THE FEDERAL COURTS LAW REVIEW

Volume 3, Issue 2 2009

Privacy: Is there any Left?

Arthur R. Miller[1]

It is a delight to be here, and I thank you for the invitation to participate in this symposium. Having said that, I have to admit I'm a bit of a fraud. I started thinking about privacy in the 1960s and was quite active in the development of various statutes and served on commissions for a number of years. I really haven't contributed much to the debate about privacy for some time. But, Allyson[2] asked me to talk about privacy, perhaps because they wanted to get more work out of me while I was visiting the law school.

As I address this audience, I am struck by how many of you are devoted to privacy; for example, Peter Winn,[3] with whom I had a lovely conversation this morning. He will speak to you later in the day. And understand that Peter is a contemporary scholar on privacy law, and is not, as I am, years behind the subject. So, what I can offer you is some background, some history, a touch of sociology and philosophy; that will be the tenor of my remarks.

I started to get interested in privacy at the point of a gun. At

---

1. Editor's note: Arthur R. Miller was the keynote speaker at the Federal Courts Law Review's Symposium *Privacy in the Federal Courts* on April 11, 2008. Arthur R. Miller is currently a University Professor at the NYU Law School after teaching thirty-six years at Harvard Law School, where he also earned his law degree. Among his numerous areas of scholarship and expertise, Professor Miller is perhaps best known for his co-authorship, along with Charles Alan Wright, of the widely referenced multi-volume treatise, *Federal Practice and Procedure*. In addition to his many other accolades and accomplishments, he has been the reporter for the American Law Institute's Project on Complex Litigation, a member of Special Advisory Group to the Chief Justice of the United States Supreme Court on Federal Civil Litigation, and a member of the American Bar Association Special Committee on Complex and Multidistrict Litigation. Professor Miller was one of the earliest participants in the field of technology and privacy.

2. Allyson W. Haynes, Associate Professor of Law at the Charleston School of Law.

3. Peter A. Winn, Assistant U.S. Attorney with the U.S. Department of Justice, Office of the U.S. Attorney.

least, it seemed like a gun, held by that great Senator from North Carolina, Sam Ervin. He apparently had been told that I was somebody who had been thinking about technology, privacy, and law. Actually, it was technology and copyright that I had been studying. Nonetheless, the Senator insisted that I be his lead-off witness in a set of ground-breaking hearings on the proposed National Data Center,[4] which I think took place in 1966 or 1967. When I thought about the assignment and began studying the subject, I realized I was emotionally attracted to the concept of privacy. It turns out I felt—and continue to feel—deeply about privacy for reasons that shall remain private with me.

When I began to write on the subject seriously,[5] I spoke with a lot of people. I would ask, "What do you think about privacy?" If the person didn't think I was a mugger, he might say: "Privacy? I don't think much about it. It's not part of my consciousness." Or, she might respond with: "Privacy? You mean wiretapping?" I would explain that is not what I meant. Wiretapping is a very labor intensive, low productive form of surveillance. Or if I met somebody who was sophisticated, he or she might say: "Privacy is a white, middle class, suburban value. Poor people are so dependent on the dole and public benefits that they simply cannot afford to think about privacy. And rich people? Well, they buy their privacy. They put smoked glass on their automobile windows and they build big fences." Then that person would walk away. In short, privacy was barely on anyone's radar screen.

But a few years later, funny things started to happen. Privacy became something that had begun to creep into people's consciousness. Maybe it started with those hearings on the National Data Center held by Senator Sam, which received considerable attention. Maybe it was a result of IBM and other companies overselling the wonders of technology, and people beginning to see the nexus between data collection and individual privacy. In any event, privacy began to ascend in society's hierarchy of concerns and the "Big Brother" image of government intrusiveness came to the fore.

---

4. *See* Arthur R. Miller, *The National Data Center and Personal Privacy*, ATLANTIC, Nov. 1967, at 557.

5. *See, e.g.*, ARTHUR R. MILLER, THE ASSAULT ON PRIVACY – COMPUTERS, DATA BANKS AND DOSSIERS (1971); *see also* Arthur R. Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology on an Information-Oriented Society*, 67 MICH. L. REV. 1089 (1969).

As many of you know, organizations like Field,[6] Roper,[7] and Yankelovich[8] do attitudinal surveys for the business community periodically. They want to know: What are Americans thinking about? What do they worry about? And it's very, very striking what those surveys began to show in the 1970s and 1980s. Indeed, in something akin to poetic justice, in the year 1984—the Orwellian year of 1984—as reflected in the surveys for the business community, privacy became a major concern in this country. Americans had begun to fear losing it.

Privacy. What are we talking about? Who cares about it? Are we talking about Howard Hughes, the billionaire recluse? Are we talking about film star Greta Garbo and her famous, "I want (or *vant*) to be alone?" Are we talking about paranoids? What are we really talking about? What kind of a value is under discussion, and how important or unimportant is it?

To me, privacy, or the right to be left alone, is a value of great importance in a civilized society. An individual's ability to close the physical or metaphorical door is an enormously powerful human capability. Whether it is to shut out unwanted music from a teenager's room or to combat the intrusiveness of neighbors, institutions, or the government, the ability to enjoy solitude is important. But, I think privacy goes beyond that.

Privacy is about individuality. It is about autonomy. It is about self-determination. It is about the ability to control, at least to some degree, the content of and the access to the informational envelope that surrounds us as we go through our lives in today's complex, technological world.

