

Moebius

Volume 1
Issue 2 *Privacy*

Article 7

4-1-2003

Nothing to Hide, Nothing to Fear

Philip L. Fetzer

California Polytechnic State University - San Luis Obispo, pfetzer@calpoly.edu

Follow this and additional works at: <http://digitalcommons.calpoly.edu/moebius>

Recommended Citation

Fetzer, Philip L. (2003) "Nothing to Hide, Nothing to Fear," *Moebius*: Vol. 1: Iss. 2, Article 7.
Available at: <http://digitalcommons.calpoly.edu/moebius/vol1/iss2/7>

This Essay and Article is brought to you for free and open access by the College of Liberal Arts at DigitalCommons@CalPoly. It has been accepted for inclusion in Moebius by an authorized administrator of DigitalCommons@CalPoly. For more information, please contact mwyngard@calpoly.edu.

NOTHING TO HIDE, NOTHING TO FEAR

Philip L. Fetzer

We live in an age when governmental and commercial interests are actively undermining our right to privacy. “Privacy” is an amorphous concept. It may entail the simple right “to be let alone.”¹ Additional aspects of privacy include: protection from public scrutiny of one’s intimate relations, informational regulations that restrict access to financial and medical records, and rules that address an individual’s right to terminate a pregnancy. In spite of an apparent desire for privacy, our commitment to privacy appears to be weak and inchoate.

Television is a prime source of a slow, but indisputable blurring of the differences between the “private” and “public.” As Joshua Meyrowitz noted in the mid-1980’s:

“Television removes much of the doubt as to what subjects one’s children or parents know about. Any topic on any popular situation comedy or talk show, news program, or advertisement—be it death, homosexuality, abortion, male strippers, sex-change operations, political scandals, incest, jock itch, or bras that ‘lift and separate,’—can be spoken about the next day in school, over dinner, or on a date, not only because everyone now knows about such topics, but also because everyone knows that everyone knows that everyone knows. In fact, it almost seems strange not to talk and write about such things. The public and all-inclusive nature of television has a tendency to collapse formerly distinct situations into one.”²

American consumers have played an active role in encouraging this breakdown as well. Ubiquitous cell phone usage and ATM machines mean that formerly private conversations and financial transactions are now conducted in a public setting. Large numbers of individuals not only are unaware of this loss of privacy but are positively eager to participate in it.³

Public Opinion and Privacy

Three weeks after the attacks of September 11, the *New York Times* reported that “8 in 10 Americans believe they will have to give up some of their personal freedoms to make the country safe from terrorist attacks.”⁴ The initial government response to the attacks included aggressive efforts to diminish traditional privacy rights. Attorney General John Ashcroft, for example, ordered monitoring of the conversations “between selected inmates and their lawyers.” Ashcroft’s argument? “Let’s be clear about what it is: [it’s] designed to keep people from continuing to perpetrate crimes through their lawyers’ sometimes unwitting cooperation,” he said.⁵ The White House believes that the public will support their position on this and other related actions that undermine privacy.⁶ And the leaders of the Executive Branch may be right.

In times of fear, security concerns rise to the top. As Georgetown law professor David Cole states, “We love security more than we love liberty.”⁷ Will the courts protect us from a diminution of our privacy rights? Not likely. “[T]he justices are part of the same culture that is willing, in times of war, to trade civil liberties for security,” in the opinion of University of Virginia law professor Michael Klarman.

Privacy and the Courts

The primary legal foundation for a “right to privacy” is found in the Fourth Amendment to the Constitution.

