST-INTELLIGENCER, Nov. 16, 2001, at B6.

47. *See* Ashcroft FOIA Memorandum, *supra* note 44; *see also* Testimony of Attorney General John Ashcroft before the Senate Committee on the Judiciary (Dec. 6, 2001), *available at* http://www.usdoj.gov/ag/speeches/2001/1206 transcriptsenatejudiciarycommittee.htm.

48. *E.g., CBS News: Face the Nation* (CBS television broadcast, Sept. 16, 2001), *available at* http://www.cbsnews.com/stories/2001/09/17/ftn/main311563.shtml (Senator Shelby, ranking minority member of Senate Intelligence Committee, referred to the terrorist attacks as "a massive intelligence failure.").

49. USA PATRIOT Act, Pub. L. No. 107-56, § 213, 115 Stat. at 285-86 (amending the U.S. Code to allow for delayed notification of the execution of a

means that public reporting of the use of surveillance authority by federal investigators will be less detailed and less useful than reports on similar activities in the past. And on large open questions, like who was responsible for the dissemination of deadly anthrax spores in the nation's capital in mid-October, the government can continue to make representations about the status of the case with little opportunity for the public to probe the government's claims because information associated with the investigation remains secret.[50]

IV. UNDERSTANDING PRIVACY AND SECRECY

What we have witnessed since September 11 is both the diminishment of personal privacy and the expansion of government secrecy. Now this is a significant development that bears some exploration however we may feel about the specific steps taken in the wake of September 11. It is my aim at this point to look more closely at the interplay of these two trends and to see if the traditions in privacy law help us understand the transformation taking place since September 11. Should it surprise us that as personal privacy is diminished, government secrecy expands?

We can begin with the observation of some commentators that there is a tradeoff between privacy and transparency or privacy and openness. According to this view privacy stands in opposition to these values, and we may give up some privacy to gain greater public accountability.

The communitarian scholar Amitai Etzioni, for example, has argued that privacy must be balanced against competing interests.[51] Since September 11 Etzioni has endorsed a number

---

warrant).

50. Former CIA Director R. James Woolsey alleged in a *Wall Street Journal* editorial in mid-October that the use of "weapon-grade" made clear that Saddam Hussein was responsible for the dissemination of anthrax in the nation's capitol. R. James Woolsey, *The Iraq Connection*, WALL ST. J., Oct. 18, 2001, *at* http://opinionjournal.com/editorial/feature.html?id=95001338. Subsequent reporting by the *Washington Post* and other newspapers established that the anthrax was almost certainly obtained from a U.S. lab. See also the report of the Federation of American Scientists on the profile of the likely perpetrator, a U.S.-trained scientist at http://www.fas.org/bwc/news/anthraxreport.htm (last visited June 26, 2002). Rick Weiss & Susan Schmidt, *Capitol Hill Anthrax Matches Army's Stock: 5 Labs Can Trace Spores to Ft. Detrick*, WASH. POST, Dec. 16, 2001, at A1; Rick Weiss & Dan Eggen, *US Says Anthrax Germ in Mail is "Ames" Strain: Microbe is of Type Commonly Used in Research*, WASH. POST, Oct. 26, 2001, at A8.

51. *See generally* ETZIONI, *supra* note 33.

of proposals to expand surveillance, including adoption of a National ID card and new airport screening procedures.[52] It is Etzioni's view that these measures will promote public safety and reduce the risk of future terrorist acts.[53]

David Brin, author of *The Transparent Society*, argued in similar fashion that privacy should give way to other social interests, particularly the need for greater openness and transparency that characterizes democratic society.[54] Brin has also argued since September 11 for greater tracking and monitoring procedures.[55]

Corporate leaders such as Scott McNealy and Larry Ellison have also argued that the interests of privacy must be traded against the interests of openness and both have argued since September 11 for the creation of a system of national identification.[56] Ellison has specifically proposed that software and services developed by his company could provide the basis for greater information sharing across federal agencies.[57]

In my view, none of these scholars, writers, or business leaders properly understands the relationship between privacy and secrecy. For privacy scholars and advocates, the relationship between privacy and transparency is well understood. It was expressed most famously, and a bit paradoxically, by the European scholar and early architect of data protection laws Jan Freese, who said, "We must protect privacy to enable the free flow of information."[58] But whereas many have seen a sharp contrast between the U.S. privacy and the European privacy tradition, the similarities are significant, particularly in understanding the proper relationship between privacy and secrecy.