Now, Judge Carr,[9] who spoke earlier, said: "Well, South Carolina's got it in its state constitution; the Feds don't." So how important can it be? After all, stop and think about all the other societal values and objectives that work against the right of privacy and, some would say, trump it. Consider free speech and its sacred subpart, free press. Some would say that, that is this nation's most distinctive right. Consider the public's right to know. "Transparency" has become a popular mantra in both the public and private sectors. Consider our desire for fiscal accountability. "We have got to get

6. Level Field Institute, http://www.levelfieldinstitute.org/.
7. Roper Center for Public Opinion Research, http://www.ropercenter.uconn.edu/.
8. Yankelovich, http://www.yankelovich.com/.
9. The Honorable Robert S. Carr is a United States Magistrate Judge in Charleston, South Carolina.

those welfare cheats" is a common refrain. Think about effective law enforcement—making our streets and homes safe. Think about national security and the war against terror. After all, the Constitution, as the cliché goes, is not a suicide pact. Now, those are important things and, some—indeed, many—say, take precedence over an individual's privacy.

What considerations can the privacy proponents identify in support of privacy that matches the importance of any of those? Well, let's pick up the judge's reference a few minutes ago to the Constitution. I ask you to think about yourselves as you sit in this audience. You all appear to be relatively peaceful, calm, and relaxed. I doubt that any of you are concerned that some policeman is breaking down the door of your home while you are at this Symposium.

Why? Because you know about the Fourth Amendment to the Constitution. You know there is a right to be protected against unreasonable searches and seizure by the government.[10] That, in effect, is a privacy right. It is a spatial privacy right.[11] And it is in the Constitution.

Again, I ask you to reflect as you sit here: Are you worried about being seen near the person sitting next to you? Are you worried that he or she may be a commie? A republican? A vegetarian? A Yankee fan? No, you are not worried because you know that our sacred document—again, the Constitution—right there in the First Amendment[12]—guarantees your freedom of association. That is another form of privacy. We call it relational or associational privacy.[13]

---

10. U.S. CONST. amend. IV ("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.").

11. *See* Lawrence v. Texas, 539 U.S. 558, 562 (2003) ("Liberty presumes an autonomy of self that includes freedom of thought, belief, expression, and certain intimate conduct . . . [and by invoking] liberty of the person both in its spatial and in its more transcendent dimensions.").

12. U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.").

13. *See* Roberts v. U.S. Jaycees, 468 U.S. 609, 618 (1984) ("The Court has long recognized that, because the Bill of Rights is designed to secure individual liberty, it must afford the formation and preservation of certain kinds of highly personal relationships a substantial measure of sanctuary from unjustified interference by the State.").

Once again think about what you are doing while you are sitting out there. I know you are trying to make it appear that you are listening to me, but in reality your mind probably is filled with other far away thoughts, "What's for dinner? What movie this weekend?" All sorts of thoughts; all sorts of unrelated thoughts, including some crazy thoughts. The moon is made of green cheese. The Atlanta Braves will win the World Series. You are not concerned. You know you have the intellectual freedom to think these thoughts—you have freedom of thought. Your mind is a no trespassing zone. That too is privacy, and that too is in the Constitution.[14]

And finally, in what probably is the most emotional legal (and ethical) issue of our time, whether you agree or disagree, there is a constitutional right to make decisions about your own body.[15] And it takes a variety of forms, from the right to choose whether to terminate a pregnancy, within certain limits, all the way over to the right to decline medical assistance—loosely called the right to die.[16]

If you remember *Roe v. Wade*, you may recall that Justice Blackmun, in his opinion for the Court, said this right was in the Constitution; he was writing about a privacy right.[17] To be sure, he had a little bit of difficulty locating it in the text of the document. He worked through the First, Fifth, Ninth, and Fourteenth Amendments, concluding, in effect, he just knew it was there.[18] This is something that former Federal Judge Robert Bork refused to acknowledge when he was a nominee for the Supreme Court, and I believe it cost him the position.[19] I was then quite active on television so people used to recognize me, stop me in the street, and ask: "How can this guy be appointed to the Supreme Court if he doesn't believe there's a right to privacy?" Of course, Bob never really said that; he simply was unwilling to concede privacy was provided for in the Constitution. And, in fact, the word "privacy" does not appear in the document's

---

14. *See, e.g.*, Palko v. Connecticut, 302 U.S. 319, 327 (1937) ("[Freedom of thought] is the matrix, the indispensable condition, of nearly every other form of freedom."), *overruled on other grounds by* Benton v. Maryland, 395 U.S. 784 (1969).

15. *See* Union Pac. Ry. Co. v. Botsford, 141 U.S. 250, 251 (1891) ("No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.").

16. *See* Yale Kamisar, *The "Right To Die": On Drawing (and Erasing) Lines*, 35 DUQ. L. REV. 481 (1996); *see also* Yale Kamisar, *Against Assisted Suicide—Even a Very Limited Form*, 72 U. DET. MERCY L. REV. 735 (1995).

17. Roe v. Wade, 410 U.S. 113 (1973).

18. *Id.* at 152-54.

19. 100 CONG. REC. S29063 (1987).

text.

As I have just indicated, there are four strands of the right of privacy that are constitutionally based. But what this meeting is about is a fifth form of privacy, which one would have to acknowledge, has not received and may never receive constitutional sanctioning from the court—informational privacy. I personally believe that the status of informational privacy presents the true central challenge for the policy makers in the twenty-first century.

