

Panel I: The Conflict Between Commercial Speech and Legislation Governing the Commercialization of Public Sector Data

Moderator: James Goodale^{*}
Panelists: Robert Sherman^{**}
Paul Schwartz^{***}
Deirdre Mulligan^{****}
Steven Emmert^{*****}

MR. GOODALE: The issue today we are going to try to grapple with is: Privacy and the First Amendment: Is there a tension; and if so, where is it?

I want to welcome to the panel, Steve Emmert, who is Director of Government Affairs for *LEXIS-NEXIS, Reed Elsevier, Inc.*; Deirdre Mulligan, who is at the Center for Democracy & Technology; Paul Schwartz, who is a Professor at Brooklyn Law School, and who teaches courses in the Internet and telecommunications; and Bob Sherman, a partner at Paul Hastings, who I have talked into being our opening speaker. He told me just before we started that he submitted an *amicus* brief in the *United Reporting Publishing* case,¹ which was decided by the Supreme Court, and which tangentially raises some of the issues to which we wish to address our attention. He also has kindly, not only agreed to be the first speaker, but has said that in his speech he

^{*} Founder, Media/Communications/Intellectual Property Section, Debevoise & Plimpton; Adjunct Professor of Law, Fordham University School of Law. Yale University, B.A. 1955; University of Chicago Law School, J.D. 1960.

^{**} Partner, Paul, Hastings, Janofsky & Walker; General Counsel, Direct Marketing Association. University of Rhode Island, B.A. 1967; The American University Law School, J.D. 1971.

^{***} Professor of Law, Brooklyn Law School. Brown University, B.A. 1981; Yale Law School, J.D. 1985.

^{****} Staff Counsel, Center for Democracy & Technology. Smith College, B.A. 1988; Georgetown University Law School, J.D.

^{*****} Director of Government & Industry Affairs, LEXIS-NEXIS, Reed Elsevier, Inc. The Ohio State University, B.A. 1979; J.D. 1982.

¹ See *Los Angeles Police Dep't v. United Reporting Publ'g Corp.*, 528 U.S. 32 (1999).

would try to frame the issue.

So, sir, you are on.

MR. SHERMAN: Thank you, I think.

First of all, I am pleased to be here. I want to thank everybody who made it possible for me to participate.

I want to spend the first couple of minutes describing where the industry is today and then try to frame the issues regarding the tension between the First Amendment and privacy.

I found the first two speakers' comments very enlightening. I wish I had a few hours to respond to them, but I don't. The industry now is pretty much in a self-regulatory mode.² There are not many privacy statutes that directly affect marketing and commercial speech. There are a few, but only a few.³ And so, right now the industry is depending on trying to do the right thing.

What that comes down to are five elements of self-regulation that are now being followed. Let's see where they fit into the tension between the First Amendment and privacy.

The first is notice: let the consuming public know what your privacy practices are. Put simply, they are entitled to be aware and make informed choices. That, of course, is a perfect segue into point number two, which is choice. It should be left to the consumer to choose what is done with his or her personally identifiable information.⁴ Of course, there is a raging debate on whether that should be "opt-in" or "opt-out",⁵ and I am going to

² See Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1247 (1998). See also A Framework for Global Electronic Commerce (July 1, 1997), available at <http://www.ecommerce.gov/framework.htm> (last visited Nov. 1, 2000).

³ See Kang, *supra* note 2, at 1231-32 ("[O]f those statutes governing the collection of personal information, none are particularly constraining.")

⁴ See *Comments of the Direct Marketing Association on Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy* (July 6, 1998), available at <http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/DMA.htm> (last visited Nov. 1, 2000); see also Kang, *supra* note 2, at 1247.

⁵ See, e.g., Leslie A. Kurtz, *The Invisible Becomes Manifest: Information Privacy in a Digital Age*, 38 WASHBURN L.J. 151, 170 (1998) (discussing "opt-in" and "opt-out" regulation); Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation Is Inadequate*, 49 S.C. L. REV. 847 (1998) (proposing model statute seeking to address consumer privacy concerns in lieu of industry self-regulation).

address that in a few minutes.

So, notice and choice are really bedrock to sound privacy principles.

The third one has created real controversy, and that is the notion of access. The European Union is pushing hard for access.⁶ It is a concept that is familiar to those who conduct their businesses subject to the Fair Credit Reporting Act,⁷ but it is something that really is alien to commercial or marketing companies. After all, what does access mean? Access to what? Does it come with the right to correct? If it does, how important is it to one's privacy to be able to correct transactional data – for example, I bought a blue shirt, but my records say I bought a green shirt and I want that fixed up. At what expense? At whose expense?

Does any right to access reach data and information that are inferred by marketing companies that did not get this information from you but perhaps obtained it through modeling or other methods they believe apply to you? Is there such a thing as correcting those types of data?

Access is an important issue that is right now being debated, as we heard from our keynoters. The Federal Trade Commission is holding hearings on what has been dubbed “profiling,” and access is a key issue there.⁸

Then, of course, there is security. Whether it is online or through traditional media, I do not believe anybody will argue with the fact that personally identifiable information should be kept in secure places and in secure ways.

Finally, what is the enforcement regime? What are the punishments or the sanctions for anybody who violates whatever the appropriate way to handle data is? That is pretty much what the self-regulatory process is requiring now.

⁶ See *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Part Two, ¶ 13 (Sept. 23, 1980), available at <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> (last visited Nov. 1, 2000) (recommending that individuals have the right to access information maintained by data controllers about him/herself).

⁷ 15 U.S.C. § 1681 (2000).

⁸ See *Workshop Notice, Department of Commerce Federal Trade Commission Workshop on Online Profiling*, Fed. Reg. Docket No. 990811219-9219-01, available at <http://www.ftc.gov/os/1999/9909/FRN990915.htm> (last visited Nov. 1, 2000).

A large, indeed leading, industry association has made a privacy promise to the American public.⁹ It is requiring each of the above-referenced principles to be honored or a member company that fails to do so is expelled from the organization, perhaps publicly censured, and if it also results in a legal violation of some kind, then the file is turned over to a law enforcement agency.¹⁰

So those are the key elements of self-regulation. We believe it works and we believe it should be permitted to continue to work.

But what are the conflicting forces here in trying to do the right thing and in having government and law enforcement agencies allow business to do the right thing while still making sure that all constitutional and other protections are provided?

Let's go back to the 18th century. Benjamin Franklin, in 1744, actually developed the first catalogue.¹¹ He mailed out 600 of them.¹² His sole goal was to have everybody pay the same price, everybody treated the same way, everybody get the same customer service.¹³ During that same period of time, 55% to 75% of the pages in newspapers consisted of ads - almost exclusively commercial information.¹⁴ In fact, the first case that defended free speech was a commercial case.¹⁵

And so, when the Framers drafted the First Amendment and interchangeably used the words "freedom of speech" and "freedom of the press,"¹⁶ there is little doubt that what they had in mind

⁹ See generally, Online Privacy Alliance, Effective Enforcement of Self Regulation: Verification and Monitoring, available at <http://www.privacyalliance.org/resources/enforcement.shtml> (last visited Nov. 4, 2000); The DMA's Privacy Promise in Direct Marketing Association: The United States of America Land of Opportunity Direct Marketing An Overview, available at <http://www.the-dma.org/librarylandofopportunity.shtml> (last visited Nov. 4, 2000).

¹⁰ See generally, Online Privacy Alliance, Effective Enforcement of Self Regulation: Consumer Complaint Resolution, available at <http://www.privacyalliance.org/resources/enforcement.shtml> (last visited Nov. 4, 2000).

¹¹ See Benjamin Franklin, A CATALOGUE OF CHOICE AND VALUABLE BOOKS, Philadelphia (1744).

¹² See *id.*

¹³ See *id.*

¹⁴ See generally, ALFRED MCCLUNG LEE, THE DAILY NEWSPAPER IN AMERICA: THE EVOLUTION OF A SOCIAL INSTRUMENT 31-33 (1937).

¹⁵ *Republica v. Oswald*, 1 U.S. 319 (1788).

¹⁶ U.S. CONST. amend. I; see also Melville B. Nimmer, *Is Freedom of the Press a Redundancy: What Does it Add to Freedom of Speech?*, 26 HASTINGS L.J. 639, 641 (1975) (suggesting that the Framers may have regarded freedom of speech and freedom of the press as interchangeable). But see Arlen W. Langvardt, *Media Defendants, Public*

included commercial free speech. Commercial speech then clearly was a first-class citizen. There was no difference in the treatment of political speech and commercial speech.

Now let's fast-forward. In 1980, after some serious struggle, the U.S. Supreme Court, in *Central Hudson*,¹⁷ established a four-step test to determine whether or not the right to commercial free speech was being violated.¹⁸

The four steps essentially are: (1) the state has to demonstrate a substantial state interest; (2) it has to show that the regulation of speech was in proportion to that interest; (3) it has to demonstrate that in achieving that goal it has to directly advance the state interest; and (4) it has to do so in the "least-restrictive manner," which subsequently has been modified to require that it be in a "tailored way or in a way where there is a reasonable fit between the restriction and the goal to be achieved."¹⁹

In summary, that is what the First Amendment side requires: a substantial state interest, regulation proportionate to the interest, the direct advancement of that interest, and doing so in a tailored manner. In other words, the restrictions may not be overly broad, excessive, or go further than they have to.²⁰

On the other side of this equation is the issue of privacy. There is no question about there being a right to privacy, but you will never find the word in the Constitution.²¹ It is not really well-defined.²² In 1965, *Griswold v. Connecticut*,²³ referred to it as a "penumbra" or a zone that covered many different kinds of rights.²⁴ But before one can tread on First Amendment grounds,

Concerns, and Public Plaintiffs: Toward Fashioning Order From Confusion in Defamation Law, 49 U. PITT. L. REV. 91, 117-18 (1987) (stating that "[T]he intent of the Framers with regard to the speech and press clauses is unclear.").

¹⁷ See *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980).

¹⁸ See *id.* at 564-66.

