RESTORING A PUBLIC INTEREST VISION OF LAW IN THE AGE OF THE INTERNET

MARC ROTENBERG[1]

ABSTRACT

In November 2003, Mr. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, lectured at Duke Law School on the importance of protecting individual privacy. In his remarks, Mr. Rotenberg recounted the successful campaign against the government's Clipper Chip proposal. He argued that successful public interest advocacy in the Internet age requires the participation of experts from many fields, public engagement, and a willingness to avoid a simple "balancing" analysis. He further concluded that privacy may be one of the defining issues of a free society in the twenty-first century.

INTRODUCTION

¶1 On November 10, 2003, Mr. Marc Rotenberg, Executive Director of the Electronic Privacy Information Center (EPIC),[2] lectured at Duke University School of Law as part of the Information Ecology lecture series sponsored by the Center for the Study of the Public Domain.[3] In his lecture, Mr. Rotenberg spoke on the importance of individual privacy in the Internet Age, and specifically discussed the "Clipper Chip" proposal, the "Carnivore" network surveillance scheme, the Total Information Awareness Program, and the USA PATRIOT Act. In addition, Mr. Rotenberg discussed techniques for establishing effective technology policy, First Amendment privacy concerns, and alternative approaches to privacy protection. In concluding his lecture, Mr. Rotenberg postulated that privacy

---

[1] Mr. Rotenberg is a graduate of Harvard College and Stanford Law School. He has served as Counsel to Senator Patrick J. Leahy on the Senate Judiciary Committee and currently teaches information privacy law at Georgetown University Law Center. He chairs the ABA Committee on Privacy and Information Protection and is Secretary of the Public Interest Registry. He is editor of *The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments* (2003), co-editor (with Philip E. Agre) of *Technology and Privacy: The New Landscape* (1998), and co-editor (with Daniel J. Solove) of *Information Privacy Law* (2003).

[2] Electronic Privacy Information Center, http://www.epic.org (last visited Mar. 13, 2004).

[3] Center for the Study of the Public Domain, http://www.law.duke.edu/cspd/index.html (last visited Mar. 13, 2004).

may be one of the defining issues of a free society in the twenty-first century.

¶2 This iBrief is an edited transcript of Mr. Rotenberg's lecture.[4]

I. THE CLIPPER CHIP

¶3 I'm going to start my talk with you tonight by telling you a story about something that happened almost ten years ago. It concerned a proposal for a new encryption standard for the United States, called the "Clipper Chip."[5] In the early 1990s, computer firms were beginning to realize that they needed to provide some security for people who were beginning to transact on a more regular basis on the Internet. People were sending electronic mail; they were engaging in financial transactions; there was a lot of talk about the emergence of electronic commerce. The World Wide Web, as we know it today, in fact, had not yet come into existence. Mosaic,[6] I think, was introduced in the fall of 1993. But there was a lot of interest in cryptography, and there was also a lot of concern. There was concern being expressed by the United States government, by the law enforcement community, and the Department of Defense, that this new technology of privacy could enable secretive criminal activities that would threaten public safety.

¶4 Now, to set out their argument, for just a moment, they would say, "If two people wish to conspire in a criminal act, they could do so now in this digital world by encoding their messages so that no third party would have access to the content of their communications." And this, they said, was completely in opposition to how the government had traditionally been able, by means of wiretap and electronic surveillance—with court supervision, in the context of a criminal investigation—to intercept communications and obtain evidence of criminal wrongdoing. And because of this concern, they argued that the widespread unrestricted use of encryption technology posed a threat to public safety and national security. And they proposed technical standards—not subject to the lawmaking

---

[4] A complete recording of Mr. Rotenberg's lecture is available at http://www.law.duke.edu/webcast/webcastsArchive.html (last visited Mar. 13, 2004).

[5] *See, e.g.*, Edmund L. Andrews, *U.S. Plans to Push Giving F.B.I. Access in Computer Codes*, N.Y. TIMES, Feb. 5, 1994, at A1 (discusses the Clinton Administration's attempt to encourage Clipper Chip technology in telecommunications devices).

[6] Mosaic was the first widely-available web browser, written by Marc Andreessen at the National Center for Supercomputing Applications at the University of Illinois and released in February 1993. Robert Cailliau & Dan Connolly, *A Little History of the World Wide Web from 1945 to 1995*, *at* http://www.w3.org/History.html (last visited Nov. 24, 2002).

process, to public debate, or to agency rulemaking—that would ensure the government access to private communication by an approach that was known as Escrowed Key Encryption.[7] What it would have required was that every time someone tried to digitally lock their electronic message, their business plan, or their financial information a copy of that private key would be made available to a government agency, and, if necessary, obtained in the course of a criminal investigation to give access to that private communication. That was the Escrowed Encryption proposal.

¶5 At the time that it was announced, I was doing work with a group of computer scientists and technology experts on a range of privacy issues and I began to discuss with them their views about the impact of such a technical standard. Now, understand the significance of this proposal. This is not an investigative technique applied to a suspect in the context of a particular investigation. This is a technical standard that becomes the cornerstone for all security architecture in the United States and most likely around the world, going forward from that point in time. And as I spoke to technical experts such as Ron Rivest (the R of RSA), Whitfield Diffie (the Diffie of the Diffie-Hellman public key cryptography standard) and others—these are famous cryptographers,[8] by the way, and sort of rock stars in their own right (I have to do that translation so you understand the significance)—they said this was a really bad idea.

¶6 This is a really bad idea. Not only because it is an enormous assault on privacy—it basically treats every individual as a potential criminal suspect—but it also creates a new security flaw that would not otherwise exist. How do we know the circumstances under which someone might obtain access to that escrowed key? In the best of circumstances—in the ideal circumstances—it will be through court order, subject to judicial oversight with appropriate public reporting which we would hope would be preserved if at some future time there might be an actual terrorist event in the United States threatening national security that somehow could change those legal safeguards. Those were the ideal circumstances for the use of escrowed-key encryption in the early 1990s.