Now let's explore why people are concerned about the need to protect the privacy of information about themselves. Why is it that it has ascended in the consciousness and concern of Americans? There are several elements to these apprehensions. When you look at them, they give you a sense of the implications of contemporary information practices and indicate what is on the scales to balance against the strong societal values I mentioned earlier.

It is not immediately apparent how you balance privacy and national security or the public's right to know or any of the other things that potentially work against privacy. I must confess, I just don't know how you do that. Indeed, can it be done other than by guess work? But, one of the joys of being in the legal profession is that we are supposed to be problem solvers. We are supposed to be adept at balancing competing interests, competing values, and competing rights. That to me is the joy and challenge of being a lawyer.

Today we all appreciate the scale of modern information gathering and the power of computer technology. But I'll tell you, back in the 1960s and 1970s, people did not appreciate the data revolution that was underway. But now, people understand a stark reality: there is very little we do in our life that is not recorded. It is true that we live in the most free nation on the planet. Yet, we are the most recorded, dossier subjected, and data-banked people on the planet—with the possible exception of one or two of the Scandinavian countries. Therein lies the first concern people have.

Let me be autobiographical. I go to an airport a couple of times a week. Before the self-service computerized ticketing kiosks appeared, I used to wheel up to the check-in counter, and frequently there would be a beatific face shrouded in brown hair looking at me. And the face would say, "good morning," and I would feel uplifted by the human contact. But then, suddenly, the face would be gone. All I would see is the brown hair that used to surround the face, because the face was now completely devoted to a computer screen. At that

moment, I would begin to realize certain depressing things, and my paranoia would come into focus and to the fore.

My ability to fly the friendly skies of—let's say—United Airlines to Des Moines, did not depend on the fact that I was standing there. It did not depend on the fact that, as in the old days, I was waving a ticket into the brown hair. My ability to get aboard the plane depended on whether that computer screen told that beatific face I existed and really was booked as a passenger. I was nothing more than a mere three-dimensional version of the computer screen.

In other words, I had lost my ability to control the situation. I had lost my autonomy, my self-determination, and my individuality. I was dependent on the accuracy of what had been electronically recorded in that machine. It is no different today, of course, with the information in the kiosks. And sadly, I don't even have the pleasure of seeing and interacting with the beatific face.

And what might be recorded in that machine? Obviously, it says whether or not I was to be allowed to board that United flight to Des Moines. My credit card information is in there. The identity of the people I might be traveling with, that's also in the reservation system. There may be carry-on reservations made through the airlines: perhaps a hotel room or car rental. Also that computer screen will show whether I have a physical disability that the airline must know about and whether I've ordered one of those crazy "special" meals. When you put all of these pieces of information together you have a dossier, an informative document for anyone skilled in data analysis.

And that dossier will not disappear when I touch down at my destination. That assemblage of data elements will remain in the system, depending on the airline's tariff and practices, perhaps for 180 days. And those dossiers are quite freely available to law enforcement and security agencies. So, if you happen to be a passenger on a plane on which a mafia Capo[20] is flying, there is a clear informational relationship between you and that Capo that might be of interest to some governmental agency that will deem you worthy of further tracking—looking into other associations and activities.

And that is only the tip of the data-collecting iceberg. The phenomenon extends to all of our daily activities and beyond. The credit card you use, for example, tells where you go in any major urban area and what your buying habits are. If you go over a bridge

---

20. Capo means a high ranking member, similar to a captain or a sergeant, within organized crime. *See* HOWARD ABADINSKY, ORGANIZED CRIME (1985).

or through a tunnel and you use the Fast Lane or EZ Pass, your location and time are tracked whenever you pass through the toll barrier. Even if you use cash, the toll gate camera will record you. Increasingly, city centers are covered by camera surveillance.

How many of you turned on your TV this morning? How many of you saw a very interesting story about certain lawsuits against Google?[21] Google apparently has cars roaming around neighborhoods recording everyone's property and putting it on the net. The global internet, of course, consolidates and magnifies all of this data collection.

Another question. How many of you read Huxley's classic *Brave New World* when you were in school?[22] Remember the references to the so-called womb-to-tomb dossier? When I was a kid that was Buck Rogers, science fiction stuff. Today, of course, computer and communications technologies effectively have created a womb-to-tomb dossier on most of us. It's a reality.

Let's consider a second apprehension people feel about privacy. Again, if you watched the boob tube this morning, you saw remote feeds from reporters in far-away places. They could have come out of China with stories of oppression in Tibet; they could have come out of Texas dealing with the current polygamy controversy;[23] very likely there was a report from Iraq.

We saw our President embrace Russia's Putin last week.[24] Years ago, we watched a spacecraft explode in space, killing a number of

---

21. Google's introduction of Street View, which offers a photographic view of a streets, has raised numerous privacy concerns as well as being the subject of several lawsuits due to the multitude of individuals who have been inadvertently photographed in the process. *See* Associated Press, *Google sued over Street View*, THE BOSTON GLOBE, Apr. 5, 2008, *available at* http://www.boston.com/business/technology/articles/2008/04/05/google_sued_over_street_view/.

22. *Brave New World* is a 1932 novel by Aldous Huxley set in a future London where technology developments have dramatically changed societ. ALDOUS HUXLEY, BRAVE NEW WORLD (1932).