---

52. Amitai Etzioni, *You'll love those national ID cards*, CHRISTIAN SCI. MONITOR, Jan. 14, 2002, at 11.

53. *See id.*

54. *See generally* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY MAKE US CHOOSE BETWEEN FREEDOM AND PRIVACY? (1998).

55. David Brin, *Some Notes About Calamity and Opportunity*, *at* http://www.futurist.com/911/notes_about_calamity.htm (last visited May 17, 2002).

56. *See* David Streitfeld & Charles Piller, *Response to Terror, A Changed America: Big Brother Finds Ally in Once-Wary High Tech*, L.A. TIMES, Jan. 19, 2002, at A1; Larry Ellison, *Digital Ids Can Help Prevent Terrorism*, WALL ST. J., Oct. 8, 2001, at A23, *available at* http://www.oracle.com/corporate/index.html?digitalid.html.

57. *See* Ellison, *supra* note 56.

58. Marc Rotenberg, *Privacy and Transparency: The Paradox of Information Policy* , *at* http://www.rlg.org/annmtg/rotenberg01.html (2001).

I would like to turn now to the American tradition of seeking to protect both privacy while limiting government secrecy. It is my contention that this tradition, the one that sees privacy and openness as complimentary values, is most at risk after September 11. To make this point I will point to three critical historical references: the opinions of Justice Brandeis, the post-Watergate reforms of the U.S. Congress, and the establishment of the OECD Privacy Guidelines in 1980.

To understand the complimentary nature of privacy and openness, it is useful to look briefly of the legacy of the jurist most responsible for the legal right of privacy in America. Louis Brandeis is well known for the publication of the 1890 article on *The Right to Privacy,*[59] which became the basis for the American privacy tort, and almost as well known for the 1928 dissenting opinion in *Olmstead v. United States*, in which he described privacy as "the most comprehensive of rights."[60] But Brandeis is less well known, at least in many of the popular debates on privacy, for his views on the First Amendment and open government. It was Brandeis who said, "[s]unlight is said to be the best of disinfectants. . . ."[61] It was Brandeis who, together with Justice Holmes, wrote opinions that challenged the World War I convictions for unpopular speech under the Sedition Act.[62] In these opinions and others, Brandeis championed a view of the world in which both a secure private sphere could be protected in law and a robust public sphere of debate and

59. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

60. 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

61. LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY, AND HOW THE BANKERS USE IT 92 (1914) ("Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.").

62. *See* Abrams v. United States, 250 U.S. 616, 626 (1919) (Holmes, J., dissenting and Brandeis, J., concurring in the dissent). *Cf.* Schaefer v. United States, 251 U.S. 466, 482 (1920) (Brandeis and Holmes, J.J., dissenting) ("The constitutional right of free speech has been declared to be the same in peace and in war."); Whitney v. California, 274 U.S. 357, 372 (1927) (Brandeis, J., concurring).

> [The founding fathers] knew order cannot be secured merely through fear of punishment for its infraction; that it is hazardous to discourage thought, hope, and imagination; that fear breeds repression; that repression breeds hate; that hate menaces stable government; that the path of safety lies in the opportunity to discuss freely supposed grievances and proposed remedies; and that the fitting remedy for evil counsels is good ones.