¶7 We put together a letter that was signed by forty-two experts in law and technology and public policy, politely addressed to President Clinton urging him to withdraw the Clipper encryption scheme and we posted the

---

[7] *See, e.g.*, John Markoff, *Flaw Discovered in Federal Plan for Wiretapping*, N.Y. TIMES, June 2, 1994, at A1 (discusses the Clipper Chip as an escrowed encryption system).

[8] *See, e.g.*, SSH Communications Security, *Cryptography A-Z: Public Key Cryptosystems*, *at* http://www.ssh.com/support/cryptography/algorithms/asymmetric.html (last visited Mar. 25, 2004) (outlines and describes both the RSA and Diffie-Hellman encryption protocols).

letter on the Internet. And then something extraordinary happened. People began to send email to me when they saw the letter that said, "You've made a lot of good points here. I didn't really understand what this encryption proposal was about, but I see what you're saying. Would you add me please to your letter?" We said okay, and then we got a few more email messages asking to be added to our letter to the President. Over the course of six weeks in 1994, we received more than 50,000 email messages from individuals asking to be added to the letter. And I have to add by the way, for some of you newcomers, that 50,000 people on the Internet back in 1994, that was a big number. Now, it's like an AOL chatroom or an REM mailing list or something. I appreciate now it does not seem like much, but ten years ago it was a lot. And we had in effect created the first online petition—the first Internet petition around the Clipper encryption scheme—and we printed this out, consuming as much paper as we possibly could to add heft to our document, and delivered it to the White House. That petition, combined with a lot of other factors, including industry opposition and a lot of skepticism among European governments about whether this would serve their national security interests, led to a decision by the administration to withdraw the Clipper encryption scheme. And it was an extraordinary moment, I think, in the history of the Internet.

¶8 Now, I don't want to spend so much time gloating over that petition. What I really want to tell you about is what I learned from the experience and what lessons it might suggest today for some of the challenges that we face in this era of the Patriot Act,[9] of Total Information Awareness,[10] and an ongoing question in this country about how to safeguard civil liberties and freedom even as we strive to protect the country against future terrorist acts.

II. LESSONS IN TECHNOLOGY POLICY

¶9 Here are a few of the things I learned. The first thing I learned is that these issues are hard, and you need help to understand them. You need people from different disciplines and different expertise to come together and have discussions about what the implications are of these proposals going forward. To have cryptographers involved in this discussion was enormously important for us to be able to assess the impact of the Escrowed Encryption scheme. But we needed legal experts as well. We had to be able to understand how well the federal wiretap law would operate in this new electronic environment where information was already provided to a

---

[9] The term "Patriot Act" refers to the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[10] *See, e.g.*, John Markoff & John Schwartz, *Many Tools of Big Brother Are Now, Up and Running*, N.Y.TIMES, Dec. 23, 2002, at C1 (discusses the scope of the Total Information Awareness project).

government agency that might have otherwise required a warrant at the outset, before it could be obtained. And we needed people who had an understanding from a comparative law approach—how what the U.S. was proposing to do compared with what Europe was doing or with what Asian governments might be doing. All of these perspectives, I would argue, increasingly come together as we try to understand the impact of technology on law and civil liberties broadly.

¶10 I would also say that we needed to involve a process of public engagement. There were in the early 1990s probably only a handful of people in Washington who understood the significance of cryptography policy for a world of network computers, electronic commerce, or the rapid adoption of electronic mail. There may have been more up at Fort Mead,[11] but that's technically not within Washington, D.C. It was very important for our efforts to be able to engage the public and to reach people on an issue that, at the outset to many, seemed arcane, seemed abstract, seemed unrelated to the policy process of Washington and Congressional hearings and the talk shows and so forth. It was precisely because this debate was taking place at the outskirts that the need to engage the public was all the more critical.

¶11 A third point from our early experience with the Clipper Chip, which I think many people in the IP community have come to realize in the last few years, is that technology is a very powerful way of creating policy. It is a very powerful way of making law. Now, Larry Lessig probably said this most famously in his book *Code and Other Laws of Cyberspace*,[12] where he argued that by code we create coercive powers much like law creates coercive powers, but when I wrote *What Larry Doesn't Get*,[13] my article a couple of years ago for the *Stanford Technology Law Review*, the observation I was making was that in fact this wasn't new. This was something that many of us in the privacy community had come to understand in the early 1990s, when we were confronting a proposal put forward by the federal government of enormous impact that would never be debated in Congress, that would never be the subject of an up or down vote, that no one could write to their elected representative and say, in effect, "Please vote this way or please vote that way on this matter." Increasingly in this realm, technology plays an extraordinarily important role in shaping the structure of this new electronic environment.

---

[11] Fort Mead, Maryland is home to the National Security Agency.

[12] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[13] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1 (2001),

¶12 We found ourselves also being asked to reconcile competing interests. Now, Duke Law School Professor Jamie Boyle[14] is going to hear from me something that I often say, and I'm sorry for repeating this, but it's something I feel very strongly about and am generally pleased that over EPIC's ten years of existence we have tried very hard to avoid using the phrase, "We need to balance competing interests." Now, the concept of balance is very inviting in the policy world. In my office, I sit and I watch C-SPAN all day long. Okay, that may explain some things about me, but I'm not going to go there tonight. And I have noticed that when members of Congress really don't know much about an issue, they will come to the floor of the House or come to the floor of the Senate and they will drop their voices an octave or so and say, "We need to balance these two competing interests," as if there is some great wisdom in recognizing that often times in the policy process there are competing interests. To say that you need to balance them, I would argue, really tells you very little about outcomes. I was actually counting yesterday when former Vice President Al Gore spoke in Constitution Hall in Washington on freedom and security after September 11th. He gave a great speech, by the way, but I was actually counting the number of times that he used the word "balance" and he used it only once, and in passing, and it was probably the fewest uses of that word in a speech on freedom and security after September 11th from any politician that I've heard recently.

