

## Panel II: The Conflict Between Commercial Speech and Legislation Governing the Commercialization of Private Sector Data

Moderator: Professor Joel Reidenberg<sup>\*</sup>  
Panelists: Jennifer Barrett<sup>\*\*</sup>  
Evan Hendricks<sup>\*\*\*</sup>  
Solveig Singleton<sup>\*\*\*\*</sup>  
David Sobel<sup>\*\*\*\*\*</sup>

PROFESSOR REIDENBERG: I am Joel Reidenberg and am delighted to moderate our second panel this afternoon.

Many interesting ideas were raised by our keynote speakers and by the previous panel that I hope we will have a chance to discuss and argue.

Our topic for this panel is the conflict between commercial speech and legislation governing the commercialization of data held by the private sector. I would like to spend a few minutes setting the stage for each of our panelists and raise three provocative comments on self-regulation, legislation, and First Amendment commercial speech.

First, we heard earlier this afternoon from Attorney General Spitzer and Peter Swire, who are each doing excellent work in their public service. They each explained the case for a market approach and explained why in New York and in the Federal Government the emphasis has been on the market approach. I believe, on the other hand, that the self-regulation approach is a

---

<sup>\*</sup> Professor of Law and Director of the Graduate Program, Fordham University School of Law, New York, NY. Dartmouth College, A.B. 1983; Columbia University School of Law, J.D. 1986; Universite de Paris I (Pantheon-Sorbonne), D.E.A. 1987.

<sup>\*\*</sup> Company Leader for Information Practices and Government Affairs, Axiom Corporation. University of Texas, B.S. 1966.

<sup>\*\*\*</sup> Editor/Publisher, Privacy Times. Columbia College, A.B. 1979.

<sup>\*\*\*\*</sup> Director of Information Studies, Cato Institute. Reed College, B.A. 1987; Cornell Law School, J.D. 1992.

<sup>\*\*\*\*\*</sup> General Counsel, Electronic Privacy Information Center. University of Michigan, B.A. 1976; University of Florida College of Law, J.D. 1979.

myopic vision for effective privacy protection in the United States.<sup>1</sup> As we have heard, the increasing use of technology in data gathering undermines our expectations of protection for privacy. Indeed, I think we see that privacy is different. Privacy is a political issue.<sup>2</sup> It is a political right,<sup>3</sup> what Paul Schwartz has called a “constitutive right.”<sup>4</sup> Privacy is something that is different from those things we generally associate with marketplace sales. In that context, I would certainly argue that legislation setting forth fair information practice standards is a necessity.<sup>5</sup>

Well, that brings us front and center to the question of today’s panel, which is: “If we have legislation providing substantive standards for privacy, what does that mean for commercial speech rights?”

My second provocative comment is that the issue is not about speech at all and the First Amendment simply should not apply in this area. We see in two recent Supreme Court cases, *Los Angeles Police Department v. United Reporting*<sup>6</sup> and *Reno v. Condon*,<sup>7</sup> an articulation that the sale of personal information is not being treated as speech. In *Condon*, the court described the personal information and drivers’ records as a “thing in commerce,” while

---

<sup>1</sup> See Joel R. Reidenberg, *Restoring Americans’ Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 771 (1999) (“[T]he theory of self-regulation has normative flaws and . . . public experience shows the failure of industry to implement fair information practices. Together the flawed theory and data scandals demonstrate the sophistry of U.S. policy.”).

<sup>2</sup> See, e.g., Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497 (1995) (“The Information Superhighway . . . and the emerging Global Information Infrastructure place standards for the treatment of personal information at the forefront of policy discussions among . . . governments . . .”).

<sup>3</sup> See Reidenberg, *supra* note 1, at 787 (“In a democratic state, privacy is and remains a basic right of citizens.”) (citations omitted).

<sup>4</sup> See Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1664 (1999) (“[R]ather than establishing individual privacy-control, constitutive privacy seeks to create boundaries about personal information to help the individual and define terms of life within the community.” (citing Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CAL. L. REV. 957, 985 (1989))).

<sup>5</sup> See Reidenberg, *supra* note 1, at 771 (recommending “a framework privacy law in the United States modeled on the O.E.C.D guidelines that includes a safe harbor provision for policies and technologies and that creates a U.S. Information Privacy Commission to assure the balance between citizens’ privacy, industry needs, and global competitiveness”).