23. On April 3, 2008, Texas enforcement officers and child welfare investigators raided a compound in Eldorado, Texas, which was founded by convicted polygamist sect leader Warren Jeffs, after receiving a call for help from a fourteen-year-old who said she was being sexually abused inside the compound. John Dougherty & Kirk Johnson, *Sect Leader Is Convicted as an Accomplice to Rape*, N.Y. TIMES, Sept. 26, 2007, http://www.nytimes.com/2007/09/26/us/26jeffs.html?_r=1.

24. On April 5, 2008, President Bush visited Russian President Vladimir Putin in Sochi, Russia to discuss the United States' plan to install inceptor missiles in Europe. Steven Lee Myers, *Putin Unlikely to Agree on Missiles, White House Says*, N.Y. TIMES, Apr. 6, 2008, *available at* http://www.nytimes.com/2008/04/06/world/europe/06prexy.html.

American astronauts.[25] Live. What does that tell us? It tells us that information and communications technology can move any amount of pictures and information anywhere on the planet in under two seconds.

The next time you see a television feed out of Beijing or some far away place, watch the time delay between the question and the answer. That's the satellite transmission time. It's typically under two seconds. If the broadcaster is using certain satellites, the delay will be shortened and just flow. Think about it. We can move any amount of information nearly anywhere on the planet almost instantaneously. That means that in terms of personal information, we are truly globalized. There are no barriers to data transfer. We exist in virtual form anywhere and everywhere.

Remember what that great newspaperman Horace Greeley said in the middle of the nineteenth century: "Go West, young man, go west. Go to the frontier. Start a new life. Look for the opportunities. Go West, young man."[26] If Greeley were here today and he said to

---

25. On January 28, 1986, the space shuttle Challenger exploded in mid-air killing all seven crew members.

26. As many derivations of this famous quote exists, there are an equal amount of derivations on who is the source.

> Quoted in *Punchinello*, 20 Aug. 1870. This is one of the great examples of the prevalence of misinformation about famous quotations. The *Oxford Dictionary of Quotations* says that Greeley used it in his book *Hints Toward Reform* (1850), then John Babson Lane Soule used it in an 1851 editorial in the *Terre Haute* (Indiana) *Express*. *Bartlett's Famous Quotations* says that the Soule article inspired Greeley to use the quotation in an editorial in the *New York Tribune.* The *Oxford English Dictionary* gives a vague citation to Soule; many other reference works take pride in attributing the phrase to Soule rather than Greeley, who is closely associated with it in popular history. However, inspection of *Hints Toward Reform* shows that the quotation does not appear there. Thomas Fuller, writing in *Indiana Magazine of History*, Sept. 2004, found that these words also do not appear in the *Terre Haute Express* in 1851. There is no trace of the attribution to Soule before 1890, when the *Chicago Mail* made this assertion (30 June). Fuller concludes that "John Soule had nothing whatsoever to do with the phrase" and was also unable to find "go West, young man" in Greeley's writings, including the *New York Tribune* and other sources where various people have claimed it occurred. The *Punchinello* citation given is the earliest attribution to Greeley found to date, although Josiah Grinnell asserts plausibly in his autobiography *Men and Events of Forty Years* (1891) that Greeley gave Grinnell the famous advice in September 1853. James Parton, *The Life of Horace Greeley* (1855), quotes Greeley (without a specific source) as follows: "I want to go into business, is the aspiration of our young men . . . . Friend, we answer to many, . . . turn your face to the Great West, and there build up a home and fortune."
>
> Fred R. Shapiro & Joseph Epstein, The Yale Book of Quotations 322-323 (2006).

you, "go West, young person"—we have to assume he would be politically correct in his phraseology, "go west, young person"—it is a very different reality. Your credit report would arrive six hours before you did. There is no frontier. There is no fresh start. There is no escape from the past—not as far as personal data is concerned. We are followed by an informational alter ego that surrounds us and which we no longer control.

A third apprehension. If you stop and think about it, many things we do in life require decisions. Decisions about us are made by other people all the time. Many of them—if not most—are not made face to face. Many of them are made based on records we often don't know about that show whether we meet certain criteria. That will determine whether you are credit worthy, job worthy, medical procedure worthy, or social benefit worthy. People have come to recognize that reality of modern life. People understand that not only have they no control over the content and circulation of the information relating to them, but increasingly they are aware that other people who do have access to that data are making decisions about them.

For example, how does a youngster get into college or law school these days? For many law schools, it may go something like this. Let us be fanciful and consider a hypothetical, would-be law student. I will call her Alicia Aardvark: she is twenty-two, aspiring, filled with energy and enthusiasm, and she really wants to go to law school and do good things. So, first she fills out a school's application form. It may be eight pages long and call for all sorts of personal information. She probably will have to write one or more essays revealing additional aspects of herself—possibly about the most unforgettable book she ever read or why she wants to go to law school.

She probably will fill out the application manually, although the age of computer application is upon us. She folds the document up, puts it in an envelope, and commits it to the postal system. In due course, it arrives at the admissions office. There, a member of the admissions office takes the application and melds its contents with Alicia's undergraduate grade transcripts and the Law School Aptitude Test score. The LSAT was developed by the Educational Testing Service[27] in Princeton, New Jersey, and is designed to try to determine whether the applicant will be a success at her law studies. I never have been a fan of or believed in the effectiveness of that test and

27. Educational Testing Service, http://www.ets.org.

have felt it is more appropriately a product of industrial New Jersey, not Princeton.

All of this information about Alicia is input into a computer. The machine takes the grades and translates them onto a four-point scale. It also discards certain courses that the particular law school, in its infinite wisdom, believes irrelevant for appraising applicants for a legal education. It may throw out grades in military science or physical education. Perhaps it will exclude music appreciation; after all, lawyers generally are tone deaf. Then the machine recalculates Alicia's grade point average ("GPA").