¶13 When we confronted the issue of privacy in the context of the Clipper encryption scheme, we could not say that we needed to balance privacy and security. Both interests are substantial, and we needed a proposal or a response that recognized that both interests needed to be protected in this online environment. And we found ourselves, after Clipper, often times in discussions where people said, "Well, privacy is important but so is the First Amendment;" "Privacy is important but so is open government;" "Privacy is important but so is this other thing." And on many of these issues we came to realize that if you look closely there may be a way to pursue both interests simultaneously. In other words, in my view, the best resolution of many of these difficult policy challenges is not to conceive of a zero sum arrangement that asks us to give up on the one hand what we gain on the other but rather solutions that seek to preserve both interests.

III. ANONYMITY, PRIVACY, AND THE FIRST AMENDMENT

¶14 I'll just jump ahead a little bit and tell you that one of the things I came to realize very quickly about trying to reconcile competing privacy

---

[14] *See* Duke University School of Law, *Faculty Profile: James Boyle*, *at* http://www.law.duke.edu/fac/boyle/ (last visited Mar. 30, 2004).

and First Amendment claims is the very important role that anonymity plays, both in law and in technology. I became fascinated with a series of Supreme Court cases going back to 1960, the first of which was *Talley v. California*,[15] where the Court considered the question of whether the State could compel a person to disclose their identity on a hand-bill that they would circulate. There are lots of arguments for this law. I mean you could say that a person may engage in defamatory conduct and certainly you want to be able to identify the author of a defamatory work. But, significantly, in the three cases since 1960 in which the Supreme Court has addressed this question,[16] each time it has struck down statutes that compel individuals to disclose their identity.

¶15 Now, let's think about this for a moment. These are people engaging in speech acts in the public realm who are simultaneously seeking to protect their privacy. The core privacy interest must surely be the ability to withhold disclosure of identity. When the Court granted cert a couple of years ago in a case called *Watchtower Bible v. Village of Stratton*,[17] the question was whether the city of Stratton could require individuals who were going door to door—and they had in mind Jehovah's Witnesses knocking on private homes—to first obtain a permit from the mayor of the city before knocking on the door of a private residence. I saw that case going up to the Court and I said, "We are going to get involved in that—that's a very important privacy case." And people said to me, "That's a great thing, you know. I don't like those people knocking on our doors. I think you should get behind them." And I said, "That's so twentieth century."

¶16 I said, "Privacy, you have to understand, is about controlling disclosure of identity. It's about enabling participation in political life and expressing your views. We are going to side with the Jehovah's Witnesses." And I can tell you we wrote a pretty good amicus in that case, and I can tell you a story about the oral argument. It was a great oral argument. Justice O'Connor asked the attorney for the village of Stratton at one point about how this system operated. And she said to the attorney for the Village, "So if I understand this correctly, to go door to door for any cause"—which was the language in the ordinance—"I would need to first obtain the mayor's permission. Is that correct, counsel?" And the attorney for the Village of Stratton said "Yes, your honor, that is correct." And Justice O'Connor paused and said "What if I think we need a new mayor?" Right. You get it?

---

[15] 362 U.S. 60 (1960).
[16] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); Buckley v. American Constitutional Law Foundation, 525 U.S. 182 (1999); Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150 (2002).
[17] 536 U.S. 150 (2002).

¶17 This really is an illustration, I think, of the point that sometimes in the policy process when we face competing interests to simply assume, "Well, if we are going to engage in First Amendment activities you need to sacrifice some privacy." Often times that's not correct. And perhaps even more significantly the courts have recognized this. The courts recognized this, for example, in the 1958 case of *NAACP v. Alabama*,[18] where the State of Alabama was trying to obtain the membership lists of the organization, which they viewed as a foreign corporation. And rather than simply requiring the officers of the corporation to register with the State Secretary, they said, "We want all the members' names." Well, imagine the impact that might have on organizations that may be unpopular or controversial that are trying to organize on important and emerging political issues. Privacy in many circumstances comes to the aid of other critical values such as the First Amendment and political participation.

¶18 I want to talk about another theme that I've picked up over the years working in this field and that is the relationship between personal privacy and government secrecy. I get calls from the press, and they say, "Some organization is trying to get private memos from a federal agency disclosed to the public. Aren't you concerned about that?" And on one of these calls I actually said, "Well no. Actually, that was our organization that filed the Freedom of Information Act request to obtain the information from the government." But it is interesting how often people conflate privacy and secrecy. And they say while just as individuals have the right to engage in private communications, so too should government actors be able to engage in private communication. But in fact, U.S. law views those two relations very differently. I can take you back to 1974, which was the post-Watergate era of reform in the U.S. Congress. A lot of good legislation was passed by the Congress in 1974. Two bills were of particular significance for my organization. One was the Privacy Act,[19] which protected the privacy of personal information held by the federal government. The other was a series of strong amendments to the Freedom of Information Act,[20] which basically said that public records held by government agencies should be widely available to the public.

¶19 Now, you look at those two events, both taking place in 1974, and you think to yourself, "You know what's up; are these people schizophrenic?" You know, one day they're passing privacy laws, the next day they're passing open records laws. I mean, it's like one group of Congressmen vote the first day and they go home and talk to the

---

[18] 357 U.S. 449 (1958).