Id.

democratic activity could be achieved.[63]

My second piece of historical evidence are the statutes enacted by Congress in the post-Watergate era that sought to protect the rights of citizens and to limit abuse by government, particularly in the context of new information technologies. In enacting both the Privacy Act of 1974[64] and adopting the amendments that same year which significantly strengthened the Freedom of Information Act, Congress sought to ensure that personal information collected and maintained by federal agencies would be properly protected while also seeking to ensure that public information in the possession of federal agencies would be widely available to the public.[65] The complimentary goals of safeguarding individual liberty and ensuring government accountability were enabled by legislation that protected privacy on the one hand and promoted government oversight on the other. To this day, the twin goals of limiting disclosure of personal information held by government agencies and enabling access to public information has been followed by nations around the world.[66]

Finally, let us consider the OECD Privacy Guidelines of 1980,[67] considered by many the most widely adopted articulation of privacy rights in the world.[68] The OECD Guidelines clearly impose restrictions on the collection and use of personal information.[69] Indeed, one of the critical contrasts between the OECD Guidelines and other less robust means for privacy pro-

63. *See generally* PHILIPPA STRUM, BRANDEIS: BEYOND PROGRESSIVISM (1993); PHILIPPA STRUM, LOUIS D. BRANDEIS: JUSTICE FOR THE PEOPLE (1984); *cf.* Int'l News Serv. v. Associated Press, 248 U.S. 215, 263 (1918) (Brandeis, J., dissenting) (suggesting that, given the vast public interest in news stories, such information should not be copyrightable, because to do so would "effect an important extension of property rights and a corresponding curtailment of the free use of knowledge and of ideas.").

64. *See* Privacy Act of 1974, 5 U.S.C. § 552 (2000), *reprinted and discussed in* MARC ROTENBERG, PRIVACY LAW SOURCEBOOK 2001 at 39 (2001) [hereinafter PRIVACY LAW SOURCEBOOK].

65. *See* PRIVACY LAW SOURCEBOOK, *supra* note 64, at 39, 60.

66. *See, e.g.*, Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, ch. 165 (1993) (Can.).

67. *See* OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) [hereinafter OECD Privacy Guidelines], *reprinted in* PRIVACY LAW SOURCEBOOK, *supra* note 64, at 268-96.

68. *See, e.g.*, David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 11 (1999).

69. *See* OECD Privacy Guidelines, *supra* note 67.

tection, such as the FTC articulation of Fair Information Practices, is the failure to specifically include such concepts as "use limitation," "collection limitation," "disclosure limitation," or "secondary purposes."[70]

But it is equally clear that the other metric by which privacy policies often fail to match the standards set out by the OECD Guidelines is the absence of a corresponding requirements for transparency. The OECD Privacy Guidelines make clear that for privacy protection to be effective, transparency and access concerns are paramount.[71] In many respects the OECD Guidelines mirror the goal set out in the 1973 report that gave way to the adoption of the Privacy Act in 1974, and that was to ensure that there were no secret databases in government tracking the lawful activities of citizens.[72]

In outlining this argument that privacy and openness are complimentary values, I do not intend to deny that there are hard cases that may place these interests in conflict.[73] This was clear in the Court's consideration of *Bartnicki v. Vopper* last term, in which the Court held that the First Amendment precluded liability under the federal wiretap statute for publication of information obtained by means of illegal wiretap where the publisher was not the person who had committed the unlawful interception.[74] Although it is fair to note that there are competing free speech values for the participants in a conversation who wish to make use of new technology to exchange information that might not otherwise be disclosed absent the statutory protection, for those who wish to publish the contents

---

70. *See* Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (May 2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. *See also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137 (2002); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1461 (2001); Paul Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV. 743, 781-86 (2000).

71. "The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard." PRIVACY LAW SOURCEBOOK, *supra* note 64, at 290 (citing OECD Privacy Guidelines).

72. DEPT. OF HEALTH, EDUC. AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973).

73. *Fla. Star v. B.J.F.*, 491 U.S. 524 (1989), which held a rape shield statute unconstitutional, is clearly one such case.

74. 532 U.S. 514 (2001).

of the conversation, their right to publish conflicts directly with the privacy interests of the parties to the conversation.