¹⁹ *Id.*

²⁰ See *id.*

²¹ See, e.g., ELLEN ALDERMAN & CAROLINE KENNEDY, *THE RIGHT TO PRIVACY* (Vintage Books 1997) (1995).

²² See Fred H. Cate, *PRIVACY IN THE INFORMATION AGE 3* (Brookings Institution Press 1997) (explaining the lack of consensus of what "privacy" means).

²³ 381 U.S. 479 (1965).

²⁴ See *id.* at 483 ("[T]he First Amendment has a penumbra where privacy is protected from governmental intrusion.").

one must have something more than an abstract concept.²⁵ The concept must be concretely defined, there must be some demonstrated harm, before one abridges free speech.²⁶ The *Griswold* definition of a zone or a penumbra does not appear to provide the justification.

In 1973, *Roe v. Wade*²⁷ held that only personal rights that can be deemed fundamental or implicit in the concept of ordered liberty are included in this guarantee of personal privacy.²⁸ The Court gave examples such as marriage, procreation, contraception and family relationships as those areas of privacy that are protected by the Constitution.²⁹

Then the tension began to mount. In the 1960s, the Supreme Court stated that requiring people to give one permission to communicate to them violates free speech.³⁰ When it comes to speech, inhibition and inconvenience, as well as prohibition, violate the First Amendment.³¹ The famous quote out of that case was “[I]t would be a barren marketplace of ideas that had only sellers and no buyers.”³² Clearly there was a recognized right to communicate; equally clearly there was a right not to have true privacy invaded.

Then more recently, in *Shapero v. Kentucky Bar Association*,³³ where the more modern techniques of targeted marketing were involved, the Supreme Court decided that a state may not restrict solicitations in a way so that what would be left is the ability to contact only those least likely to respond to a promotion.³⁴ In other words, target marketing is not bad per se.³⁵ The Court did not address the issue of privacy, of how one determines the

²⁵ See Cate, *supra* note 22, at 55.

²⁶ See *Edenfield v. Fane*, 507 U.S. 761, 770-71 (1993).

²⁷ 410 U.S. 113 (1973).

²⁸ *Id.* at 152 (citations omitted).

²⁹ See *id.* at 152-53.

³⁰ See *Lamont v. Postmaster Gen.*, 381 U.S. 301, 307 (1965) (holding that requiring addressee to request delivery of his mail in writing is an “unconstitutional abridgment of the addressee’s First Amendment rights”).

³¹ See *id.* at 309 (Brennan, J., concurring).

³² *Id.* at 308.

³³ 486 U.S. 466 (1988).

³⁴ See *id.* at 479.

³⁵ See *id.* at 476 (“[M]erely because targeted, direct-mail solicitation presents lawyers with opportunities for isolated abuses or mistakes does not justify a total ban on that mode of protected commercial speech.”).

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 27

targeted audience, by what means, what computers, et cetera.³⁶

The speakers on this panel are supposed to discuss the tension between the First Amendment and privacy with respect to public data. Of course, the fact that data are required to be made public, presumably, serves a public interest. Why else would the state or the federal government require that information to be placed on the public record? So one must ask, “Why is that information required in the first place? Why is it required to be public?” There is a public interest being served just by the simple fact that the data are made public.

Once they are made public, one could argue that any privacy interest starts to fade. The information is public. The very antithesis of private is public.

Then the issue seems to become: If the subjects of the information that has been made public were not given a choice, should they have been; and, if so, should it be “opt-out” or “opt-in”?³⁷

Referring back to the bullet points of what self-regulation covers now - notice, choice, access, security, and sanctions - the choice element may be viewed as either “here’s what we do; we’re going to do it unless you say not to;” or “here’s what we would like to do; we won’t do it unless you say it’s okay.” The first one is “opt-out” – we are going to do it unless you say no.³⁸ The second one is “opt-in”.³⁹ Clearly, “opt-in” raises First Amendment issues by creating additional impediments for commercial communication.⁴⁰

I would like to make one point before attempting to join the issue, and that is to highlight the one aspect of the First Amendment that seems to be completely overlooked in all of the debates, that I either have heard or participated in. *Central*

³⁶ See generally *id.*

³⁷ See Leslie A. Kurtz, *The Invisible Becomes Manifest: Information Privacy in a Digital Age*, 38 WASHBURN L.J. 151, 170 (1998) (“There are two basic approaches to the issue of choice and consent, generally called opt-out and opt-in.”).

³⁸ See *id.* (“[A]n opt-out approach . . . presupposes permission to use and disclose personal information unless the consumer takes affirmative steps to state an objection.”).

³⁹ See *id.* (stating that under “an opt-in approach . . . information cannot be used for purposes other than that for which it was given and cannot be disclosed to others unless the consumer expressly agrees or opts in”).

⁴⁰ See *id.*

*Hudson*⁴¹ not only stated that it is the speaker's right to communicate his or her message, but also that it is the listener's or reader's right to receive the message.⁴² Listeners and readers have First Amendment rights, and when one treads on that aspect of the First Amendment, one violates the Constitution the same as when one inhibits or prohibits the speaker's right to be heard.⁴³

One must ask the question: If there are a number of willing listeners or readers, then, by requiring all of them to take some affirmative action before one can communicate with them, isn't the communicator being restricted or inhibited, or being confronted with artificial obstacles with respect to those who want to receive the communication? The First Amendment does not allow that.

I was hoping I would go last because, as a litigator, I am well aware of the advantage of being heard last. But going first wasn't so bad because I had a chance to pose a lot of questions, without having to answer them.

"Opt-in" versus "opt-out", just a few observations about that debate.

Historically, the self-regulatory regime has been notice and "opt-out".⁴⁴ It is friendly to the free flow of information. It allows that flow unless someone feels so strongly that they say "no, thank you, I don't want to be included in this, I don't want to have my name and address transferred to another marketer who may have information that is valuable to me, or who may send a solicitation that I may want, but I have chosen not to receive it, so I "opt-out"." That has historically been the methodology.⁴⁵

Even legislative requirements, few as they were, had taken the "opt-out" approach. That was changed by the Children's Online Privacy Protection Act,⁴⁶ which requires affirmative parental consent, verifiable consent by the parent, i.e. "opt-in", before one

⁴¹ See 447 U.S. 557 (1980).

⁴² See *id.* at 567.

⁴³ See *id.* at 567-68.

⁴⁴ See generally Linda A. Goldstein, *Emerging Issues in Online Advertising and Promotion Law*, 570 PLI/PAT 821 (1999); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

⁴⁵ See generally Sovern, *supra* note 44.

⁴⁶ See Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6505 (1998).

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 29

can collect information *from* a child, as distinguished from information *about* a child.⁴⁷

The new Health Data Privacy Guidelines categorize certain types of information from certain types of relationships,⁴⁸ e.g., physician-patient where it may require the affirmative consent of the patient before that information may be disclosed or transferred.

But when it comes to general marketing or transactional information, historically it has always been “opt-out”.

What are the pros and cons of each? They both result in consumer choice. There is no greater or lesser protection after the consumer has exercised that choice. The consumer either will or will not participate in the marketing process, depending on whether he or she says “okay” or “not okay.”

“Opt-out” is certainly friendlier to the free flow of information because it allows the flow unless somebody says “no.” “Opt-in” is viewed by many as creating barriers to entry. It creates difficulties for new, small, under-capitalized, potential competitors. They may not have the wherewithal to go through the permission process that it takes. As can be seen, there are other problems (besides First Amendment v. Privacy) that have to be considered when examining “opt-in”.

In the interest of full disclosure, I have spent the last twenty-eight years representing the direct marketing industry, which more recently includes the e-commerce and Internet companies. The Direct Marketing Association (the “DMA”), for which I serve as general counsel, has acquired two major Internet trade associations.⁴⁹ So, although I personally, and the industry generally, respect and seek to honor privacy principles and privacy requests, we also have to stand tall when it comes to the right to be heard and the consumer’s right to receive information that they may find valuable.

⁴⁷ *See id.*

⁴⁸ *See* Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 *VAND. L. REV.* 295, 333 (1995); *see generally*, Health Privacy Project: Institute for Health Care Research and Policy Georgetown University, available at <http://www.healthprivacy.org> (last visited Nov. 4, 2000).

⁴⁹ *See* Courtney Macavinta, *Lobbying Group Acquires Internet Alliance*, (May 4, 1999), available at *CNET News.com* <http://news.cnet.com/category/0-1005-200-342053.html>. (last visited Nov. 1, 2000); *see also*, DMA Affiliates, available at <http://www.the-dma.org/aboutdma/dmaaffiliates.shtml> (last visited Nov. 18, 2000).

Maybe this is a good time to sit down. Thank you for your time and attention.

MR. GOODALE: Thank you very much.

I have to tell you that the decision to have the first speaker speak first was only made about six minutes ago, and immediately the first speaker gets up and has five points. Only a litigator can do that.

PROFESSOR SCHWARTZ: Let me begin by saying I am happy to see Peter Swire in the audience, a friend of mine from law school, and the first privacy advisor to the Federal Government. I have enjoyed talking with Peter over the years about privacy and many other issues. He is doing a great job in D.C., and I am very happy to see him here.

Now, what I wanted to do is make only three points, but I am going to make a fourth point, because for me it's a little surprising to have someone, Mr. Sherman, first tell us how great self-regulation is, but then also tell us he has been working for the DMA for twenty-eight years and has been part of the ongoing DMA activities with self-regulation. Now I could be wrong, but my impression was that, historically, self-regulation by the DMA has not been a success and that it has essentially been used to stave off more effective regulation.⁵⁰ Historically, self-regulation has been mostly—and I may be wrong—a smoke screen.⁵¹ And so for us to hear today that self-regulation has worked and it is now going to work in e-commerce, well, my perspective, which, again, may be incorrect, is that, due to a lot of pressure on the direct marketing industry, it is trying to get ahead of the legislative bandwagon by sprinting to the front and trying to make its policies somewhat more effective.