[19] 5 U.S.C. § 552a (2000), available at http://www.usdoj.gov/foia/privstat.htm (last visited Mar. 25, 2004)

[20] *See, e.g.*, Elias Clark, *Holding Government Accountable: The Amended Freedom of Information Act*, 84 YALE L.J. 741 (1975).

constituents, and then another group vote the next day. The point was in 1974, when Congress passed the Privacy Act and strengthened the Freedom of Information Act, they were saying that personal information is entitled to protection and should not be improperly disclosed. (I don't think they anticipated that 30 years later Linda Tripp would get a $600,000 judgment in a Privacy Act case. But even that could happen in protecting privacy rights under this legislative scheme.) But public information should, in fact, be widely available, and Congress made this clear as well. And so we have also pursued, through EPIC Freedom of Information Act requests, where we have sought the disclosure of many types of records held by the government agencies. We obtain the information concerning—this is a great name, by the way—an Internet surveillance scheme called "Carnivore." Now, they reassured us after these records were disclosed, when the program was explained, that it could have been worse. They had another program in mind called "Omnivore." But Omnivore, you see, was not sufficiently focused as a wiretapping technique. They wanted to assure us that only the information properly being sought under the warrant would be obtained. Hence, "Carnivore."

¶20 There's this whole name change thing happening, by the way, around a lot of these issues that's really interesting. John Poindexter announced the Total Information Awareness Program, which was pretty Orwellian, and then he had a website that had the Latin phrase, "information is power," and then a weird Masonic temple with an eye on top. I don't think this is the way to assure people that you're not about some Big Brother operation. They also decided to change the name for that program. They went from "Total Information Awareness" to "Terrorism Information Awareness."

¶21 Now, none of the functional capability was changed, but we were so gladdened by the good news we actually put an item on our website that led, "Name Changed, Problem Solved," right? Because, hey, there was no more "Total Information Awareness." One other comment on this whole name thing: we were doing Freedom of Information Act requests surrounding the FBI's legislative proposal to require communications service providers to ensure that their products could be wiretapped. This was the telephone corollary of the debate that was taking place around the encryption standard but for the traditional analog telephone network. And the law enforcement community expressed concern that with advances in the communication network and so forth that they couldn't even do the old-fashioned wiretap, so they wanted to ensure that services would ensure the functionality of wiretap capability. They had a legislative proposal called the "Communications Assistance for Law Enforcement Act."[21] We

[21] Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §§ 1001-1010 (1994).

obtained the documents for the original proposal, which had actually not surfaced in Washington before consideration and vote on the bill in 1994. The code name for this proposal—I'm not making this up—was "Operation: Root Canal." You get it?

IV. ALTERNATIVE APPROACHES TO PRIVACY PROTECTION

¶22 One of the other things we've tried to do in our work at EPIC is to think broadly about different approaches to emerging challenges in the legislative and regulatory realm, and by this what I have in mind is really a comparative approach. Privacy turns out to be a very exciting topic, in part, because so many countries today are wrestling with privacy issues.[22] India is considering legislation for private sector data practices. Argentina recently passed legislation. Japan is about to adopt legislation. There are questions in Eastern Europe relating to the adoption of data protection standards and whether they're fully compliant with the requirements of the EU Data Directive.[23] All around the world, different countries are struggling with the question of how best to protect privacy in this age of information and global commerce. We have used that as an opportunity to explore and compare all these different models. In some situations, for example, you might look to the European Data Directive standard and say, "It makes a lot of sense to have a comprehensive approach to privacy protection that also allows consumers in the marketplace, whether they have cable subscriber records or magazine subscription records, to be afforded a common standard for privacy protection in the information they provide to get that service." We don't take that approach in the U.S. In the U.S., which has followed more of a sectoral approach, we might say, for certain factors relating to the adopting of cable legislation in the early 1980s, "We'll provide privacy protection for cable subscriber records, but not for magazine subscription records." And so that's one kind of a comparison that gives you some insight into how different countries respond to emerging privacy challenges.

¶23 But in other areas, for example wiretapping in the United States, we actually have just about the toughest laws on wiretapping in the world. Not only in terms of the showing that government needs to make before it may engage in electronic surveillance, but also in the extensive reporting that's required any time electronic surveillance is undertaken by a U.S. federal agent. And at EPIC we track all that information. I can tell you, for

---

[22] See generally EPIC, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS (2002).

[23] Council Directive 95/46/EC, 1995 O.J. (L 281), 31, *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett (last visited Mar. 30, 2004).

example, how wiretapping activity in the United States in 2002 compared with 2001 or, for that matter, twenty years earlier. You can't do that with any other country. And that comes about in part because of a particular approach that the United States took toward the protection of privacy in the communications environment more than 30 years ago.

¶24 One of the reasons I think it's particularly important to value a comparative approach to these emerging policy issues is that these are real policy alternatives. Think about it this way: if you ask yourself the question, "What kind of privacy protection should we have for DRMs?" (Digital Rights Management)—several people asked me about that topic today—if you take a narrow, U.S.-centric approach to this, you might say, "Well, we've done basically nothing, but some people have written some interesting articles that maybe we should look at and consider in the development of some privacy policies for DRMs." I mean that's not much, unfortunately, of a policy discussion; it's very difficult through the legislative process to say, "There's an important approach that maybe you should consider." But if you were to say instead, "On DRM privacy, the European Commission is very interested in consumer safeguards, consumer privacy in this digital environment, and has recommended the adoption of a directive to try to safeguard privacy even as these new services go forward," suddenly you have a comparison. You can look at an approach in the United States; you can look at an approach in the European Union. Maybe there's a third approach from Japan, or maybe from Australia. You begin a policy process that enables debate and enables choice. It may be at the end of the day that the United States, through its Congress says, "Well, thank you very much for that, but we prefer our approach and that's the way we're going to go," and that could happen. But I'm at least hopeful that increasingly the U.S. courts and perhaps even the U.S. Congress will look abroad to new approaches to emerging policy issues. Many of you probably saw the opinion this summer in *Lawrence v. Texas*[24] by Justice Kennedy. I mean, it was a remarkable opinion—this was the decision striking down the Texas homosexual sodomy statute—it was a remarkable opinion, in part because of the outcome. It was also a remarkable opinion because Justice Kennedy cited to the European Convention on Human Rights,[25] and some of the Article 8 cases concerning the protection of privacy, which has opened the door a bit to what will be a very valuable process of enabling more comparison of different approaches to privacy protection. In my own field, in the privacy field, I think we've benefited greatly from the work of a

---

[24] 539 U.S. 558 (2003).