The machine next looks to the particular law school's experience table with applicants from various colleges, which directs the computer to augment the GPA that the applicant earned at certain schools and, conversely, to discount the GPA earned at other schools. Grades earned at Cal-Tech may well be thought of as having a different value from those awarded at Dingbat U. And the computer even may have plus and minus factors for each of the majors at Alicia's college. Although certain majors are intense and difficult, increasingly, many undergraduate majors are thought to be fluff and short on substance.

In other words, the machine is constantly recompiling Alicia's college record. Then it turns to the Law School Aptitude Test score, a test devised by people, I fear, who may never have practiced law or may not fully understand the range of skills needed by different types of contemporary lawyers. Once again, each law school has its own weighting factor. Some weigh the LSAT equally with the GPA. Some weigh the GPA more heavily than the LSAT, two to one, three to two, or whatever. The machine massages these two variables. Ultimately, it produces a score—a number—often called a predictor index score.

That number is sent back to the law school's admissions office. See what this impersonal process has done? We started with Alicia, a living, breathing human being. First, we reduced her to an eight-page application. Then she became a group of electronic entries in a computer. Now, the process has reduced her to a four-digit number. But we are not done. When the number comes to the law school, someone in the admissions office will go to a large chart on the wall. It has a lot of axes on it, and at the proper location, given Alicia's number; the admissions official will put a dot. Alicia Aardvark is now a dot on the "Great Chart" on the admissions office wall.

Sometime early in the spring, in what might be called a crypto-

religious "rite of spring," the admissions officers will go to the "Great Chart" on the wall. They will draw two parallel lines. If Alicia, or I should say, her dot, appears above the upper line, she will be admitted. If her dot appears below the lower line, she will be rejected. If her dot appears between the lines, something unusual will happen because the school will have to differentiate the dots that fall between the two lines. Someone actually will have to look at Alicia's file. She will not be interviewed, however. Law schools don't interview applicants anymore.

In any event, no matter where Alicia's dot falls, she will receive a letter from the law school. The letter will say, "welcome, you are admitted" or "sorry, we do not have a place for you," or maybe it will say, "no decision yet, just hang in there, baby." Every one of those letters, of course, is machine produced. That is decision-making 2008 style.

The final concern of people stems from the obvious question of the degree to which massive data collection, particularly by the government, represents a threat to our civil liberties. This is not a new phenomenon. Most of you know about the Vietnam War and sadly recall that there was a lot of agitation in the country about various aspects of that war, including many public—and not so peaceful—demonstrations about it. What some of you may not remember is that the United States Army, totally without authority, developed a massive data bank called CONUS (Continental United States) on Americans who were thought to be a threat to the war effort.[28]

Who are they? Anyone who raised his or her voice disagreeing with American policy during that period ended up in the CONUS database as a potential danger to national security. When the existence of the database finally was revealed, there were a million Americans recorded in the system—a million Americans who's supposed "evildoing" may have been writing a letter to a newspaper, signing a petition, or attending a demonstration.

I was in that system. The University of Michigan, where I was then teaching at the law school, erupted over a HUAC (House Un-American Activities Committee) subpoena that the school foolishly responded to ahead of the required return date and did so without notifying the students whose names were on the membership lists of

28. *See Spying on Civilians*, TIME, Mar. 9, 1970, http://www.time.com/time/magazine/article/0,9171,878770,00.html.

the organizations identified in the HUAC request.[29] So three of us on the law school faculty went out to the crowd of college students that had taken over one of the university's buildings. We had this simple-minded idea of conducting an open-air seminar on the powers of the House Un-American Activities Committee, the value of free speech, and the legalities of subpoenas. We all were covertly photographed and our pictures ended up in the Ann Arbor police department's rogue gallery and ultimately in the Army's intelligence system. Our desire to educate, apparently, was thought to be a threat to the war effort.

That was over forty years ago. How much have we learned? For Vietnam, read Iraq or the War on Terror. For the Army, read the National Security Agency, or the FBI, or the Department of Homeland Security. For the 1970s covert open-air surveillance techniques, read today's monitoring of telephone calls and computer files (data mining). I submit we haven't learned a darned thing. But now, our activities have the imprimatur of the PATRIOT Act,[30] hastily enacted after 9/11. Now, various invasive practices by the government have been legitimized by Congress. We'll have to wait to see what the courts have to say about some aspects of that statute. To date, the picture has been mixed. For the time being at least, the balance between privacy and data surveillance has tipped dramatically in favor of the latter.

We do have to face the reality that, as a result of the Act, the government can explore the massive amount of data gathered about us simply because we are alive and active, any time it wants, using what appear to be lower than Fourth Amendment standards. The government may proceed in a way that, in effect, goes almost unsupervised unless there is a whistle-blower. In a real sense, no one is watching the watchers. Despite the realistic possibility of overzealous or excessive behavior, lawsuits challenging governmental conduct face an uncertain result, especially in the absence of a heroic judge.

---

29. *See* M. J. HEALE, MCCARTHY'S AMERICANS: RED SCARE POLITICS IN STATE AND NATION, 1935-1965 (1998) (explaining that Michigan was on top of the list for anti-communist tactics and that the state's university system became and remained the primary target).