I think there is room for self-regulation. There is also room for thinking about using markets to regulate, and using norms to regulate, and using self-regulation to regulate. We should not only depend on law and “command and control” regulation. But nevertheless, to the extent that the direct marketing industry has moved in the right direction, it has been because of a lot of outside

⁵⁰ See PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION n.5 & 332 (1996).

⁵¹ See *Sovern*, *supra* note 44, at 1081.

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 31

pressure, including that of privacy advocates and journalists and other people pointing out that historically their record has been poor.⁵² But again, I could be wrong.

But by the way, what this last comment doesn't mean is that direct marketers should not try self-regulation and that we should not encourage more creative forms of regulation in the twenty-first century. But I also think we should bring an awareness of the history and see if we cannot learn from the past.

MR. SHERMAN: Well, we agree in part.

PROFESSOR SCHWARTZ: There we go.

MR. SHERMAN: You were wrong.

PROFESSOR SCHWARTZ: Okay. Well, it's not the first time.

Let me then make three points. I want to talk about privacy's constitutive role; then I want to talk about fair information practices, which Mr. Sherman also mentioned; and then I want to talk about free speech versus privacy.

How should we think about information privacy? I think, as our first speaker has pointed out, it is a slippery concept and it can mean many different things in our legal system.⁵³ One leading approach is thinking of privacy as a right of control, namely, that the state should decide to give you more or less control over your information based on the circumstances.⁵⁴ I think that this notion, this vision, this paradigm, has not worked out particularly well,⁵⁵ and I want to briefly point out two reasons for the failure of privacy-as-control.

One problem is that privacy-as-control looks to the exception and not the rule.⁵⁶ There are many reasons in the Information Age that data about us are collected, stored, and processed; and so if we view privacy within this control notion, very quickly we see that there are real limits on the desirability of an individual controlling

⁵² See Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 542-46 (1995).

⁵³ See *infra* p. 5; see also Reidenberg, *supra* note 52, at 498.

⁵⁴ See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1659 (1999).

⁵⁵ See *id.* at 1660-64.

⁵⁶ See *id.* at 1663.

her information.⁵⁷ In other words, an external social reality is reflected in your personal information, and neither the state nor the private sector is going to want to allow us too much of a right of control. Put differently, we can not have a complete right to rewrite events that actually took place.⁵⁸ That would be highly problematic.⁵⁹

Second, it seems to me the idea of privacy as control runs into difficulty once we give up our information.⁶⁰ This kind of interest, this idea of privacy-as-control, functions best when information is kept secret or known only by a small group. But the critical issue today is usually not *whether* personal data should be collected and processed, but *how* data should be and should not be used.

So what, then, do we want from privacy if it is not this notion of control? Well, I think we should think of privacy as doing something constitutive.⁶¹ Access to personal information and limits on it help form the society in which we live and shape our individual identities.⁶² Information privacy, whether on or off the Internet, should be considered to be a constitutive value.⁶³ As an example, the structure of access to personal information will have a decisive impact in many instances on the extent to which certain actions or expressions of identity will be encouraged or discouraged.⁶⁴ Therefore, the importance of information privacy for both individuals and the community necessitates attention to how we set the boundaries about personal information.⁶⁵

Now, let me move on to my second point. What about fair information practices? These are, in fact, the building blocks of modern data privacy law, and there are various formulations of

⁵⁷ See *id.* at 1663-64.

⁵⁸ See Schwartz, *supra* note 48, at 309 (“An individual’s control over medical and other personal information cannot be complete because, at least to some extent, these data reflect an outside social reality.”); see also Schwartz, *supra* note 54, at 1646 (“Personal data often involve a social reality that is external to the individual . . .”).

⁵⁹ See Schwartz, *supra* note 54, at 1647-58.

⁶⁰ See generally, Glenn Chatmas Smith, *We’ve Got Your Number! (Is it Constitutional to Give it Out?): Caller Identification Technology and the Right to Informational Privacy*, 37 UCLA L. REV. 145, 223 (1989).

⁶¹ See, e.g., Schwartz, *supra* note 54, at 1658.

⁶² See *id.*; see generally Reidenberg, *supra* note 52.

⁶³ See Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 731-2 (1987).

⁶⁴ See generally Schwartz, *supra* note 48.

⁶⁵ See *id.*

them.⁶⁶ Let me give you one that breaks them down into four elements. Fair information practices are: (1) defined obligations that limit the use of personal data; (2) transparent processing systems, which is the notion that you should know who is doing what with your information; (3) limited procedural and substantive rights over your information; and (4) external oversight.⁶⁷ Fair information practices also help shape the kinds of constitutive territories that we have in our society.

Now, on to my third and final point. Let me say something about free speech versus privacy. It seems to me that, aside from purely public discourse, a democratic society depends on other realms of communication. I think First Amendment law should acknowledge the strengths and weaknesses of communication in different settings.

As an initial example of legal scholarship that is sensitive to the nuances of communication in different settings, I would point to Kathleen Sullivan's work regarding speech intermediaries in the age of cyberspace.⁶⁸ As a second example, I would point to the work of Robert Post.⁶⁹ Robert Post has provided a map of different communicative domains. He argues that in the realm of community, we regulate speech in terms of civility and dignity, and we do that primarily through the defamation tort.⁷⁰ According to Post, in bureaucratic organizations, we regulate speech due to the logic of what he calls "instrumental rationality."⁷¹ Finally, we have the public sphere, the sphere of the pure First Amendment, or the First Amendment unbounded. In the public sphere, the First Amendment provides quite strong barriers against limits on communication.⁷²

⁶⁶ See generally Reidenberg, *supra* note 52.

⁶⁷ See Schwartz, *supra* note 54, at 1671.

⁶⁸ See, e.g., Kathleen M. Sullivan, *First Amendment Intermediaries in the Age of Cyberspace*, 45 UCLA L. REV. 1653 (1998).

⁶⁹ See, e.g., Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249 (1995); Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957 (1989) [hereinafter *Social Foundations*]; Robert C. Post, *CONSTITUTIONAL DOMAINS: DEMOCRACY, COMMUNITY, MANAGEMENT* (1995).

⁷⁰ See Post, *Social Foundations*, *supra* note 69, at 957.

⁷¹ See *id.*

⁷² See *id.*

The tension in this area then is, on one hand, we have fair information practices, and on the other hand we have an increasingly strong and growing public sphere. We have to find a way of thinking of fair information practices as structuring the terms on which individuals confront the information demands of community, bureaucratic entities, and the public sphere. Now, I have offered this vision of mine at a somewhat high level of abstraction. The challenge for justices and judges, for policy makers and legal scholars, is to construct an information privacy law that becomes an integral part of the mission of the First Amendment and not its enemy.

Thank you.

MR. GOODALE: Thank you. Deirdre?

MS. MULLIGAN: It's a pleasure to be here. It is not very often that I actually get to talk to people who spend a lot of time thinking theoretically about things. It is also very nice to have been led off by Paul Schwartz, who has done a lot of very excellent, interesting thinking in this area, and actually, like Joel Reidenberg, has done some of that translating theory into practice. And I appreciate the ability to look at things practically, which I think is part of what Peter Swire invited your assistance in doing.

Many of us are in the position of dealing with things at the very practical level - how do we get from point *A* to point *B* - and don't always have the luxury of sitting back and thinking big, theoretical thoughts about what are the implications of various things going on in the marketplace or in the regulatory areas.

I think that in the privacy area, and in this particular area where we are talking about public records - I don't think anybody has mentioned the word yet, but that is what I think we are talking about today - it is an area where there is an overwhelming lack of good writing. And, like Peter, who invited you to think about these issues and write about them, we really need some more critical thinking about public records and privacy, and open government, and how those things come into play.

Looking at privacy, as Professor Schwartz reiterated, is an incredibly slippery concept.⁷³ Just to give you an idea of what it

⁷³ See *supra* note 53.

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 35

might be like: I feel like there is an elephant, and different people have been reaching at different parts of it, somebody has the ear and somebody has the tail.

If you look at the cases that were presented in your binder, how many of you actually read them? Did you read all of them? Okay.

Well, we have a case where a petitioner will come in and say, “You’re limiting my speech,” and the court comes back and says, “No, we’re restricting your access.” Then somebody comes in and says, “You’re regulating a state activity” - this is the Driver’s Privacy Protection Act,⁷⁴ which wasn’t really discussed today, but recently Congress decided to actually heighten the limits on what states can do with drivers’ records, and they said, “You cannot disclose them” - there are a few exceptions – “without consent.”⁷⁵

The Supreme Court, in a decision that surprised many people across the board,⁷⁶ whether you are a fan of privacy or a fan of free flow of information, or actually think that you can mesh them together, which is where I find myself, were stunned when the Court came back and said, “No, it’s a commodity in commerce, your information.”⁷⁷ Okay, so we have: it’s a limit on speech, it’s a restriction on access, it’s a regulation of a state activity, it’s a commodity in commerce.

We heard Peter talk about privacy as something that we want to leave open for the states to legislate because it is a civil right, the notion of privacy, I think closest to what Paul was talking about, a constitutive right.⁷⁸

We hear it spoken of as property.⁷⁹ Well, that begs the question as to exactly whose property. I think there are people in the commercial area who definitely think that once I have handed

⁷⁴ Driver’s Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725 (1994 & Supp. III 1997) (amended as of Oct 9, 1999 and effective June 1, 2000).

⁷⁵ See Tony Mauro, *Federal Act Barring Sale of Data Upheld*, N.Y.L.J., Jan 13, 2000, at 1; Linda Greenhouse, *Justices Uphold Ban on States’ Sales of Drivers’ License Information*, N.Y. TIMES, Jan. 13, 2000, at A29.

⁷⁶ See Mauro, *supra* note 75, at 1.

⁷⁷ See *Reno v. Condon*, 120 S.Ct. 666, 671 (2000) (holding that “[b]ecause drivers’ information is . . . an article of commerce, its sale or release into the interstate stream of business is sufficient to support congressional regulation”).

⁷⁸ See Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553 (1995).