[25] Convention for the Protection of Human Rights and Fundamental Freedoms, *opened for signature* Nov. 4, 1950, *available at* http://conventions.coe.int/treaty/en/Treaties/Html/005.htm (last visited Mar. 25, 2004).

lot of scholars who have helped us understand how different countries responded to emerging challenges.[26]

V. THE PATRIOT ACT

¶25 That's an overview of EPIC, and I want to say a few words now about the challenges we face post September 11th under the Patriot Act, and then actually I'd welcome your questions and your comments, but I thought it would be helpful at the outset to tell you a bit about our approach to public interest litigation. It's been for us extraordinarily exciting. We find ourselves before Congressional committees, in courts, before agencies, basically every opportunity we have to pursue a discussion or debate or participate in a policy resolution of one the issues of concern to us, we will try to pursue. It's possibly for that reason that I can say to you today that we face no greater challenge than we face resulting from the horrific events of September 11th. I can say that in part, because I was in Washington on that day and also because the flights originated from Boston, which is where I grew up. But also after September 11th, there were subsequent developments with the anthrax scare that were almost as unsettling as what had happened on that day. I remember speaking on a panel in mid-October of 2001 at the National Press Club with the former Director of the CIA James Woolsey who had just published an editorial[27] that day in the Wall Street Journal arguing that the presence of aeriolized anthrax in the United States established Saddam's complicity in the events of September 11th. This was October 2001, and as many of you may be sensitive to, there are still a lot of questions to be answered about how decisions were reached regarding U.S. intervention in Iraq.

¶26 Now, I'm not going to have that conversation with you tonight, but I do want to convey to you what it was like in Washington in the fall of 2001, when the Patriot Act was being debated. After the—well, even before—the anthrax hit the city, two days after September 11th, September 13th, Utah Senator Orrin Hatch went to the floor of the Senate with a proposal (the Anti-Terrorism Act[28]) that had been put together by the Attorney General, and said that within a week, we must pass this legislation to ensure the safety of the American people against future terrorist acts. And it's a little too easy, I think, with the benefit of hindsight, not to appreciate how much people in Washington felt under attack at that point in

---

[26] *See, e.g.*, DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES (1989).

[27] James Woolsey, Editorial, *The Iraq Connection*, WALL. ST. J., October 28, 2001, at A26.

[28] S.A. 1562, 107th Cong. (2001) (submitted as an amendment to 107 H.R. 2500).

time, and the willingness to give the federal government whatever authority it felt that it needed to safeguard the country, I think was very genuine. Particularly for members of Congress who were thinking not only about themselves, but also about their families, and about their constituents.

¶27 I was very proud of the fact that the next day, my former boss, Senator Patrick Leahy from Vermont, went to the floor of the United States Senate and said, "Even with this great challenge that our country faces today, we must be equally resolute in ensuring the protection of basic civil liberties, because if today we sacrifice those freedoms, then surely the terrorists will have won." Well, of course, in the weeks that followed, that phrase became overused—"If we did not go shopping at Tyson's Corner, the terrorists would have won"—but when it was first spoken on the floor of the U.S. Senate, it was significant, because it was a signal on the part of some members of Congress that there would be at least some debate before the Patriot Act was adopted. Now, it's true that the Act went through in six weeks. It went through without a hearing. There was a significant shift that took place in the position of the House of the Representatives, where a fairly good bill that had been agreed to by the House Judiciary Committee[29] was taken off the table at the last moment, and the final bill as enacted substituted in its place. But there was at least an opportunity for some debate and discussion.

¶28 Nonetheless, the Patriot Act poses enormous challenges to the protection of privacy and civil liberties in this country. Many of the traditional safeguards that exist in the Fourth Amendment, and particularly for electronic surveillance, are intended to provide oversight and accountability when the government goes about the business of conducting investigations. Now, oversight and accountability are not forms of prohibition; they do not say, "You may not obtain access to this information;" "You may not speak to these witnesses;" "You may not enter these homes;" or "You may not go to those offices for relevant records." There's hardly anything in any privacy statute that does anything like that. Invariably what privacy laws try to do is construct a series of firewalls that say, "To get access to this information you need, generally speaking, to establish probable cause." There should be some judicial oversight so that the prosecutor is not acting on his own authority. There should be some notice at an appropriate moment in time to the target of the investigation. If you are entering a home, generally speaking, you should announce your presence. If you are conducting electronic surveillance, when the investigation is concluded, the target of the investigation has the right to know that they were the subject of a court ordered wire tap, and there

[29] Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act, H.R. 2975, 107th Cong. (2001).

should be public reporting so the public is aware of how the government is using these investigative authorities.

¶29 I told you just a few moments ago, that one of the great achievements of the United States in the privacy realm was the elaborate public reporting for the use of electronic surveillance. But one of the things that happened as a result of the Patriot Act was that a lot of the electronic surveillance was shifted from the traditional Title III report, which runs about a hundred and thirty pages, and is provided to the Administrative Office of the U.S. Courts and is available on the EPIC website, to the Foreign Intelligence Surveillance Act report, which is a one page letter from the Attorney General that summarizes in approximately three paragraphs how an extraordinary surveillance authority has been used by the Department of Justice during the past year.[30] What the Patriot Act did, in many separate areas, was to remove, reduce, and push to the outskirts these various safeguards that had been established in privacy laws going back more that thirty years. It reduced the accountability of government. It increased the secrecy of government, even as it diminished the privacy of the Americans who would become subject to this authority.

¶30 Now, it has been argued, of course, that in times of national crisis power tends to shift from the individual to the executive. During wartime perhaps we are used to the President assuming more power, and we have certainly observed some curtailment of some civil liberties, although I would caution you on that point about allowing the descriptive to collapse into the normative. And of course by that I mean that the restriction of civil liberties during wartime is not necessarily something that we should allow to happen.