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”⁸

As Professor Sheldon Goldman noted, the Fourth Amendment clearly contains “a substantive right of privacy.”⁹ In a critical ruling that laid the foundation for

the Supreme Court's landmark abortion decision, *Roe v Wade*, the Court, speaking through Justice Douglas concluded that: "[S]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees, that help give them life and substance...Various guarantees create zones of privacy."¹⁰

Privacy of communications has been a subject of close analysis by the Court. In 1928, the Court first considered the use of wiretapping. The Justices held that use of wiretaps did not constitute "a search and seizure" under the meaning of the Fourth Amendment.¹¹

Nearly four decades later, the Supreme Court changed its mind. Ruling in *Katz v United States*, Justice Stewart concluded:

"...the Fourth Amendment protects people not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection...But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."¹²

Five years after *Katz*, the Court ruled on the issue of presidential power to authorize electronic surveillance in internal security matters. The government argued that it was lawful to wiretap without prior judicial approval and proper search warrants because the president was acting "to protect national security."¹³ Justice Powell held that "Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept."¹⁴

Surveillance in the 21st Century

In early October of 2001, writing in *The New York Times Magazine*, Jeffrey Rosen, discussed recent developments in surveillance.¹⁵ A company called "Visonics" is

"...the industry leader in a fledgling science of *biometrics*, a method of identifying people by scanning and quantifying their unique physical characteristics—their facial structure, for example, or their retinal patterns. *Visonics* manufactures a face-recognition technology called *FaceIt*, which creates identification codes for individuals based on 80 unique aspects of facial structure..."¹⁶

Joseph Atick is the CEO and founder of *Visonics*. After the terrorist attacks, he saw a business opportunity to market his product. He proposed that key airports

throughout the United States could be “wired up” with more than 300 cameras each. These cameras could then scan the faces of passengers in line or in other public areas. They could also be placed in sports stadiums, subway systems and near national monuments.¹⁷

It turns out that the United Kingdom has already taken the lead. Rosen writes: “According to one estimate, there are 2.5 million surveillance cameras in Britain, and in fact, there may be far more.”¹⁸ However, Rosen notes, “The cameras are designed not to produce arrests but to make people feel that they are being watched at all times...rather than thwarting crime, the cameras are being used to enforce social conformity in ways that Americans may prefer to avoid.” How good are these cameras at detecting “evil doers”? In a documentary about close-circuit television (CCTV), former Monty Python actor John Cleese fooled the *Visionics* system by wearing earrings and a beard.¹⁹ The apparent relationship between the public’s anxiety about safety and its willingness to accept a reduction in privacy can be illustrated by attitudes about surveillance activities.

Public opposition to expanded governmental surveillance has been limited. While expressing considerable opposition to telephonic intrusions by telemarketers, Adam Liptak wonders why large numbers of individuals don’t seem equally concerned about the government activity that is similar. “That dichotomy is a little hard to explain,” he writes, “given that intrusion by the government can be life-altering while most businesses can do little more than annoy people with phone calls at dinner time. The answer, it appears, is that many people believe the government will invade only someone else’s privacy. Privacy for me, they seem to be saying, but not for thee.”²⁰

Privacy and the USA PATRIOT Act

President Bush signed the “USA PATRIOT Act” into law on October 26, 2001. The law includes a wide variety of provisions that enhance the law enforcement powers of federal agencies such as the FBI and CIA. Section 215 of the act, for example, permits agents of the FBI to gain access to library records of “any individual government investigators claim is connected to an investigation into spying and terrorism.”²¹ The government does not need to have evidence “of any crime, nor provide evidence to a court that their target is suspected of one.”²²

The director of libraries in Santa Cruz said, in response to this new law: “Particularly pernicious is the idea that library staff are not allowed to tell people targeted by the FBI about what is happening. That kind of secrecy is straight

out of Nazi Germany.”²³ According to one study, government agents have visited 85 academic libraries looking for information under provisions of the *PATRIOT Act*. Assistant Attorney General Daniel Bryant stated that “Americans who borrowed library books automatically surrendered their right to privacy.”²⁴ Clarifying Bryant’s remarks, another administration spokesperson said the law was “a threat only to those who might have something to feel guilty about.”²⁵

Under the *PATRIOT Act*, the FBI has issued scores of “national security letters.” These directives require businesses to turn over a wide array of electronic records including email, telephone calls, and finances. The law permits FBI field office employees, rather than senior officials, to issue these orders.²⁶ Beryl Howell, a former advisor to Senator Patrick Leahy (D-Vt) stated that “national security letters represent “unchecked, secret power that makes it invisible to public scrutiny and difficult even for congressional oversight.”²⁷ The act also permits secret searches without notification to the owner of the dwelling or property.²⁸ Since the Constitution provides that government may not conduct searches without a warrant and a showing of “probable cause,” these provisions of the law may be found illegal.