30. The USA PATRIOT Act was signed into law by President George W. Bush on October 26, 2001. It authorizes the government in certain circumstances to intercept electronic communications and to obtain in secret private records on individual citizen. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

In my mind, this is a subject of enormous seriousness. If a person knows—or thinks—he or she is under informational surveillance, that individual may well change his or his behavior. She may not do it consciously. A person may do it subconsciously.

For example, during the Vietnam War, when the FBI descended on Boston ostensibly to determine how the Beacon Press got the Pentagon Papers,[31] which it published as a soft back book, it was a charade because the government already knew how the Beacon Press had gotten them. The FBI knew the papers had been given to the press by then Senator Mike Gravel of Alaska. But the FBI sent an overt surveillance team into the Boston area, people in trench coats and crew cut hair.

Because the Beacon Press was owned at the time by the Unitarian Universalist Church,[32] the agents began appearing at Unitarian churches. What happened is not a surprise; church attendance declined and donations dried up—except for those given in cash. Simply put, the effect of the agents' activities was behavior modification. This was a form of manipulating the conduct of citizens by the government, and of course, it can be accomplished in the name of whatever policy objective seems fashionable.

Probably all of you have read Orwell's *Nineteen Eighty-Four*[33] or seen the movie. And all of us certainly have heard of the image of "Big Brother." But do you know what the true message is of *Nineteen Eighty-Four*? It is that it does not matter if there really is a Big Brother on a screen watching us. It does not matter in the slightest. The only thing that matters is that people think there is a Big Brother watching them. Because if people *think* there is a Big Brother, they will, at some level of consciousness or subconsciousness, feel

---

31. Officially titled United States-Vietnam Relations, 1945-1967: A Study Prepared by the Department of Defense, but widely known as the *Pentagon Papers*, the study was commissioned by Robert McNamara and divulged the government's misrepresentation of the facts surrounding success in the Vietnam War. A Department of Defense employee, Daniel Ellsberg, leaked portions of the papers to the *N.Y. Times* who forthwith published excerpts. President Nixon tried to ban the *N.Y. Times*; however, the U.S. Supreme Court ruled that the President did not have the right to stop the publication. *See* N.Y. Times Co. v. United States, 403 U.S. 713 (1971). The trial court's memorandum is also a telling and interesting read. *See* United States v. N.Y. Times Co., 328 F. Supp. 324 (D.C.N.Y. 1971).

32. *See* William G. Sinkford, *Our Calling, From the President: In an Age of Terror, A New Call for Civic Courage*, THE MAGAZINE OF THE UNIVERSALIST ASSOCIATION, Jan/Feb 2003, http://www.uuworld.org/2003/01/calling.html (observing the role of the Unitarian Universalist Church and Beacon Press in the publication of the *Pentagon Papers*).

33. GEORGE ORWELL, NINETEEN EIGHTY-FOUR: A NOVEL (1949).

constrained by the "presence" of Big Brother and will modify their behavior to be pleasing in Big Brother's eyes.

Can you think of anything more inconsistent with some of the most fundamental rights we enjoy as free people—free speech, free thought, free association, free will? Not surprisingly, therefore, a lot of people are concerned about the implications for our civil liberties of today's massive data collection, especially after 9/11 and the enactment of the PATRIOT Act. These concerns relate particularly to our privacy.

I once had a student by the name of Eliot Spitzer.[34] Some of you may recognize that reference to the former governor of New York. Eliot is an unbelievably smart and talented guy in many respects. It is clear to me—looking with hindsight at what we know about the debacle that led to his resignation—that Eliot understood that when he withdrew sums of money he had to keep them below a certain amount to avoid the transaction being reported to the government. He was quite cautious in that category because he was withdrawing just under $5,000. In theory, he could have withdrawn up to $10,000 without attracting that much attention. But maybe he was simply out of date on the subject.

What Eliot did not understand was—this is supposition to be sure—that the PATRIOT Act also requires banks to file what are called "suspicious activity reports"[35] with the government. That principle covers patterns of cash transactions. So his bank, irrespective of any notion of privacy and fiduciary obligations to customers, reported his withdrawals—the rest, sadly, is history. Banks, among other entities, in a real sense, have become part of today's surveillance apparatus. That is the world in which we live.

Being an old fogey and a pessimist by nature, there are days on which I am ready to throw in the towel in terms of preserving privacy. Unless Peter Winn[36] can convince me there is hope for privacy in the future, I fear we may be witnessing an extraordinary demographic shift in terms of our commitment to privacy as an accepted social value.

Consider what so many of our young people do. In great

---

34. Eliot Spitzer became governor of New York in 2007, but resigned in 2008 after it was discovered that he had spent substantial sums on prostitute. Danny Hakim & William K. Rashbaum, *Spitzer Is Linked to Prostitution Ring*, N.Y. TIMES, Mar. 10, 2008, *available at* http://www.nytimes.com/2008/03/10/nyregion/10cnd-spitzer.html.

35. USA PATRIOT Act, *supra* note 30.

36. Peter A. Winn, *supra* note 3.

numbers they flock to YouTube[37] and Facebook.[38] For whatever reason, our young people are now happy—indeed, apparently eager—to give up their personal data. Privacy has already been an issue for Facebook. To its credit, it has taken steps to quell various concerns by upgrading the electable privacy settings and creating the individual's ability to request that an account be deleted permanently.[39] But, submerged in Facebook's terms of service it explicitly states "[b]y posting Member Content to any part of the Web site, you automatically grant . . . to Facebook an irrevocable, perpetual, non-exclusive, transferable, fully paid, worldwide license (with the right to sublicense) to use, copy, perform, display, reformat, translate, excerpt (in whole or in part) and distribute such information and content . . ."[40] This globally inclusive clause allows Facebook to negate completely any of your privacy objectives regardless of your settings, since the company has granted itself ownership of the material.