¶31 There is a second aspect to the post-Patriot Act developments, which I want to say a few words on and then maybe this would be a good place to stop. And that is that unlike law, which creates authority for surveillance and can swing back and forth as a pendulum between wartime and peace time, technologies of surveillance, I would argue, tend to follow historical arcs. By this I mean, if you make a decision in 2002 to establish a system of public video surveillance in the nation's capital, in Washington, D.C., such that any person standing in front of the Washington Monument, which is by the way not only the potential target of a terrorist act but also a enormously significant meeting point for many political movements throughout this country's history—or the Lincoln Memorial for that matter—if you make a decision to put in place technologies of surveillance it is very difficult to understand the circumstances under which that

---

[30] DEPARTMENT OF JUSTICE, 2003 FOREIGN INTELLIGENCE SURVEILLANCE ACT REPORT (2004), *available at* http://www.epic.org/privacy/terrorism/fisa/2003_report.pdf.

surveillance scheme would be removed.[31] In other words, the Patriot Act is an act of Congress, certain provisions can sunset as they do in 2005, the Act itself can be repealed as former Vice President Gore recommended yesterday, but the technologies of control, the technologies of identification, the technologies of surveillance, and the technologies of monitoring and tracking, like the Clipper encryption scheme of 10 years ago, can be put in place and remain in place with little public debate or discussion.

¶32 And so the thought I'd like to leave you with, and certainly the focus of much of EPIC's work in the years ahead, will be to better understand how these technologies of control are to be controlled. How to bring public accountability, transparency, and democratic control to these new forms of state control that seem to exist outside of the legislative process. It is an enormous challenge, but it is a very important challenge, because the one thing I have learned working in this area for more than ten years is that although people have different definitions of privacy, to some extent everybody understands that this is an important issue. And I'd like to suggest to you today and close with this thought, that privacy in fact may be one of the defining issues of a free society in the twenty-first century.

VI. QUESTIONS AND ANSWERS

¶33 Q (Prof. Boyle): EPIC has covered a variety of different issues, public and private, technological and legal, national and international; I'd be really interested in hearing your, top three or four, in terms either of the degree of threat or perhaps the degree to which you think they haven't received public attention but should have. It would be particularly useful if you could concentrate on things you've been focusing on over the past six months or a year.

¶34 A: Alright, well identification is at the top of the list. Systems of identification, the use of biometrics, in passports and visas. We're also involved in a case the Court recently granted cert in, which is *Hiibel v. Sixth Judicial District of Nevada*,[32] and if you're interested in this case you can go visit our website. This case is about a Nevada statute[33] that basically allows the police to arrest a person in a public space who is suspicious—but not with probable cause that they have committed a crime—and fails to present identification. And this is a statute that is similar to statutes that exist in many of the states which say that you can be arrested because you do not say to the police who you are. We think this is an enormously important case right now because it would create in effect the legal

---

[31] *See* Observing Surveillance, *at* http://www.observingsurveillance.org (last visited June 18, 2004).
[32] 59 P.3d 1201 (Nev. 2002), *cert. granted* 124 S.Ct. 430 (2003).
[33] Nev. Rev. Stat. § 171.123 (2002).

authority—combined with the technologies—that would more frequently require individuals to disclose their identity under any number of circumstances unrelated to criminal activity. Again a person standing at the Washington Monument walks around it a couple of times. The police approach the individual and say "Excuse me, can I see some identification?" The person says "I don't have to say to you who I am." The police arrest the person for acting suspiciously and failing to present identification. That individual could have been walking around the Washington Monument, because he was planning to meet his spouse or a friend who said she would be at the Washington Monument at that point in time. I mean these are the kinds of factual scenarios we need to begin to think about in the context of identification.

¶35 A second big topic has to do with the conflict of privacy regimes. And this arises right now between the United States and Europe, over the requirement that the United States has imposed on European air carriers that they provide to U.S. law enforcement agencies, prior to arrival in the United States, the PNRs,[34] which are the passenger records, on all of their passengers. Now, the Europeans have said that they have a privacy law that prevents the disclosure of this information absent some clear showing that someone is a suspect in a criminal investigation. The United States has said, "If you do not provide this information to us, we will revoke the landing rights for the European airlines." So you have a very interesting conflict between the efforts of the Europeans to safeguard privacy under law and the demands that the U.S. is making on the homeland security front.

¶36 Finally, since you asked me for three, a critical test on so many of these emerging privacy issues is the ongoing challenge of promoting public engagement. One of the things I also learned about privacy in the early days is that there was a lot of good law that had largely been put together by elites—academics, government officials, smart thoughtful people, but in a fairly small community—without much public understanding or support. And I came to the view that sustained political reform requires a broad constituency. That even the best of policies, without public support, will not easily endure. So here's a remarkable statistic for you. The Federal Trade Commission announced a do-not-call list. If you don't want a telemarketer to contact you at home, the FTC gave you an 800 number to call and a website to go to express your preference not to receive these calls at home. Well, I thought 50,000 people was a big number ten years ago. The FTC got 50 million people to sign up for the do-not-call list. That's more people than voted for the last president of the United States.

¶37 Q (Prof. Boyle): Nearly as many people as were on Napster.

---

[34] Passenger Name Records.

¶38 A: That's a big number. Yes, we're getting up there. We're almost up to Napster. But 50 million. Three issues. Anyone else?