There are similar clashes over access to court records in electronic form and the publication of private matters by the press.[75] Even EPIC faced the difficult question of whether to proceed with a Freedom of Information Act lawsuit against the Department of Justice to determine the status of those who were detained after September 11.[76] Clearly that case illuminates the concern that the disclosure of a person's detention could be stigmatizing and could create actual harm as to future employment and economic opportunity for the individuals whose status was disclosed. But it was also out of recognition that the privacy interests of the detainees could not become a proxy for the desire of government to maintain secrecy surrounding these possibly unlawful detentions that we at EPIC decided to go forward. It was and is our view that mechanisms could be created to enable disclosure of detainees' status that would minimize the privacy risk while maximizing the likelihood that some light would be shed as to the government's conduct.[77]

More broadly, we might say about modern privacy law that the aim is to enable both personal privacy and government accountability in the use of new technology by limiting the collection and use of personal information where possible and by imposing disclosure and reporting requirements where such collection occurs. Privacy law has made clear the particular importance of this goal in the area of new technologies where systems of surveillance dramatically amplify state authority.[78]

---

75. *See Bartnicki*, 532 U.S. 514; *Florida Star*, 491 U.S. 524; Doe v. Otte, 259 F.3d 979 (9th Cir. 2001), *cert. granted*, Otte v. Doe, 70 U.S.L.W. 3514 (U.S. Feb. 19, 2002) (No. 01-729). Similar issues have arisen with public access to court records. See generally EPIC's Public Records Page at http://www.epic.org/privacy/publicrecords/.

76. *See* EPIC, *CNS v. DOJ*, *at* http://www.epic.org/open_gov/foia/cnss_v_doj.html.

77. For example, in EPIC's 1993 litigation seeking the release under FOIA of Secret Service records pertaining to the search and seizure of *2600* employees, EPIC obtained signed statements from targets of investigation to go forward with the FOIA request for relevant records held by the Secret Service. *See* EPIC, *2600 Archive*, *at* http://www.epic.org/security/hackers/2600/.

78. So much is made clear in the Congressional findings and statement of purpose for the Privacy Act of 1974:

(a) The Congress finds that–

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Fed-

But these hard cases typically arise where there is a specific matter in dispute, a specific claim before a court. They rarely speak prospectively, as statutes do, to the ordering of privacy claims and publication requirements. And most significantly, the disputes outlined above do not require the simultaneous diminishment of personal privacy and expansion of government secrecy.

Privacy is, as Professor Raymond Shih Ray Ku suggests in his article, about power.[79] And privacy law is established to rec-

---

eral angencies;
(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination of personal information;
(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;
(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and
(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.
(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to–
(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;
(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular urpose from being used or made available for another purpose without his consent;
(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;
(4) collect, maintain, use , or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;
(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and
(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

PRIVACY LAW SOURCEBOOK, *supra* note 64, at 40-41.

79. Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002).

tify asymmetries in power and to protect the rights of individuals against institutions that are able to delve deeply into our private lives. Viewed in this light, the developments since September 11 should be seen as an expansion of state power and a consequential limitation on the freedom of individuals. The balance between the authority of the state and the rights of the individual has shifted. There has been no beneficial tradeoff between privacy and openness, as Etzioni, Brin, or Ellison have suggested.[80] There has simply been greater exposure of private life and greater secrecy surrounding the actions of government.

WHAT ARE WE TO DO?

It might be tempting at this point to stop and congratulate ourselves for this important insight about the relationship between privacy and secrecy and the underlying purpose of privacy protection in law. Much of legal study is indeed the careful consideration of doctrine, an examination of key concepts, decisions, and statutes. But I would argue today that after September 11 we have a greater obligation than just the production of a descriptive model that is intellectually satisfying.

As law students, teachers, and advocates, we should build on our legal tradition, on our Constitutional democracy, and participate in the public debates that affect us not simply as experts in the field but also as citizens who will live with the consequences of action taken or not taken by the government that we have created. We should understand that in the battle to protect privacy lies also the struggle to maintain Constitutional democracy, to safeguard the rights of citizens, and to hold government accountable. Privacy remains today as fundamental a measure of democratic society as it was when democracy when born.[81]

---

80. *See supra* notes 52, 55, 56 and accompanying text.

81.

> [J]ust as our political life is free and open, so is our day-to-day life in our relations with each other. We do not get into a state with our next-door neighbour if he enjoys himself in his own way, nor do we give him the kind of black looks which, though they do no real harm, still do hurt people's feelings. We are free and tolerant in our private lives . . . .