Thus, we appear to be raising a nation of young people willing to give up their right to privacy before they even comprehend the value of it. The sad thing about that is they have absolutely no cognition of the potential implication of what they are doing that might affect their lives five, ten, fifteen, twenty years down the line. That is why we call them young people, I suppose.

What we may be seeing is a gradual movement toward the metaphorical image of our living our lives in a fish bowl—a world in which everything about us is transparent and visible to everyone else. In other words, a world 180 degrees opposed to everything I said earlier about the value and importance of privacy. If that is true, we may have to begin educating our children about the consequences and potential of what life in an informational fish bowl world may be like.

So, what should we do if we want to protect privacy? Let me close by offering five simple but I think important thoughts. Forgive me, I am a lawyer; I try to organize everything. First, I think the law—or morality, or religion, wherever your source of values may be centered—must recognize that anyone who handles personal data about other people—whether it is in a hospital, a governmental agency, a business entity, or this law school—everyone with access to

37. YouTube, http://www.youtube.com/.

38. Facebook, http://www.facebook.com/.

39. Reuters, *Facebook Plans New Privacy Controls*, N.Y. TIMES, Mar. 19, 2008, *available at* http://www.nytimes.com/2008/03/19/technology/19facebook.html.

40. This version of the privacy policy has been replaced. *See* Facebook's Privacy Policy, http://www.facebook.com/policy.php (last visited May 30, 2009).

personal data about other human beings, which means most of the people in this audience I suspect, owes those individuals a fiduciary obligation of due care. Care in terms of what you collect, what you retain, how you provide and deny access to it, and the security measures you employ to safeguard it.

When you drive a car, you know you have a duty of care to the cars around you and to the pedestrians in front of you. After all, you can inflict grievous harm on others if you do not exercise that care. The personal information held by your institution—and remember, institutions don't control the information in their computer systems; the people in the institutions control it—similarly can inflict harm. And unless we start recognizing meaningful obligations on the part of data handlers, bad things will happen, and simple equity says that those at fault must be held accountable.

Numerous examples of bad data-handling practices have appeared. For instance, Jet Blue has been known to release passenger information for marketing purposes in direct violation of the privacy pledge on its Web site.[41] Unfortunately, a lawsuit against the company failed because the language of the relevant statutes was ill-suited to the technological situation.[42] Telephone companies have been known to provide subscriber data to governmental agencies without proper pre-authorization.[43] Sloppy data handlers in Florida have "lost"—there's a euphemism for you—discs containing medical files of thousands of Floridians who are HIV infected.[44] CVS Pharmacy has been the subject of litigation in Massachusetts because they released personal prescription information to drug manufacturers.[45] Companies insert cookies into users' computers to

---

41. See *In re* Jetblue Airways Corp. Privacy Litigation, 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

42. *Id.* at 303 (dismissing based on the grounds that "plaintiffs have failed to state a federal cause of action under the ECPA, that plaintiffs' state law claims are federally preempted, and that plaintiffs have failed to state any claim under state law").

43. Scott Shane, *Agency and Bush Are Sued Over Domestic Surveillance*, N.Y. TIMES (Sept. 18, 2008), *available at* http://www.nytimes.com/2008/09/19/washington/19nsa.html; Scott Shane, *Attention in N.S.A. Debate Turns to Telecom Industry*, N.Y. TIMES, Feb. 11, 2006, http://www.nytimes.com/2006/02/11/politics/11nexus.html.

44. Lynda Richardson, *Taking Names: A special report; New Jersey's H.I.V. List: Valuable, and Still Secret,* N.Y. TIMES, May. 29, 1998, http://www.nytimes.com/1998/05/29/nyregion/taking-names-a-special-report-new-jersey-s-hiv-list-valuable-and-still-secret.html?scp=1&sq=Florida%20HIV%20disc&st=cse ("Advocates point to a widely publicized case in Florida, in which a public health worker lost his job over a computer disk listing the names of people with AIDS that was not kept secure. The disk was mailed to two newspapers along with an anonymous letter.").

45. Kelley v. CVS Pharmacy, Inc., No. 98-0897-BLS2, 2007 WL 2781163 (Mass.

track their movements on the web, particularly their interests and buying habits.[46] These are not merely anecdotal situations. Misadventures with the handling of personal information happen over and over and over again. A level of accountability must be constructed, especially if Mr. Obama's health plan succeeds in securing the computerization of all medical records within the next five years.[47] One can only hope that there will be sufficient focus on how to maintain the privacy and security of these records, especially those of a highly sensitive personal nature.

Second, we have to be much more careful about what information people and institutions collect and preserve. Longitudinal researchers naturally want to collect everything they can about people over time. But society has decided certain data categories are off limits. Today, for example, we do not collect information about race, we do not collect individualized data about religion, and we do not collect information about marriage status or sexual persuasion. I think we have to make decisions about expanding those categories to cover subjects that are potentially more dangerous to individuals in the present information environment, given today's world of search engines and social networking sites.

Third, we are graced with an enormous experience base in data security—technological security, human security, and educational security. Now we must apply it. We must make sure data handlers of every description use state of the art security methodologies. Of course, there is no such thing as a fail-safe security system. There never has been a lock without a key. What we are talking about is developing and employing systems and procedures that increase the odds against a security breach. Certainly, we are always going to have some breaches. But we can reduce the number of times we have a problem. Indeed, standard tort doctrine relating to duty can be invoked to assure implementation.