¶39 Q (Prof. David Lange[35]): Marc, if I may, let me offer a thought—not a very well formed thought—and see what reaction it might get from you. When Warren and Brandeis wrote their article[36] on privacy at the end of the nineteenth century, they were thinking about the common law as an instrument for responding to the problems that they identified. By the middle of the twentieth century we were beginning, slowly, but with some deliberate speed, to work out privacy issues in terms of the First Amendment. Today, when you speak of privacy, and you think to speak of it in constitutional terms, I think you think of it principally in terms of the First Amendment, though the Fourth Amendment and the Fifth Amendment play some role, and perhaps the Sixth Amendment as well. Certainly, in some sense, as we come to the end of the twentieth century, we're beginning to work these things out on the ground, and as you say, in terms of technology. But one thought I've had for some time is that we lack a key piece of constitutional structure for dealing with privacy issues. We've tortured the First Amendment into a kind of uneasy submission to the needs that we have for privacy protection. And it occurs to me that the First Amendment isn't big enough, isn't capacious enough, to do the job. And more than that, that the First Amendment, in the process of its torturous submission, has actually been to a very great degree bent out of shape. Which brings me to this suggestion, that I would be interested in having your expert reaction to: perhaps what we need to do is to amend the First Amendment, so that we deal more deliberately and more specifically and straightforwardly with privacy issues than we now do. This is an opportunity for all of us, but particularly for activists like you to frame oppositions that can be made central to the debate in a way that the cases don't actually allow us to bring forth. I think of the case involving the sodomy statute in Texas. Which is in some sense a First Amendment case, though it's more of a broader case than that. It's actually a case grounded in some principle that I think has no entirely clear provenance in the Constitution as an occasion for just that kind of amendment. I'll stop here, because you get the drift, and I'm more curious about your reaction than I am hearing myself propose the thought.

¶40 A: Well, I agree with you of course. I think the First Amendment has not always had an easy relationship with privacy, certainly. I've tried to

---

[35] *See* Duke University School of Law, *Faculty Profile: David L. Lange*, *at* http://www.law.duke.edu/fac/lange/ (last visited Mar. 30, 2004).

[36] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), *available at* http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html (last visited Mar. 25, 2004).

make the best case where the privacy interests and the First Amendment interests are largely congruent, but of course there are a lot of cases where that's not as it is. You know, I'm thinking a little bit about this constitutional question, and I'm struck by the decision of the German Constitutional Court in 1983 essentially announcing a right of informational self-determination, very much like the Brandeis/Warren article at the latter part of the nineteenth century, but rooted in the German Constitution. The U.S. Supreme Court came somewhat close to that in *Whalen v. Roe*,[37] which was an opinion in the late 1970s, looking at the automation of personal information and whether people had a constitutional right to control the disclosure of that information. But I don't think we got there. It has been the experience of many people working in the privacy field that the U.S. Constitution doesn't always provide the best material for privacy protection. We have some very good decisions, and I mentioned those in the anonymity realm but in a lot of other areas, we look to statutory frameworks, the acts of Congress and the states. When I was putting together the casebook[38] on information privacy with Daniel Solove, we quite purposefully moved early on in the text from the constitutional analysis and from the tort analysis to what we described as the modern regime for privacy protection based on statutory law. Now, it is interesting to see, and this has certainly been a development in the last few years, some of the stakeholders that are concerned about the impact of privacy laws, such as marketing companies and banks, have looked to the First Amendment as a way to attack these statutory regimes by arguing, for example, that they restrict the ability of a company to communicate with its customer. It's an interesting First Amendment claim, but I don't know that I would go out and recommend amending the First Amendment. I suspect that will get me into quite a bit of trouble with the civil liberties community.

¶41 But the only other point to mention on this, and also in with the spirit of the German decision, is that the European Convention—I want to make sure I get this right cause I get it confused with the Canadians—but in 2001, the Europeans established a new constitution, a charter, the European Charter of Fundamental Rights[39], which includes a provision—I think it's Article 8—on a right to informational privacy. I mean, they simply announced this new constitutional claim. It follows a bit from similar

---

[37] 429 U.S. 589 (1977).

[38] DANIEL J. SOLOVE & MARC ROTENBERG , INFORMATION PRIVACY LAW (2003).

[39] Charter of Fundamental Rights of the European Union, *proclaimed* December 2000, *available at* http://www.europarl.eu.int/charter/pdf/text_en.pdf (last visited Mar. 25, 2004).

language that can be found in the Universal Declaration of Human Rights[40] and the International Covenant on Civil and Political Rights[41] and some of the other international instruments. But I suspect that the better approach, rather than trying to amend the First Amendment, is maybe for *Whalen v. Roe* to be reconsidered, or maybe to announce a new right. Or not.

¶42 Q: You mentioned that one of your main concerns was identification, and specifically the technologies put in place to perform identification. So, I guess one bright spot in all of this is that Tampa, which at some point after 2001 had installed cameras everywhere, face recognition software, I think primarily for security at the Super Bowl. About two and a half months ago, Tampa decided for various reasons that they were going to remove, at the very least, the face recognition software. Do you have any insight on this decision?

¶43 A: Well, it was actually more than two and a half months ago, it was in the spring. I actually debated the fellow from Visionics, his name is Joe Attick—very smart guy, by the way—who started this company on face recognition and the theory was that you can identify people in public spaces by capturing the topology of their face and matching it with a digitized image. John Poindexter, by the way, had a very similar proposal in Total Information Awareness. I mean, what was extraordinary, by the way, about Total Information Awareness was not only the desire to accumulate all the data that could be accumulated, but also to create new means of identification to create data that didn't otherwise exist. So, I, of course, was pleased that they backed off. I actually never thought that face recognition would become a particularly popular means of identification. It's not very reliable.[42] But I think the real challenge we face is that over time other forms of identification will become reliable. Iris scans, for example, can be done at a distance of about 3 to 4 feet, and that turns out to be a pretty good way to do identification in public spaces. I don't know how many of you saw the movie Minority Report. Tom Cruise is going into the Gap, or he's getting on the Metro and there is an iris scan device for identification. (This is a wonderful field, because one of the ways you study, you can almost get credit, is for going to the movies. I mean, top 3 movies for privacy:

---

[40]Universal Declaration of Human Rights (Article 12), *proclaimed* Dec. 10, 1948, *available at* http://www.un.org/Overview/rights.html (last visited Mar. 25, 2004), reprinted in MARC ROTENBERG, PRIVACY LAW SOURCEBOOK 316 (2003).