Justice Department

Earlier this year the *Los Angeles Times* reported that the Justice Department had “stepped up use of a secretive process that enables the attorney general to personally authorize electronic surveillance and physical searches of suspected terrorists, spies and other national-security threats without immediate court oversight.”²⁹ Attorney General Ashcroft testified that he had authorized over 170 emergency searches since the attacks of September 11, 2001. This is more than triple the number previously authorized by attorney generals in the last 20 years.³⁰

The *Foreign Intelligence Surveillance Act* (FISA), adopted in 1978, permits investigations under the supervision of a secret federal court known as the “Foreign Intelligence Surveillance Court.” A provision of FISA allows the government to initiate searches authorized only by the attorney general. A spokesperson for the ACLU expressed concern that the federal government is using FISA to pursue traditional criminal cases while claiming that they are “national security” investigations. Defendants’ traditional 4th Amendment rights don’t apply in FISA cases.³¹

Total Information Awareness

In late November of 2002, Adam Liptak of the *New York Times* reported on a new Defense Department proposal. Liptak wrote:

“The Pentagon also attracted considerable attention this month for a proposed database of unprecedented scale to help government antiterrorism efforts. It would collect every sort of information imaginable, including student grades, Internet activity and medical histories.”³²

Shortly after Liptak’s piece appeared, Hendrick Hertzberg wrote on the subject in *The New Yorker*.³³ Hertzberg described “the Information Office of the Defense Advanced Research Projects Agency of the Department of Defense.” “[I]t’s official mission, Hertzberg wrote, “is to imagine, develop, apply, integrate, demonstrate and transition information technologies, components and proto-type, closed-loop information systems that will counter asymmetric threats by achieving total information awareness.”³⁴ Among the office’s subdivisions is the “Human Identification at a Distance program. This office’s proposed tasks include “Face Recognition” and “Gait Recognition.”³⁵

However, the main “assignment” of the new office is, in Hertzberg’s words:

“[T]o turn everything in cyberspace about everybody—tax records, driver’s license applications, travel records, bank records, raw F.B.I files, telephone record, credit-card records, shopping-mall security camera videotapes, medical records, every e-mail anybody ever sent—into humongous, multi-googolplexibyte database that electronic robots will mine for patterns of information suggestive of terrorist activity. Dr. Strangelove’s vision—‘a chikentic complex of gumbyuders’—is at last coming into its own.”³⁶

Software for an early version of the Total Information Awareness system is called “Groove.” “Groove” was developed by Ray Ozzie.³⁷


Congress reacted negatively to the proposed new system. House and Senate conferees agreed that this project should not be used against Americans. The conference committee also concluded that further research on the program could not be continued without a specific appropriation from Congress.³⁸ Nonetheless, a Pentagon spokesperson stated that the Defense Department “[S]till feels it’s a tool that can be used to alert us to terrorist acts before they

occur.” “It’s not a program that snoops into American citizens’ privacy,” said Lieutenant Commander Donald Sewell.³⁹

Conclusion

What is one to make of this? What we know is that when people are afraid, they are quite willing to sacrifice many traditional liberties. Are expanded surveillance systems, investigation of library records, denial of traditional lawyer-client privileges, and “Total Information Awareness,” consistent with the values of a free and open society?