Fourth, the reality is that with a few hundred bucks I can probably get more information about any of you than you may even

---

Super. 2007); Weld v. CVS Pharmacy, Inc., No. CIV. A. 98-0897F, 1999 WL 494114 (Mass. Super. 1999).

46. Cookies are parcels of text, often sent by a server to an internet user's browser, to record information about the user's web browsing and buying habits. The information is recorded on the cookie and then shared with the server or other websites. *See, e.g.*, Information About Cookies on Microsoft.com, http://www.microsoft.com/info/cookies.mspx (last visited May 30, 2009).

47. *See* Barack Obama Heath Care Plan, http://www.barackobama.com/pdf/issues/HealthCareFullPlan.pdf (last visited Nov. 4, 2008).

know exists. All you need is the right connections in the subterranean intelligence world—filled with former security people, ex-military, ex-intelligence services, ex-law enforcement from the domestic and international communities. There is a universe of those people out there. But curiously, I cannot get information about the one person that I have a unique interest in. And that reflects a norm. I typically cannot get information about myself. I can see what Wikipedia has about me and what shows up on Google, but that doesn't get me very far compared to what might be circulating in the subterranean information world.

We have not yet really recognized what is, I believe, analogous to a due process right—my right to see and confront the files on me. The Freedom of Information Act[48] unfortunately is of very little utility in this context. Its exemptions from citizen access in favor of law enforcement and security agencies prevent an individual from seeing much of his or her files because of assertions that national security or the needs of crime fighting is at stake. I have my doubts about these claims. Similarly, the medical profession, among others, worries about your committing suicide if you see your medical files. Nonsense, I suspect. These forms of resistance and stonewalling have to stop.

Think about it. No institution has a vested interest in inaccurate data about anyone. And clearly, I am the best person to make sure the data about me is accurate and I have an incentive to do so. Why don't I have a right of confrontation that lets me see my files plus receive notice of their existence and an opportunity to correct them? These are principles taught to first-year law students. The Fair Credit Reporting Act,[49] which I worked on way back when it was being proposed, is a good illustration of putting the principle into operation.

Finally, there is a wonderful analogy in my perverse mind between the human life cycle and information. We are born; so is information when it is generated and recorded. We grow up, as we develop height, weight, muscle, and bone; information grows up as more and more data is aggregated with the initial data, and the file becomes more meaningful and content rich. We get married; so does data. Files electronically join together in holy assemblage as databases combine. We have children; so does information. The merged files spin off little files; the offspring start romping around independently, and then leave home. Where do they go? Often we

48. 5 U.S.C.A. § 552 (2006).
49. 15 U.S.C.A. § 1681 (2006).

don't know. Sadly, in great numbers, we get divorced; so does information. Files split; they divide; i.e., they break up. They become incompatible and go their separate ways. We get old and less agile or functional; so does information. It ages and becomes less relevant, often becoming dangerously misleading or downright inaccurate.

At this point, the analogy breaks down, because we die; information does not. It simply ages but remains in the system. I have come to believe that data collectors are genetically anal retentive with little incentive to purge their files. We have to develop mechanisms that expunge information as it ages and reduces in significance and its potential for damage exceeds the value of its content. In short, we must extend the analogy and bring death to stale data. I find this analogy between data and the human life cycle delightful.

A final thought on this last point. We are all aware that in civil litigation today, the parties can engage in e-discovery.[50] There is a frightening resource consumption reality to this. And the only way the system can deal with the current hysteria about e-discovery—which can be conducted on a scale that is almost beyond comprehension and must be contained—is to develop purging techniques for data systems, particularly those in the business community. This is an aspect of computer science and procedural readjustment that is in development. Not surprisingly, there is now an entire industry that is making a good deal of money assisting entities to establish rational data retention and data destruction policies. These policies are motivated, in part, to retain the data that is needed for compliance with various legal regulations and potential litigation. Conversely, the policies are designed to identify that which need not be retained, which the organization might as well dispose of because it represents a potential e-discovery burden, and therefore potentially an enormous economic litigation cost and a risk that its content might prove damaging.

To conclude, I surprise myself that after forty years of involvement with the subject of privacy, I still feel strongly about the topic. I guess that's the mark of being an old fogey, right? After all these years, I continue to be reminded of the passage by the great

---

50. E-discovery, or electronic discovery, is the process by which parties in a lawsuit exchange documents that exist in electronic form. Amendments to the Federal Rules of Civil Procedure now compel litigants to preserve and produce electronic file. *See* FED. R. CIV. P. 16, 26(a), 26(f).

French sociologist, Jacques Ellul.[51] Paraphrasing a thought he once expressed: If it turns out to be a dictatorship of databanks and dossiers rather than of hobnailed boots, that will make it nonetheless a dictatorship.

I hope you enjoy the day, this conference, and the beauty of Charleston.

51. Jacques Ellul (Jan. 6, 1912—May 19, 1994), a French philosopher, sociologist, and theologian, authored some forty books and hundreds of articles over his lifetime and was a professor at the University of Bordeaux. The paraphrased quote is from a book authored by Ellul, and reads "That it is to be a dictatorship of test tubes rather than of hobnailed boots will not make it any less a dictatorship." JACQUES ELLUL, THE TECHNOLOGICAL SOCIETY 434 (1964).