[41] International Covenant on Civil and Political Rights, *opened for signature* Dec. 16, 1966, *available at* http://www.unhchr.ch/html/menu3/b/a_ccpr.htm (last visited Mar. 25, 2004).

[42] *See, e.g.*, DEPARTMENT OF DEFENSE, FACE RECOGNITION AT A CHOKEPOINT: SCENARIO EVALUATION RESULTS, (2003); *see generally*, EPIC, *Face Recognition*, *at* http://www.epic.org/privacy/facerecognition (last visited June 18, 2004).

Minority Report, Enemy of the State, Gattaca. And plus, they're good movies, you know, it's not a bad thing.) So, anyway, I don't think face recognition, as the technology is currently described, is actually likely to gain much acceptance. But you'll see other techniques, including one, interestingly, that measures radiant heat from the face, which turns out to be actually somewhat more reliable than the topology of the face.

¶44 Q: I had a question about this idea of emerging technologies. It's the nature of these technologies, something like Moore's Law, where computers just multiply rapidly in terms of their capabilities. So when you're looking at a technology that's new, how do you imagine what the possibilities are for a technology that is in place. In other words, cameras on the monuments in Washington mean one thing now; they could mean a very different thing in 30 years. And once those technologies are established, as you've been saying, it's very difficult to remove them. How do you take into account the things that aren't?

¶45 A: Well it's an interesting question. It's actually a question somewhat hopefully that the U.S. Congress has focused on more intently in the last few years. We did some work with the Congress around the so called E-government initiatives to require federal agencies to conduct what are called privacy impact assessments. And in the design of new record systems, they now ask a series of questions to try to evaluate the privacy impact of these systems. This is obviously an application of a technology, but you ask what kind of information is going to be obtained, who is it going to be disclosed to, under what circumstances will it be disclosed. And this is a way, I think, to promote a bit more public discussion about the scope and impact of these systems. Again, not with the goal of saying, "Oh, you can't use technology in the federal government," but rather trying to provide some means of oversight. One of the things we did, post-September 11th, was to bring some Congressional scrutiny to bear on the Transportation Security Agency's proposal for a "Computer Assisted Passenger Profiling System."[43] We said, "Where's the privacy impact statement for the Passenger Profiling System? It's a government record system, there should be a privacy impact statement, so at least we can talk about it." And they said, well, they hadn't completed the privacy impact statement. Well, boy, if you're a Washington lawyer and you hear something like that, you're already ordering drinks for people. I mean that was actually really good news for us. So even before we get to the debate about whether or not CAPPS II should go forward, we're saying, "Why can't you disclose the impact statement, like the 9-11 commission?" But I

---

[43] *See, e.g.*, Matthew L. Wald, *U.S. Agency Scales Back Data Required on Air Travel*, N.Y. TIMES, July 31, 2003, at A18 (2003) (discusses the CAPPS II system and its proposed implementation).

think that's what you try to do. You try to evaluate and create mechanisms of evaluation for the public to assess.

¶46 Q: I'm not sure whether this question—it may be too abstract of a case, so feel free to brush if off. But I'm curious about your comment about how the Germans have come to kind of enshrine the notion of informational self-determination, and I'm thinking about that in contrast to HIPAA,[44] which is a really complicated piece of legislation. A lot of its energy goes into trying to specify all sorts of situations that you can dream up about having processes and processes around processes for dealing with who gets access to information, as opposed to just kind of saying, "Information about you is yours; you get to decide and making a presumption that that drives the decision-making." As a matter of legal strategy, what do you think about those two processes? One is a very elaborate specification in statute of things and the other is kind of setting out very general principles of who owns something.

¶47 A: I think the privacy field is somewhat lucky in this respect. We have a set of organizing principles that are generally referred to as "fair information practices." Those are magical words in the privacy realm. Fair information practices describe the allocation of rights and responsibilities in the collection and use of personal information. Also, somewhat conveniently, all of the rights basically go to the individual who's giving up the personal information, and all of the responsibilities go to the organization that obtains the information. Now, these fair information practices are actually set out in places like the findings of the Privacy Act of 1974. I know they're discussed in the HIPAA regulations, they're also in the OECD Privacy Guidelines of 1980.[45] You'll see them in many different places, but it's a set of principles numbered somewhere between five and eight, that talk about transparency, accountability, rights and remedies, and provide, again, metrics for evaluating the effectiveness of privacy statutes and regulations. Now, the problem with HIPAA of course, is that it's just enormous. I mean a few years ago I was discussing with someone the possibility of publishing the HIPAA regulations (the Health Insurance Portability Accountability Act). I wanted to publish a book, because we publish a lot of source material. We publish a lot of the federal statutory laws, we publish international materials, and we talked about publishing the HIPAA regulations. The regulations, without the public comment, ran 900

---

[44] Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

[45] OECD Recommendation Concerning and Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, Oct. 1, 1980, *available at* http://www.cpsr.org/cpsr/privacy/privacy_international/international_laws/1980_oecd_privacy_guidelines.txt (last visited Mar. 28, 2004).

pages in the Federal Register. And that's that small 9-point type. Can you imagine publishing a multi-volume set of federal regulations? I mean, that would end up in someone's trunk who needed the weight going through snow. So we decided not to do that, and I'm very sympathetic to all the people working in the privacy field, who are doing HIPAA regulations. Although, I can also tell you that for the law students here exploring career opportunities, according to *Money* magazine, August 2003,[46] the top hot job in the U.S. economy was chief privacy officer. How's that? Nice six figure salary. So I'm somewhat sympathetic to the people who are doing the HIPAA regulations, but I also know they're pretty well compensated for going through those 900 pages of rules.

[46] Joan Caplin, Ellen McGirt & Amy Wilson, *Make Your Fortune Part 2*, MONEY, Aug. 2003, at 80.