⁷⁹ See, e.g., Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 397-400 (1978).

something over to them, it becomes their property rather than my property⁸⁰ and we now have very interesting cases talking about limits on speech, not on expressive activity.⁸¹ I can draw some very good analogies of where there are very express tensions between privacy and the First Amendment. If I say to someone, “You may not send somebody else any messages or you may not call somebody,” I am setting up a real tension between somebody’s expressive activity and somebody else’s privacy.

We have laws on the books at the federal level, and at the state level, that limit when commercial entities can call people.⁸² They also limit the kind of solicitations you can get in various mediums⁸³ - some of the new ones are in e-mail⁸⁴ - and there are carefully crafted balances there, because there are privacy and First Amendment interests that are in tension.

The area dealing with what I would call “incidental impacts on speech” perhaps is what we are talking about when we talk about data privacy. It is true that I might set up some rules about how a company can use information that it has gathered about individuals, or how the government can use information that might make the cost of their speech more expensive.⁸⁵ So, for example, if I cannot target people, I might have to send many more people the same message. That is not a direct limit on my expressive activity, which would really kind of raise the First Amendment flag.⁸⁶ However, it may mean that it is more costly for me to reach an audience.

Now, we do deal with an awful lot of regulations that make a whole variety of things more expensive and more difficult to do, and all of those do not fall by the wayside because of First

⁸⁰ See Solveig Singleton, *Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector* (Cato Inst. Policy Analysis No. 295, 1998), available at <http://www.cato.org/pubs/pas/pa-295.html>. (last visited Nov. 1, 2000).

⁸¹ See, e.g., *Los Angeles Police Dep’t v. United Reporting Publ’g Corp.*, 528 U.S. 32 (1999); *Amelkin v. McClure*, 205 F.3d 293 (6th Cir. 1998).

⁸² See 15 U.S.C. § 1681a(0)(2000); Thomas J. Schramkowski, *Commerce and Trade Selling and Other Trade Practices*, 15 GA. ST. U. L. REV. 9 (1998).

⁸³ See Schramkowski, *supra* note 82.

⁸⁴ See Alderman, *supra* note 21.

⁸⁵ See *United Reporting Publ’g Corp.*, *supra* note 81.

⁸⁶ See, e.g., *Spence v. Washington*, 418 U.S. 405, 410-11 (1974) (stating that First Amendment scrutiny is triggered whenever “an intent to convey a particularized message was present, and in the surrounding circumstances the likelihood was great that the message would be understood by those who viewed it”).

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 37

Amendment concerns.⁸⁷ I think Peter raised this in thinking about fiduciaries and in thinking about rules that govern how people use information that they may have in a variety of settings where they are privy to personal information or facts; and that those rules do not all fall by the wayside because they have an incidental impact on, for example, the cost of speaking. So it does raise some questions.

So, what are these tensions that we are talking about when we talk about public records and privacy and speech? Well, many, many years ago, when public records laws as they exist were being formulated - and it is an area that is very interesting to go back to and actually look at and see if there is any kind of legislative history or debate at the state level or the local level⁸⁸ - they were talking about why certain records should be made public.⁸⁹ I think generally, people who have looked have found there is not a whole lot of record basis that led to the determination about what information was going to be made public or not.⁹⁰

I think part of that was because that information was made public to benefit certain purposes.⁹¹ So, for example, if you were selling a piece of property or if you were registering a piece of property, that information was going to be available so other people could make sure that taxes were being assessed properly and fairly, so that the person living next-door to you with the identical lot and the same house was not paying \$200 and you were paying \$8,000. So, there is some mechanism for making sure that the government is functioning properly, that people are being treated fairly, that records were being made public.⁹²

⁸⁷ See *The Florida Star v. B.J.F.*, 491 U.S. 524, 538 (1989).

⁸⁸ See generally, S. REP. NO. 90-1815, pt. 1 (1967); S. REP. NO. 90-1815, pt. 2 (1967); H.R. REP. NO. 90-1209 (1968); Bruce D. Goldstein, *Confidentiality and Dissemination of Personal Information: an Examination of State Laws Governing Data Protection*, 41 EMORY L.J. 1185 (1992).

⁸⁹ See e.g., CAL. GOV'T CODE (2000 Supp.) §§ 6270, 6275 (West 2000).

⁹⁰ See generally, Fred H. Cate, et al., *The Right to Privacy and the Public's Right to Know: The "Central Purpose" of the Freedom of Information Act*, 46 ADMIN. L. REV. 41, 67-9 (1994).

⁹¹ See Glenn Dickinson, *Comment: The Supreme Court's Narrow Reading of the Public Interest Served By The Freedom of Information Act*, 59 U. CIN. L. REV. 191 (1990).

⁹² See Cheryl M. Sheinkopf, *Balancing Free Speech, Privacy and Open Government: Why Government Should Not Restrict the Truthful Reporting of Public Record Information*, 44 UCLA L. REV. 1567, 1575 (1997).

At that time, though, those records were not automated. Those records were buried in buildings at the state and local level. They were very hard to get to. They were on paper. They may not have been there and searchable under the name of Deirdre Mulligan. They might have been by plot number. They might have been cross-referenced by name. But while they might have been legally publicly available, they were practically undiscoverable without an awful lot of effort.⁹³

So, while we might have had a legal regime of public accessibility, for many people we had barriers - economic barriers, time barriers, distance barriers - that meant that for many of us, those private facts that might be contained in those so-called public records were not going to be widely available to many people, and that for somebody to want to expend the time and energy to actually seek out those private facts, they were going to have a real interest. And so at some level, when Paul was talking about fair information practices, there is the notion that information should be used for the purpose that it was provided.⁹⁴

There are some checks that just were part of the way in which information was held and stored, the efficiencies of data, that meant that for the most part, the people who were using those records were going to be using them for the right purpose; that it was not very easy just to randomly or casually browse information or to put it together with other information that would make it useful for other purposes.⁹⁵

So what has changed? Well, I think the *United Reporting Publishing*⁹⁶ case that you have is a very good example of what has changed. Today, information in every branch of government, whether it is the courts, or the welfare agencies, or the school records; all of that information is becoming automated,⁹⁷ and much of that information is publicly available.⁹⁸ What happens when information that is publicly available and automated becomes

⁹³ *See id.*

⁹⁴ *See id.*

⁹⁵ *See* Thomas H. Moore, *You Can't Always Get What You Want: A Look at North Carolina's Public Records Law*, 72 N.C. L. REV. 1527, 1530-31 (1994).

⁹⁶ *Los Angeles Police Dep't v. United Reporting Publ'g Corp.*, 528 U.S. 32 (1999).

⁹⁷ *See* Simitis, *supra* note 63, at 709-10 (pointing out that the privacy debate has been altered "by the intensive retrieval of personal data on virtually every employee").

⁹⁸ *Id.*

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 39

available in the private sector?⁹⁹

One of the things that we see happening is that information is no longer being used for specific purposes.¹⁰⁰ It is being combined with data from many different sources.¹⁰¹ It is being used in ways that were never contemplated by folks when they made those records public to begin with.¹⁰² They are being used, rather than to promote open government, in fact to create fairly detailed profiles about what individuals do that are culled from both data in the public sector and data in the private sector.¹⁰³

Some of that has some pretty troubling results. If you look at the *United Reporting Publishing* case,¹⁰⁴ you will see that the Los Angeles Police Department was talking about their concern that records that were being brought out into the private sector and compiled into a separate database about arrest records and arrest information, were not going to be bound by the same rules that might govern that information if it was in a public database.¹⁰⁵

I will give you some examples. Many states have purge requirements,¹⁰⁶ many states have suppression requirements,¹⁰⁷ and they have disposition requirements,¹⁰⁸ which mean a few things. If, as an individual, I am arrested, that information is not going to be available without a disposition: so, was I tried and found guilty, or was I innocent, or was there no disposition, was the case not followed through on?

In addition, if, after a certain amount of time, that information is no longer found to be useful or relevant for the criminal justice system, that information might actually just be purged right out of

⁹⁹ *Id.*, at 717-8.

¹⁰⁰ *See e.g.*, David S. Jackson, *Privacy and Ohio's Public Records Act*, 26 CAP. U. L. REV. 107, 108 (1997).

¹⁰¹ *See* Mark E. Budnitz, *Symposium: Conducting Business Over the Internet*, 49 S.C. L. REV. 847, 853-4 (Summer 1998).

¹⁰² *Id.*

¹⁰³ *See* Simitis *supra* note 63, at 729.

¹⁰⁴ *Los Angeles Police Dep't v. United Reporting Publ'g Corp.*, 528 U.S. 32 (1999) (rejecting a facial attack on CAL. GOV'T CODE § 6254(f)(3) which requires that a person requesting an arrestee's address declare that the request is being made for one of five prescribed purposes and that the address will not be used directly or indirectly to sell a product or service).

¹⁰⁵ *See* Brief for the Petitioner, *United Reporting Publ'g Corp.*, 528 U.S. 32 (1999).

¹⁰⁶ *See* Zuckman et al. MODERN COMMUNICATION LAW § 4.9 at 519-27.

¹⁰⁷ *See id.*

¹⁰⁸ *See id.*

the system, because society has an interest in making sure that I can return to society.¹⁰⁹ I have paid my societal debt, perhaps I was put away for awhile, but the notion is that there is a “re-entry into society interest” and that having that information continue to be very available is not in the individual’s interest or in society’s interest.

What happens when this information gets brought out into the private sector? Well, many of those public policy decisions that were made to balance out a variety of not just privacy interests, but also social interests, disappear because the rules that might govern the data in the criminal justice system do not flow out and control what happens in the private sector.¹¹⁰ So, information might be available that is outdated, and it might be available for use for purposes far beyond criminal justice systems.¹¹¹ So, there are some real issues that are coming up about whether or not making this information public in a grand way and in a flat way, without any thought about limiting access or limiting use, is in the public’s interest.¹¹²

What do I think about it? Eliot Spitzer talked a lot about the market.¹¹³ I think it is pretty clear. I do not know if any of you have ever tried to get a driver’s license and shopped forums: Try going to New Jersey, you really cannot, there is no market, you are dealing with the government. Many of the services that we get from the government, from driver’s licenses to health care, are not services that we can shop around for.