THUCYDIDES, HISTORY OF THE PELOPONNESIAN WAR 145 (Penguin Books 1972) (431 B.C.E.) (quoting Pericles' Funeral Oration before the Athenians); *see also* DONALD KAGAN, PERICLES OF ATHENS AND THE BIRTH OF DEMOCRACY 146-47 (1991) (In Pericles' speech to the Athenians he compares the absence of any privacy in Sparta to the Athenian regime, which "leaves considerable space for individualism and privacy, free from public scrutiny.").

If there are to be proposals to establish new systems of public surveillance, then the legal community has an obligation to assess these developments and to determine their impact on current law and the rights of citizens.[82]

In going forward with this effort, I would like to make three points. First, we should understand that the balance to be achieved here is not the one too often stated as between security and freedom. Benjamin Franklin rightly cautioned that those who would sacrifice "essential liberty for temporary security" will have neither liberty nor security.[83] The balance that must be achieved is between the authority created for government and the means of oversight to ensure that these new powers are not misused. This tradition is well established in law and it remains critical that every proposal put forward by Congress after September 11 explains how new state authority will be balanced by new means of oversight.

Second, we must avoid the risk of allowing the descriptive to collapse into the normative. By this I mean that we should not simply restate the observation that during times of national crisis, the authority of the government is necessarily expanded and the rights of the citizens are necessarily diminished. It is descriptively correct to say that Japanese Americans were interned during World War II. It is also normatively fair to say that the internment was wrong and should not have occurred. Those who cite the internment of the Japanese during the Second World War, the prosecution of pacifists during the First World War, and arguably even the suspension of habeas corpus during the Civil War in support of new restrictions on the rights of citizens should not go unchallenged. Many injustices occur in times of crisis, and the fact of prior injustice should not justify the commission of new injustice.

---

82. For example, the American Bar Association created a new committee, the Cyberspace Committee Task Force, to examine the legal issues surrounding electronic surveillance, security, and privacy in the wake of September 11. The task force was developed to formulate guidelines in the face of "[t]he new frontier forged by the intersection of data protection, electronic communications and Cybercrimes, including CyberTerrorism, [which raise] novel business problems, particularly in light of new laws and standards related to the privacy of customer information." *See* Press Release, New ABA Cyberspace Committee Task Force to Examine Legal Issues Surrounding Electronic Security & Privacy (Jan. 30, 2002) (on file with author). In particular, the Task Force "will work to identify and interpret the ramifications of new laws, such as the anti-terrorism USA Patriot Act of 2001." *Id.*

83. *See* THE OXFORD DICTIONARY OF POLITICAL QUOTATIONS 141 (Anthony Jay ed., 1996).

Most critically, we must oppose the fatalism that has captured the minds and hearts of too many Americans. We should reject the premise that after September 11 we can no longer afford the privacy or freedom that we previously enjoyed.[84] The United States has survived world war, presidential assassination, domestic riots, and economic depression. We have had nuclear weapons targeted on the nation's capital by foreign adversaries for much of the twentieth century. But none of these developments has required a permanent sacrifice in the structure of liberty established by the Constitution or by law, or, specifically, a sacrifice of the individual's freedom to limit the oversight of government. To allow crisis, even of the magnitude of September 11, to necessarily diminish the rights of citizens or the responsibility of government is a path without end.

And that remains our challenge today, after the events of September 11, and that remains the special obligation of the legal profession and legal educators. Alexis de Tocqueville told us that in the American form of government, lawyers come forward when there are great challenges.[85] We are at a similar point in history. We have a duty to safeguard privacy, to oppose secrecy, and to ensure the protection of constitutional freedom.

84. *See, e.g.*, Judy Mann, *It's a Changed World, and We Will Adapt to It*, WASH. POST, Oct. 3, 2001, at C12; Robin Toner, *Some Foresee a Sea Change in Attitudes on Freedoms*, N.Y. TIMES, Sept. 15, 2001, *at* http://www.nytimes.com/2001/09/15/national/15CIVI.html.

85. 1 ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 290 (Random House 1945) (1835).