Can any government, including the current administration in Washington, be trusted not to abuse the unprecedented powers that it has already or that it is seeking to acquire? While in commercial transactions, we “can always opt out...[because we] have a certain amount of choice. In terms of government surveillance, we really do not,” notes Jane Kirtley, a professor of law and media ethics at the University of Minnesota.⁴⁰

At the same time, the governmental response to the new threats facing Americans might help uncover terrorist networks. The trade-off between liberty and security might be worth the price. And, after all, as former British Prime Minister John Major said, “If you’ve got nothing to hide, you have nothing to fear.”⁴¹ 

Endnotes

1. Mason, Alpheus T., and Stephenson, Donald Grier, Jr. *American Constitutional Law* 13th ed. Upper Saddle River, NJ: Prentice-Hall, 2002. 592.
2. Meyrowitz, Joseph. *No Sense of Place*. New York: Oxford University Press. 1985. 92.
3. See, for example, Markoff, John and Schwartz, John, “Many Tools of Big Brother Are Now Up and Running.” *New York Times*, December 23, 2002, C1. “Because of the inroads the Internet and other digital network technologies have made into everyday life over the last decade, it is increasingly possible to amass Big Brother-like surveillance powers through Little Brother means. The basic components include everyday digital technologies like e-mail, online shopping and travel booking, A.T.M. systems, cell phone networks, electronic toll-collection systems and credit-card payment terminals.
4. Rosen, Jeffrey. “A Watchful State,” *New York Times Magazine* 7 October 2001: 93.
5. Toner, Robin. “Civil Liberty vs. Security, Finding a Wartime Balance.” *New York Times* 11 Nov. 2001: B6.
6. *Ibid.* “The administration is convinced that the public is on its side and share the view that, as one White House Official put it, ‘it’s a new reality.’ The old rules, the old legal and law enforcement cultures, have to change, to prevent future attacks and to prosecute terrorists in ways benefiting their acts.”
7. *Ibid.*
8. Amendment IV, United States Constitution.

9. Goldman, Sheldon. *Constitutional Law: Cases and Essays*. 2nd ed. New York: Harper Collins, 1991. 569.
10. *Griswold v Connecticut*, 381US479 (1965) Justice Douglas went on to list the 3rd, 4th, 5th and 9th Amendments as, together, creating this “zone of privacy.”
11. *Olmstead v United States*, 277US438 (1928).
12. *Katz v United States*, 389US347 (1967) Italics added.
13. *United States v United States District Court*, 407US297 (1972) The case related to the bombing of a CIA office in Ann Arbor, Michigan.
14. Ibid.
15. Rosen, op.cit, 38 ff.
16. Ibid, 38. Italics added.
17. Ibid., 40.
18. Ibid., 41.
19. Ibid., 42.
20. Liptak, Adam. “In the Name of Security, Privacy for Me, Not Thee.” *New York Times* 24 Nov. 2002, sec. 4, 1.
21. Donegan, Lawrence. “Anger as CIA home in on new target: library users.” *Guardian Unlimited* 16 March 2003 (on-line). Section 215 applies to bookstores also.
22. Ibid.
23. Ibid.
24. Ibid.
25. Ibid.
26. Eggen, Dan and O’Harrow, Robert, Jr. “U.S. Steps Up Secret Surveillance.” *Washington Post* 24 March 2003: 1.
27. Ibid.
28. See “Surveillance Under the Patriot Act,” (on-line aclu.org) See section 213 of the USA PATRIOT Act..
29. Schmitt, Richard, “U.S. Expands Clandestine Surveillance Operations.” *Los Angeles Times* 5 March 2003: 10.
30. Ibid.
31. Ibid.
32. Liptak, op. cit., 1.
33. Hertzberg, Hendrick. “Too Much Information.” *The New Yorker* 9 December 2002: 45.
34. Ibid.
35. Ibid.
36. Ibid.
37. Markoff and Schwartz, op. cit. Ozzie was the inventor of Lotus Notes.

38. Ibid.
39. Ibid.
40. Liptak, *op.cit.*, 3.
41. Rosen, *op.cit.*, 41.