I think Peter brought up a very good concept, the notion of a fiduciary.¹¹⁴ The truth of the matter is that the government has not been a very good fiduciary to us in many respects. It has not applied these fair information practices when it has looked at its own handling of data at the local and state level.¹¹⁵ I think that has

¹⁰⁹ *See id.*

¹¹⁰ *See* Sheinkopf, *supra* note 92 at 1601.

¹¹¹ *Id.*

¹¹² *Id.*, at 1601-2.

¹¹³ *See supra* note 53.

¹¹⁴ *See* BLACK’S LAW DICTIONARY, 7th ed. (1999) (defining fiduciary as “One who must exercise a high standard of care in managing another’s money or property”). *See also* Restatement (Second) of Agency §13 (“An Agent is a fiduciary with respect to matters within the scope of his agency.”).

¹¹⁵ *See* Los Angeles Police Dep’t v. United Reporting Publ’g Corp., 528 U.S. 32 (1999).

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 41

put us in the place where we are today, where there are some real tensions. Automation, electronic records, electronic record-keeping, the quick and easy dissemination of information, and the incredibly inexpensive storage of that information means there is very little reason for anybody to let go of any data, forcing us to revisit issues that we did not really examine closely enough years ago.

I am going to close there.

MR. GOODALE: Thank you.

MR. EMMERT: Everybody says, "Gee, it's great to go last." Now I have, not one presentation but three, because I keep rewriting it. Instead of ten minutes, I have two.

MR. GOODALE: No, that's not right. Four.

MR. EMMERT: Okay. So we are going to go from a marginally coherent presentation to a series of non sequiturs, so bear with me.

I am with LEXIS-NEXIS. I am an attorney. I have been there for a good ten years. As the people up in your library will tell you, I have no idea how to use the service.

One of the things that you can all look forward to once you graduate from law school and you get a job, especially if you go with a corporation, is that you can count on one hand the number of cases you will read in a year. You never have the time to get much into that.

So this has been an interesting year because in the last few months I have been very interested in two Supreme Court cases, the *United Reporting*¹¹⁶ case and also *Reno v. Condon*.¹¹⁷

We were involved in an *amicus* brief¹¹⁸ in the *United Reporting Publishing*¹¹⁹ case as a member of the Individual Reference

¹¹⁶ *Id.*

¹¹⁷ See *Reno v. Condon*, 120 S.Ct. 666 (2000) (upholding the Driver's Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (1994 ed., in Supp. III), which restricts the ability of the States to disclose a driver's personal information without the driver's consent).

¹¹⁸ See Brief of the Individual Reference Services Group and the Software & Information Industry Association as *Amici Curiae* in Support of Respondent, 1999 WL 513672.

¹¹⁹ 528 U.S. 32 (1999).

Services Group (“IRSG”) and also in prepping Bruce Enis to argue the case on behalf of United Reporting, an attorney we helped identify and select.

Why did we do that? LEXIS-NEXIS has long been involved in public records issues. I’m sorry, but we’re one of those companies that kind of helped start us all down this path, because we took all that public records stuff that nobody could find and we put it on a computer. We started down that path almost thirty years ago. What was seen entirely as goodness at its inception makes people nervous now, because in the scheme of things, the scary part about what we do is that we make public information available.¹²⁰ It causes us to want to rethink and reevaluate exactly what is in the public record.¹²¹

I had an interesting conversation with a state court judge last week. One of the trends we are seeing in the state courts, as they start to make more information available electronically, is that it’s not just a matter of making the dockets available. It is also about allowing people to file pleadings electronically.¹²² Well, if you file your pleading electronically, why doesn’t the court make the pleadings available electronically? It seems logical.

So, we are talking about divorce cases where you are getting the wife’s complaint about how many nights in the last thirty days her husband beat her and graphic reports from the doctors about that. All of that information is now being made available as a matter of public record, which it has been all along but nobody really went

¹²⁰ See, e.g., Alderman, *supra* note 21 at 323 (noting that “[p]erhaps the scariest threat to privacy comes in the area [of] informational privacy.”).

¹²¹ See *id.* at 332 (commenting on the ramifications of technology on privacy and public knowledge). “The law in general, and each of us in particular, will have to make some fundamental adjustments in the way we think of personal information and electronic communication. In doing so, we will ultimately have to change our idea of what we can reasonably expect to keep private.” See *id.*

¹²² See Tracy L. Klestadt & Wayne D. Holly, *Gaining Unauthorized Access to Bankruptcy Court Electronic Filing System*, N.Y. L. J., June 3, 1998 at 1 (discussing how the U.S. Bankruptcy Court for the Southern District approved a proposal to implement an electronic filing system that allows pleadings and other documents to be electronically filed). This proposal includes administrative procedures for filing, signing and verifying documents by electronic means and a proposed electronic filing system user’s manual. These procedures mirror a pioneering electronic filing system that is currently used only in the U.S. District Court for the Northern District of Ohio, where it was implemented in January 1996. The Ohio filing system “permits pleadings and other documents to be electronically signed, verified, filed and retrieved through use of a court-issued password and registration process, via the Internet.” See *id.*

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 43

to look for it. But then the next time somebody applies for a job, somebody goes online, does a few searches and, “Oh my gosh, look at this.”

I mean, think about that in the context of the *O.J. Simpson*¹²³ case. What if all of the police reports from all of the investigation had been available online? What would people think about that case? How would you go about selecting a jury?

Now, I am not trying to make a case against what we do, because I like what we do and I think it is an important function.

One of the big concerns that I have is that the First Amendment,¹²⁴ which guarantees freedom of speech, does not draw a distinction between commercial speech and political speech or other types of protected speech.¹²⁵ That is a distinction that has been developed by the courts,¹²⁶ and there is sort of a practical issue that is driving that wedge. My concern is that as you start down a path that has repercussions that are not necessarily foreseeable, you begin to restrict access to information.¹²⁷

We are “evil” because we sell data. I have talked to legislators in a dozen states in the last year, and I cannot tell you some of the reactions I have gotten, like “Oh my gosh, you sell this?” It is like they want to run you out of their office. It is like they expect us to say, “No, no, we just give it away because we are nice guys.”

¹²³ The People of the State of California v. Orenthal James Simpson, No. B3BA097211 (unpublished).

¹²⁴ U.S. CONST. amend. I.

¹²⁵ U.S. CONST. amend. I. (The First Amendment reads: “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.”).

¹²⁶ See, e.g., *United States v. Edge Broadcasting Co.*, 509 U.S. 418, 426 (1993) (“Our decisions . . . have recognized the ‘common sense distinction between speech proposing a commercial transaction, which occurs in an area traditionally subject to government regulation, and other varieties of speech.’ The Constitution therefore affords a lesser protection to commercial speech than to other constitutionally guaranteed expression.” *Id.* at 2703 (quoting *Ohrlik v. Ohio State Bar Ass’n*, 436 U.S. 447 (1978)). See generally, JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW §§ 16.26-16.31 (4th ed. 1991).

¹²⁷ See, e.g., Tim J. McGuire, *Laws Regarding Data Privacy Should Err on the Side of Openness*, STAR TRIBUNE NEWSPAPER OF THE TWIN CITIES (MINNEAPOLIS-ST. PAUL) Jan. 16, 2000, at 23A (warning that data privacy laws create the danger of restricting access to information: “[A]ny restrictions at all start us down a slippery slope of restricted access . . . I have a deep fear that by going after public records the Legislature is going to cause serious unintended consequences.”).

The problem is that what we do is apply technology to information to make it accessible, to make it usable, to allow people to learn what is going on, whether it is about an individual, or whether it is about a government institution. In many respects, we open up information to the public.

Reporters, and the media, are one of our largest customer groups. Reporters routinely use our service to do research for stories. I will not say that reporters are exactly gatekeepers to the information that is made available to the public, but they are certainly large facilitators.

So if you go down this path and you say, “Well gee, it is commercial speech.” Why is it commercial? It is commercial because it [the information, the news] is being sold. “Therefore, you [the newspapers] should not be allowed to have access.”

Let us look at the *Reno v. Condon*¹²⁸ decision. If you have read the decision, the Court really picks up on the idea that, “Oh my gosh, the state sells this stuff.”¹²⁹ Somebody made eight million dollars last year selling – one state, I think it was Wisconsin - access to driver’s license data.¹³⁰ This is just terrible. It [these public records] is a “good in commerce.”¹³¹

Okay. Take it one step further. Let’s say the state does not sell it. Let us say the state gives it away. Is that a “good in commerce” if the state is merely making its information available to its citizens? Do you get a different result in that case if they are not selling? I do not know the answer, but I can tell you that there are

¹²⁸ 528 U.S. 141 (2000).

¹²⁹ *Id.* “The motor vehicle information which the States have historically sold is used by insurers, manufacturers, direct marketers, and others engaged in interstate commerce to contact drivers with customized solicitations. The information is also used in the stream of commerce by various public and private entities for matters related to interstate motoring. Because driver’s information is, in this context, an article of commerce, its sale or release into the interstate stream of business is sufficient to support congressional regulation.” *Id.*

¹³⁰ *See* *Travis v. Reno*, 163 F.3d 1000, 1002 (7th Cir. 1998) (noting that the Wisconsin Department of Transportation receives approximately \$8 million each year from the sale of motor vehicle information).

¹³¹ *See* *United States v. Lopez*, 514 U.S. 549, 58-59 (1995) (identifying “three broad categories of activity that Congress may regulate under its commerce power,” including “persons or things in interstate commerce”). The Court in *Condon* affirmed that drivers’ personal information is a “thing in interstate commerce” and that the sale or release of this information is therefore a proper subject for congressional regulation. *See Condon*, 120 S.Ct. at 671.

an awful lot of public records that are available today to the public and to companies like ours that we do not really buy. Some states simply say “You have to reimburse us for the cost of the tape.”

We have 28,000 data sources up right now, and the vast majority of the public records databases we have up probably cost us less than \$75 a month to update. That is because the government makes these records available to the public, not as a commercial commodity but as a public service; they simply try to recoup the cost of the tapes that they put the data on before they give it to us.

Does Congress have the right to regulate the distribution of that information? And if they can regulate the distribution to us because, heaven forbid, we are going to actually sell access, then ultimately it also means that restrictions on our users, whether they are lawyers or reporters, especially investigative reporters, that look into government activities, also restrict the ability of the public to know what their government is doing.

Now, Justice Brandeis always gets quoted on this stuff.¹³² A hundred and ten years ago, they scared the “bejesus” out of him. Privacy was down the toilet. Guys, that was 110 years ago. We are still here. We still have some semblance of privacy.¹³³ That does not mean we do not have problems, but I am not sure it is quite the crisis that it is portrayed to be. It was not the crisis then, and it is not quite the crisis now, that it may be perceived to be.¹³⁴

Brandeis was also a great believer in freedom of information and open government.¹³⁵ I think that he would be very concerned if the reaction was to unduly restrict access to information about government and its operations, because in a free and open society you have got to know what your government agencies are doing.¹³⁶

One of the things I also notice when we talk about the sale of information - I was at the newsstand this morning - is that they still charge for *The New York Times*. So, I guess that stuff is not

¹³² Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 19 (1890).

¹³³ *See id.* at 196 (“The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world . . . [B]ut modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”).

¹³⁴ *See Alderman supra* note 21.

¹³⁵ *See Warren supra* note 132.

¹³⁶ *Id.*

legal either because they charge for it. It is obviously commercial activity.

One of the other concerns that I have is this phobia that emerges when you apply technology to information. Anytime you apply technology, there is a reaction. Automobiles? Automobiles were terrible because bad guys would get automobiles and they would drive away from the scene of the crime. There was a great deal of concern about this when they made cars.¹³⁷

Well, we have got the same problem with information. The presumption is that, if we give information to the people in this room, they will misuse it and they will do bad things because they are informed.¹³⁸ I guess it depends on which side of the ledger you are on, whether you are doing a bad thing because you are informed or a good thing.

Clearly, there are people who misuse information. I think you need to question the use of the information as much as you do the fact that it is available.

One of the things I have also noticed . . . I do not want to pick on this group in particular, so I will share a deep secret here. A long time ago, between my first and second years of law school, I actually clerked for the ACLU¹³⁹ and worked on First Amendment issues. One of the things I have noticed over the last five years is that they have gone from being an adamant pro-access-to-government-records, pro-access-to-government-information, group to "Oh my gosh, we should close these records, we should limit who gets access and why, and we should limit how the information is being used."¹⁴⁰ It is an interesting switch, and you can see this same thing happening with any number of groups.¹⁴¹

¹³⁷ See generally, Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 935 (1996).

¹³⁸ See generally, ZUCKMAN ET AL., MODERN COMMUNICATION LAW § 2.2, at 184 (1999).

¹³⁹ The American Civil Liberties Union is a non-profit, public interest organization dedicated to protecting civil liberties. See generally, ACLU Briefing Paper #1, Guardian of Liberty: American Civil Liberties Union (ACLU, New York, NY), 1997, available at <http://www.aclu.org/library/pbpl.htm>. (visited Nov. 1, 2000).

¹⁴⁰ *Implementing the Driver's Privacy Protection Act Positive Notification Requirement: Hearing Before the Transportation Subcommittee of the Senate Appropriations Committee*, FDCH Political Transcripts, April 4, 2000 (testimony of Greg Nojeim, Legislative Counsel of ACLU).

¹⁴¹ See *Id.* (testimony of Ed Mierzwinski, public citizen, U.S. Public Interest Research

The problem is, you don't know whose hands ultimately this will play into. You know it is a civil liberties issue – access to information.¹⁴² I think you need to think very carefully about it before you close access off.

A couple of other quick points and I will sit down.

Attorney General Spitzer made a couple of remarks that I just kind of wanted to talk about for a second. Web sites that say that “for \$100 I can get you anybody's credit card, their birth certificate, their medical records, their cell phone records. . .” - Guys, I'm assuming people in here are smart enough to realize that these are not online services; these are private investigative services who have placed ads onto Web sites. You know, when it says “send your money here and we will mail the results to you in two to three weeks,” that it is not an online service. That is some guy working out of his garage who is calling people on the phone and lying to them to get access. It is good, old-fashioned fraud. It is not an online service. So do not go saying that all these online services are out there giving all this stuff away on the Internet. That is nonsense. It is a red herring. The problem is that these “offers” are being used to justify restrictions on legitimate online services. So do be careful about that.

Market failures? You know, there can be a difference of opinion on this. I think that when you start selling data you assume that everything is going along just fine, and then, all of a sudden, somebody wakes up one day and says “Oh my gosh, did you know that they were doing. . .or whatever?” When that realization hits, I do not think that is a market failure yet. Certainly we have identified a problem, we have identified a problem recently with several companies.¹⁴³ Image Data had a problem with driver's license photos.¹⁴⁴ We are having a problem right now with regard

Group on behalf of Ralph Nader).

¹⁴² See *Reno v ACLU*, 521 U.S. 844, 856-7 (1997).

¹⁴³ See *In re Trans Union*, FTC Docket No. 9255 (July 31, 1998), at 53, also available at <http://www.ftc.gov/os/1998/9808/d9255pub.id.pdf>.

¹⁴⁴ See Robert O' Harrow, Jr., *Firm Changes Plan to Acquire Photos; Driver's Pictures Ignited Privacy Furor*, WASH. POST, Nov. 12, 1999 at E3. (Image Data LLC is a small company that signed contracts with Colorado, Florida, and South Carolina to buy their databases of driver's license photographs to create a private network to fight identity fraud. This plan was abandoned after news reports ignited a furor among privacy advocates. In addition, Congress, as well as many state legislatures, have since proposed laws restricting access to driver information. See *id.*

48 *FORDHAM INTELL. PROP., MEDIA & ENT. L.J.* [Vol.11:21

to what we call network advertisers, the ad server companies like DoubleClick.¹⁴⁵

The question of a market failure is whether once the problem has been identified, does the market respond adequately to address the concerns that have been raised? If the answer is no, then you have got a market failure.¹⁴⁶ At that point, I think it makes sense for Congress or the legislature to step in.

But until the problem has been identified as a problem, it is not efficient for the marketplace to “correct” it.¹⁴⁷ If you are running a company, you don’t just sit there and say, “Gee, what problems could possibly happen next month?” You do a little bit of that, but you do not do a lot of it. It is not proactive, but it is not necessarily a terribly efficient way to run an economy either - to try to be so proactive that you speculate on all the things that could go wrong in the future. You wait. A problem gets identified, then you have to respond to address the problem.

If the problem is not adequately addressed - for instance, if the network advertisers do not come up with adequate rules that will in fact protect the privacy of consumers,¹⁴⁸ - then at that point I think you’ve got a market failure and at that point it would make sense for legislation to happen.¹⁴⁹ The question is whether industry is going to respond or not. I do not think we’ve got a market failure with network advertisers yet. The jury is still out on that one.

The last one, I’m sorry, I’m beating up on Mr. Spitzer, and he’s not here to defend himself. That’s probably better for me, isn’t it?

Anyway, federalism.¹⁵⁰

MS. MULLIGAN: This is on the public record.

¹⁴⁵ See, e.g., Jeri Clausing, *Privacy Advocates Fault New DoubleClick Service*, N.Y. TIMES, Feb. 15, 2000 at C2; Deborah Kong, *Consumers Fight Back as Online Tracking Spreads*, SAN JOSE MERCURY NEWS, Feb. 12, 2000 at 1.

¹⁴⁶ See Marilyn Geewax, *Laws Needed to Protect Online Privacy, FTC Says*, COX NEWS SERVICE, May 22, 2000.

¹⁴⁷ See Marilyn Geewax, *FTC Seeks Legislation for Internet Privacy; Safeguards Called Weak: Democrats Plan Bill, But Republicans Are Wary of Web Regulations*, ATLANTA JOURNAL AND CONSTITUTION, May 23, 2000 at 3D.

¹⁴⁸ See, e.g., Steve Lohr, *Seizing the Initiative on Privacy; On-Line Industry Presses Its Case for Self-Regulation*, N.Y. TIMES, Oct. 11, 1999 at C1.

¹⁴⁹ See Geewax, *supra* note 147.

¹⁵⁰ See Marcia Coyle, *New Term, Big Issues; A Still-Incomplete Docket is Relatively Slim, but The Court Is Squaring Up to Major Matters*, NAT’L. L. J., Oct. 4, 1999, at A1.

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 49

MR. EMMERT: Oh, so he can read this? Okay. Well, I will not go to New York again for awhile.

Federalism. I find it interesting, and I have got to say that, being on the industry side of this, I have been truly impressed with the way the present Administration has handled privacy issues.¹⁵¹ I think they have been extremely careful in this area.¹⁵² They have been very thoughtful and they have been very careful not to overreact. The interesting thing is that it allows the opportunity for the market to work.

I spent many hours at the Federal Trade Commission¹⁵³ a few years ago talking about industry self-regulation,¹⁵⁴ but the result was the Federal Trade Commission¹⁵⁵ allowed us to work through the issues, develop meaningful programs to try to address those issues, make sure that they had a way to enforce the programs, and then step back and see “does it work or not.” We did this with a group called the Individual Reference Services Group (“IRSG”).¹⁵⁶

The work of the IRSG has addressed a number of specific problems.¹⁵⁷ It is not a panacea. It does not address everybody’s problems. It does not address all privacy problems. It addresses a specific set of problems. But the Administration gave us the opportunity to work with them to come up with a solution that made sense, that would allow industry to function, and would still protect privacy.¹⁵⁸

¹⁵¹ See e.g., Stephen Labaton, *White House and Agency Split on Internet Privacy*, N.Y. TIMES, May 23, 2000, at C1; Norman A. Willox and Gary Clayton, *Why Privacy Can Hurt Businesses*, BUSINESS CREDIT, May 1, 1999, No. 5, Vol. 101, at 38.

¹⁵² See Jennifer Gilbert, *Ad Groups Hail Privacy Pact, Rivals Voice Fears; DoubleClick Rep Calls Agreement ‘Tough but Fair,’* ADVERTISING AGE, July 31, 2000, at 3.

¹⁵³ *Lexis-Nexis to Reveal Personal Data*, THE LEGAL INTELLIGENCER, June 25, 1997, at 4.

¹⁵⁴ See Lohr, *supra* note 148.

¹⁵⁵ See Brian Krebs, *Senators Agree to Concessions in Identity Theft Bill*, NEWSBYTES, July 12, 2000.

¹⁵⁶ *Prepared Statement of Steven M. Emmert - Director, Government and Industry Affairs, Reed Elsevier Inc. and Lexis-Nexis; President, Individual Reference Services Group - Before the Senate Judiciary Committee Subcommittee on Technology, Terrorism, and Government Information*, FEDERAL NEWS SERVICE, July 12, 2000.

¹⁵⁷ *New National Fraud Center White Paper Addresses Solutions and Challenges in Fighting E-Commerce Fraud*, BUSINESS WIRE, June 19, 2000.

¹⁵⁸ See e.g., *Online Privacy Alliance Says Web Sweeps Confirm Significant Progress in Privacy Self-regulation*, BUSINESS WIRE, May 12, 1999; Tom Lowry, *One Step Ahead of the Law: Information Brokers Agree To Self-Regulation as Governments Begin*

The Administration has been very good about this, and I find it interesting that, under the guise of federalism, the forbearance of the Administration or of Congress is being portrayed as an invitation for the states to legislate.¹⁵⁹ The message to the states has really got to be more one of “take a step back, look at what is going on.” Congress did not act, the Administration did not act, not because they do not want to, not because they feel that this is an area that the states should legislate in, rather it is because they feel that it would be better for the issue to be resolved using market approaches that ultimately get the right balance.

MR. GOODALE: Thank you.

We only have a few minutes left and we want to get the panelists to comment on my questions, or on any audience questions.

I am tempted to focus the discussion on the issue raised last, that is to say, the tension between the right of access to information and the privacy of such information. But since no court has yet held there is a First Amendment right of access - and, indeed, the *United Reporting Publishing*¹⁶⁰ case held there was no such right. I would just say, as a practical matter, that issue is academic.

Therefore, I want to turn to a practical issue. I think the hottest issue right at this moment when we are speaking, anywhere, is the issue of “opt-in” or “opt-out”.¹⁶¹ If you look at yesterday’s *New York Times*,¹⁶² there was an ad by DoubleClick - which through cookies, traces wherever you go and sells that information to its clients so that these clients can sell advertising to you. This ad says, “We are home free, don’t worry about privacy at DoubleClick because we have an “opt-out” policy.”¹⁶³ I want to ask the panel, let’s suppose that Congress passes legislation which

Cracking Down, THE CINCINNATI ENQUIRER, February 7, 1999 at E7.

¹⁵⁹ See *supra* note 53.

¹⁶⁰ 528 U.S. 32 (1999).

¹⁶¹ See, e.g., Edmund Sanders, *Why Your Bank Can (Legally) See Your Secrets; Privacy: A Lack of Specific Regulations, has Opened the Door to a Bustling Market for Consumer’s Private Financial Information*, L.A. TIMES, Nov. 7, 1999, at C1; William Safire, *Consumer Faces Growing Invasion of Privacy*, HOUSTON CHRONICLE, Sept. 24, 1999, at 38; Lisa Fickenscher, *Reporter Notebook: States Expected to Tighten Reform’s Privacy Provision*, AMERICAN BANKER, Nov. 19, 1999, at 11. See also Michele Heller, *No Privacy Laws Seen in N.Y. State this Year*, AMERICAN BANKER, Mar. 27, 2000, at 2.

¹⁶² *DoubleClick: Committed to Consumer Choice and Privacy*, N.Y. TIMES, Feb. 14, 2000, at C19.

¹⁶³ See *id.*

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 51

requires “opt-in” for entities such as DoubleClick. Is that constitutional? I just want to point out the tension would be between privacy and the First Amendment right of DoubleClick to speak.

MR. SHERMAN: First, I would like to refer the audience to *U.S. West, Inc. v. Federal Communications Commission*¹⁶⁴ where that exact issue was raised. The Tenth Circuit held that requiring “opt-in” was unconstitutional and excessive.¹⁶⁵ There was a less-restrictive method of allowing consumers to exercise their choice, namely, “opt-out”.¹⁶⁶

Now, it was a somewhat specific case. It had to do with CPNI, Customer Proprietary Network Information,¹⁶⁷ because it was information gathered from telecommunications companies.¹⁶⁸ At least in that context, and that may be appealed, I do not know whether there has been a petition for *certiorari* filed yet or not, but at least as of now, the one court, the Tenth Circuit, that has addressed it found that restriction went too far.¹⁶⁹

I think it slightly confuses the issue to place the “opt-in” versus “opt-out” debate in the DoubleClick context because there are at least allegations that DoubleClick did not follow or adhere to its own privacy policy statement,¹⁷⁰ and that is just good old-fashioned deception if that turns out to be the case.

¹⁶⁴ 182 F.3d 1224 (10th Cir. 1999).

¹⁶⁵ *See id.*

¹⁶⁶ *See id.* at 1238-39.

¹⁶⁷ *See* William J. Sill et al., *Man Your Battle Stations*, WIRELESS REVIEW, Oct. 15, 1999, at 32. CPNI is “[I]nformation about the destination of a customer’s calls, the telecommunications services to which a customer subscribes, and the frequency with which customers use these services . . . [CPNI] data allows companies to measure their competitiveness as well as to build their business plans and design new service offerings. For the last three years, carriers have found themselves in the middle of a regulatory battlefield as the FCC designs and redesigns CPNI regulations.” *See id.*

¹⁶⁸ *See* U.S. West, 182 F.3d 1224.

¹⁶⁹ *See id.*

¹⁷⁰ *See, e.g.*, Will Rodger, *Surfer Beware: Advertisers on your trail DoubleClick tracks online movements*, USA TODAY, Jan. 26, 2000, at 01B; Carol Emert, *Internet Marketer DoubleClick in Hot Water*, SAN FRANCISCO CHRONICLE, Jan. 27, 2000, at B.1; Chris O’Brien, *Lawsuit Against On-Line Ad Firm Raises New Questions on Privacy; Some Wonder Whether Policies Can Be Trusted*, CHICAGO TRIBUNE, Feb. 7, 2000, at 13; Heather Green et al., *Privacy: Outrage on the Web*, BUSINESS WEEK, Feb. 14, 2000, at 38.

So I think we have to look at it in a different framework; namely, does it violate the First Amendment to require people to take the initiative - to give affirmative consent in advance - rather than being given notice of their opportunity to say no and take that opportunity if they want to? If I can, just one last statement, because I failed to make it while I was the lead-off rather than the clean-up hitter, and that is, I believe the real issue will come down to harm when you pit the First Amendment against privacy. We know what the First Amendment stands for; it has been developed over the past 200 years. Privacy seems to be evolving.

I have been on national television shows, once because I simply quipped "privacy is a state of mind." That was it. That is all the producer had to hear. What someone considers invasive, someone else couldn't care less about.

So until we can define privacy, not only in concept, but also with respect to what harm is caused when it is invaded, for example, in the marketing context, by receiving an unwanted solicitation, we cannot shortchange the First Amendment by invoking the buzzword "privacy." Something may be one of life's little annoyances, and we all have our list of annoyances, but depending on what one's frustration quotient is, one gets very upset, mildly upset, or not upset at all. However, until we can define the harm, reliance on an argument of privacy will not overcome First Amendment rights.¹⁷¹ You've got to define the harm, at least in the marketing context. I am not talking about identity theft or threat of physical harm. I am referring to just receiving a solicitation.

MR. GOODALE: Yes. And in *U.S. West*,¹⁷² part of the problem with the case was that no such proof was made, but I think we could assume perhaps that Congress would make such a record. Your comments about DoubleClick are fair enough. Nonetheless, let's call it the "DoubleClick issue" for ease of conversation. What is making the Internet go, in some part, as a commercial entity, is the fact that there is so much information out there about individuals, and those individuals are sales targets like never before. And that's why we should call it the DoubleClick issue. Fair enough, it is technically not, but for me there is going to be an

¹⁷¹ See *supra* note 53.

¹⁷² See 120 S.Ct. 666.

awful lot of legal action out there over “opt-in”. That is why I raised it in this context.

Other comments, or anything else on this from the panelists?

MS. MULLIGAN: Actually, I wanted to respond to your question. I think if you look at the *Reno v. Condon* decision,¹⁷³ where the Court upheld Congress setting “opt-in” limits on data held by the state,¹⁷⁴ they said “we [Congress] can regulate state databases because personal information is a thing in commerce, it is a commodity in commerce.”¹⁷⁵ I think if the Supreme Court is going to say that they can regulate information in the hands of the states, where there are federalism concerns, I would find it quite probable that they would say that Congress could pass an “opt-in” limit on what private-sector companies do with data.

While I agree that the *U.S. West* decision in the Tenth Circuit¹⁷⁶ comes out another way, I also think that it is wrong-headed procedurally. I do not know if you all have read the decision, but it was a statutory interpretation question: Was the agency being true?¹⁷⁷ The agency deserves a lot of deference, under the *Chevron* doctrine,¹⁷⁸ which I am sure you are all much more familiar with than I am at this point in your careers. It is still useful, though, and the question of whether or not an “opt-out” or an “opt-in” was a permissible interpretation of the statute was a challenge to the statute on its face.¹⁷⁹ I think, in light of the *Reno v. Condon*¹⁸⁰ decision, they might be barking up the wrong tree.

MR. EMMERT: I would like to respond to that for a moment. I respectfully disagree that *Reno v. Condon*¹⁸¹ had anything to do

¹⁷³ See *Reno v. Condon*, 120 S.Ct. 666 (2000).

¹⁷⁴ See *id.*

¹⁷⁵ See *id.* at 13 (“Because drivers’ information is, in this context, an article of commerce, its sale or release into the interstate stream of business is sufficient to support congressional regulation.”).

¹⁷⁶ See *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999).

¹⁷⁷ See *id.*

¹⁷⁸ See *Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 842-44 (1984) (setting out a two-step analysis to determine what deference should be given to agency interpretations of statutes). First, if congressional intent is clear, then deference must be so given. If, however, the statute is ambiguous, then it must be determined whether the agency’s construction of the statute is reasonable. If it is found to be a reasonable construction, then the court will defer to the agency’s interpretation. See *id.*

¹⁷⁹ See *U.S. West*, 182 F.3d at 1230.

¹⁸⁰ 528 U.S. 141 (2000).

¹⁸¹ *Id.*

with the “opt-in” standard. That is a law that was just passed. It was the Shelby Amendment to the Driver’s Privacy Protection Act.¹⁸² It was passed thirty days before the oral argument in the Supreme Court case.¹⁸³ It was not even before the Court. If you read the decision, there is no discussion of “opt-in” or “opt-out” in that decision, or about the validity of it. *Reno v. Condon*¹⁸⁴ is strictly a case that was decided on the basis of the Commerce Clause,¹⁸⁵ and it is ultimately a states’ rights case under the Tenth Amendment.¹⁸⁶

MS. MULLIGAN: As a rejoinder, I agree most of us expected that case to come down as a Tenth Amendment case, but if you read the decision, I agree with you, there is not a discussion of the “opt-in”; although there is a footnote¹⁸⁷ - good Law Review style, huh? In fact, regarding the question of whether it is an “opt-out” or an “opt-in”, I think it does say that a congressional limit on state use of data and state disclosure of data passes the test.¹⁸⁸

MR. EMMERT: If it is in commerce.¹⁸⁹

MS. MULLIGAN: If the issue is if it is an “opt-in” or an “opt-out”, I don’t know if that would change the Court’s mind one way or the other because they certainly could have looked at that.

MR. GOODALE: I have got to teach *Central Hudson*¹⁹⁰ in about six minutes, and I am going to walk right upstairs and do it.

But let’s hear from you, Paul.

PROFESSOR SCHWARTZ: Just very briefly, I think in terms of the question of “opt-out” versus “opt-in”, a shift is taking place away from the full range of fair information practices, to saying

¹⁸² 18 U.S.C.A. §§ 2721 – 2725 (West Supp. 2000) (amended as of Oct. 9, 1999 and effective June 1, 2000).

¹⁸³ See *Reno v. Condon*, 120 S.Ct. 666 (2000).

¹⁸⁴ *Id.*

¹⁸⁵ U.S. CONST. art. I, §8, cl.3 (“[The Congress shall have the Power] To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes.”).

¹⁸⁶ U.S. CONST. amend. X (“The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.”).

¹⁸⁷ See *Condon*, 120 S.Ct. at 669, n.1.

¹⁸⁸ See *id.* at 670-671.

¹⁸⁹ See *id.*

¹⁹⁰ 447 U.S. 557 (1980).

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 55

that all we need is some kind of notice and then some kind of choice. I think fair information practices are intended to be more than that. The real question, it seems to me, is whether at the end of the day, we are going to have fair information practices, for example, in cyberspace?¹⁹¹ And then as a part of that broader question, we get to the question of, as Mr. Sherman has put it, choice. But I would like to keep our focus on the fact that there is a full range of fair information practices that we shouldn't let be defined down to notice and then consent.

MR. GOODALE: Why don't we take questions for the panel.

QUESTION: A question for Deirdre. In light of the Driver's Privacy Protection Act decision,¹⁹² what new restrictions would you like to see the Federal Government place on states with regard to disclosure of information that they hold?

MS. MULLIGAN: Personally, I think that this is an area where states, as custodians of their citizens' records, should take the lead. I believe states have a long tradition of dealing with citizens and being experimental laboratories. I do think that providing citizens with the full range, as Professor Schwartz said, of fair information practices when you are talking about their records is important. I think it is also true that there are always exceptions. We are talking about public records, as you know probably far better than I do, we are talking about an enormous range of records. We are talking about driver's license records, we are also talking about vital health statistic tapes, we are sometimes talking about cancer registries, and we are talking about lots of different kinds of data. I think that it is a really important exercise.

Peter Swire was talking about the fact that the Federal Government has been going through that exercise of looking at whether or not they are adhering to the Privacy Act,¹⁹³ which is the Federal Government's fair information practice law.¹⁹⁴ I think I would personally like to see it happen from the bottom up. I think this is a citizen concern. I would like to see the states look at this

¹⁹¹ See Kang, *supra* note 2, at 1194 ("Cyberspace is shorthand for the web of consumer electronics, computers, and communication networks that interconnects the world.").

¹⁹² See *Reno v. Condon*, 120 S. Ct. 666 (2000).

¹⁹³ 5 U.S.C. § 552a (1994).

¹⁹⁴ *Id.*

issue, and there are a number of states that I think are doing just that, with the assistance of their attorney generals, I believe.

QUESTION: Do you see any attempt to focus at this from the perspective of ownership of property? In other words - I don't know how it works with the government - you are effectively leasing information as a citizen to the government and you can restrict it, and regulation affects that information from a property perspective rather than a First Amendment perspective?

MR. SHERMAN: The answer is I don't think so. There have been two lawsuits where individuals have attempted to claim ownership rights in their name, and they have both been rejected.¹⁹⁵ One was *Shibley v. Time*,¹⁹⁶ back in the 1960s, and one was *Avrahami v. U.S. News & World Report*¹⁹⁷ in 1995.

QUESTIONER: And *Dwyer v. American Express*.¹⁹⁸

MR. SHERMAN: I am not sure there was a property right asserted there. That was under the Uniform Deceptive Practices Act¹⁹⁹ and invasion of privacy.²⁰⁰

QUESTIONER: Why is it not - I mean, I don't know too much about this - but why, has it been so easily dismissed?

MR. SHERMAN: I don't know the direct answer to that, other than I don't think the courts view the fact that a person's name is on an aggregate list of hundreds if not thousands, if not millions of names, means that there is any property right.

QUESTIONER: I'm talking about the information about the person, not so much the name. But, for example, information about medical information or . . .

MR. SHERMAN: What kind of property right?

¹⁹⁵ See *Shibley v. Time, Inc.*, 341 N.E.2d 337 (Ohio Ct. App. 1975); *U.S. News & World Report, Inc. v. Avrahami*, No. 95-1318, 1996, WL 1065557, at 1 (Va. Cir. Ct. June 13, 1996).

¹⁹⁶ See *Shibley v. Time, Inc.*, 341 N.E.2d 337 (Ohio Ct. App. 1975).

¹⁹⁷ *U.S. News & World Report, Inc. v. Avrahami*, No. 95-1318, 1996, WL 1065557, at 1 (Va. Cir. Ct. June 13, 1996).

¹⁹⁸ *Dwyer v. American Express Co.*, 652 N.E.2d 1351 (Ill. App. Ct. 1995).

¹⁹⁹ 815 ILL. COMP. STAT. ANN 505/1 (West 1999); See *Dwyer*, 652 N.E.2d at 1353 (discussing Illinois' Consumer Fraud and Deceptive Business Practices Act).

²⁰⁰ See *Dwyer*, 652 N.E.2d at 1353.

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 57

QUESTIONER: Somebody was talking about things about cancer, I think you were saying that or. . .

MR. SHERMAN: I'm trying to figure out what kind of property is that?

QUESTIONER: I don't know. I'm asking.

MR. SHERMAN: Maybe it isn't.

PROFESSOR SCHWARTZ: There is a lot of scholarship looking into this area recently, looking at it from the perspective of real property and looking at it from the perspective of intellectual property.

The answer in the 1960s, and maybe up until the 1970s, as provided by Judge Posner, for example, in the *Georgia Law Review*,²⁰¹ was that the reason not to look at personal data as property was transaction costs. It was viewed as too expensive to aggregate and distribute personal property rights in personal data.²⁰²

Well, in the Information Age and the Internet Age, that is no longer entirely correct. Information technology has lowered the transaction costs associated with property interests in personal data. So many scholars are viewing privacy as an intellectual property issue or a property issue. But a counter-attack is also appearing in the literature in this area that questions the commodification of personal data.

QUESTIONER: Well, it has utility in the sense that it changes the regulatory format in which you then talk about it.

PROFESSOR SCHWARTZ: Absolutely. But what some scholars have been saying is it may not advance the debate very far to put it, for example, in the intellectual property category.²⁰³ Some of the leading intellectual property scholars in the country

²⁰¹ Richard A. Posner, *John A. Sibley Lecture: The Right to Privacy*, 12 GA. L. REV. 393 (1978).

²⁰² *See id.* at 398-99.

²⁰³ *See generally, Symposium, Warren and Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8 (1999) (urging that while many traditional arguments advanced against including privacy interests under the intellectual property umbrella are unpersuasive today, there remains a large gap between the protection that intellectual property can provide and that which privacy advocates seek.).

58 *FORDHAM INTELL. PROP., MEDIA & ENT. L.J.* [Vol.11:21

have said, copyright is traditionally for a limited period of time,²⁰⁴ although Congress has kept moving that period of time out.²⁰⁵ Should privacy-as-property last forever? Should privacy, like copyright, continue after your death? And what do we do with the fair use notions? But there is tremendous intellectual ferment taking place about privacy-as-property.

MR. SUSSMAN: On behalf of the *Journal*, I would like to thank our panelists. We will now take a five-minute break and then return for the second panel.

²⁰⁴ 17 U.S.C.A. § 302 (Supp. 1998) (“Copyright in a work . . . endures for a term consisting of the life of the author and 70 years after the author’s death.”).

²⁰⁵ *Id.* (Amended in 1998 from fifty to seventy years after the author’s death.).