<sup>6</sup> *Los Angeles Police Dep’t v. United Reporting Publ’g Corp.*, 528 U.S. 32 (1999).

<sup>7</sup> *Reno v. Condon*, 120 S.Ct. 666 (2000).

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 61

the court allowed a clear delineation of the purpose for disclosure of arrest records in *United Reporting*. I would argue that the sale of personal information in these contexts is actually quite different from any of the familiar commercial speech cases, because in each of the classic commercial speech cases, the Supreme Court ruled on restrictions affecting the solicitation itself, that is the advertisement.<sup>8</sup> That is not what we are talking about in the marketing and trafficking of personal information.

My third provocative point that I will leave for the panelists is, even if you disagree with me on the argument that the sale of personal information is not within the commercial speech doctrine, and I suspect most people will, then the *Central Hudson* test can readily be satisfied.<sup>9</sup> There is clearly a strong case that privacy legislation in the United States is a compelling state interest, and such legislation can easily be tailored to satisfy the *Central Hudson* balancing.<sup>10</sup>

So those are my three provocative comments.

Our panelists today, I think in the context of their comments, will be touching on different issues related to these points.

We will start with Jennifer Barrett, who is the Company Leader for Information Practices and Government Affairs at Acxiom. Acxiom is probably one of the largest sellers of personal information in the United States. They provide substantial marketing database management services and data warehouse services, for many companies in the United States.<sup>11</sup>

---

<sup>8</sup> See, e.g., 44 *Liquormart, Inc. v. Rhode Island*, 517 U.S. 484 (1996) (challenging state statute prohibiting advertising of liquor prices); *Fla. Bar v. Went For It, Inc.*, 515 U.S. 618 (1995) (challenging Florida Bar rules which prohibit lawyers from sending targeted direct mail to solicit personal injury or wrongful death clients within thirty days of accident); *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980) (challenging regulation which banned promotional advertising by electric utility).

<sup>9</sup> *Central Hudson*, 447 U.S. at 566. The Court's four-part test used to judge government restrictions of commercial speech is: 1) Whether the expression is lawful and non-misleading; 2) Whether the government has a substantial state interest in regulating the speech; 3) Whether the regulation directly and materially advances that interest; and 4) Whether the regulation is no more extensive than necessary to serve that interest. *Id.*

<sup>10</sup> See *id.*

<sup>11</sup> See *Acxiom Corporation Overview*, at <http://www.acxiom.com/about/about-about.asp> (last visited Nov. 1, 2000).

Then we will hear from Evan Hendricks, who is the Editor and Publisher of *Privacy Times*<sup>12</sup> and a very well-known privacy advocate in the United States.

Following Evan, we will hear from Solveig Singleton, who is the Director of Information Studies at the Cato Institute,<sup>13</sup> a think tank based here in New York that, unless I am wrong, has a very libertarian bent in its philosophy and the studies they do.

And then, finally, we will hear from David Sobel, who is the General Counsel for the Electronic Privacy Information Center, known as EPIC.<sup>14</sup> EPIC has been at the forefront of privacy litigation and the privacy policy debate in Washington.

With that, I will turn the podium over to Jennifer.

MS. BARRETT: Thank you. It is a pleasure to be here.

I should probably frame these remarks that I am about to make by saying that I may be the only one in the audience who is not a lawyer, although I do have a legal team back at the office that keeps me on the straight and narrow. But what I do have, and what I think I can bring to the discussion today, is twenty-five years of practical experience in the industry working with not only a company that provides personal information, but also many, many customers who manage personal information of their own.

With regards to the question that was posed today: “Whether greater legislation governing the commercialization of data is needed; and, if so, in what form, and so on?” I would like to begin by saying that I think there are four simple points that need to be made and studied before you can answer the question.

The first point is, what laws are already in place, and which of those seem to be most effective?

Number two, what industry self-regulation exists and appears to be working?

Number three, what benefits does the consumer enjoy from the free flow of information?

---

<sup>12</sup> See *About Us*, at [http://www.privacytimes.com/index\\_about.htm](http://www.privacytimes.com/index_about.htm) (last visited Nov. 1, 2000).

<sup>13</sup> See *About the Cato Institute*, at <http://www.cato.org/about/about.html> (last visited Nov. 1, 2000).

<sup>14</sup> See *About EPIC*, at <http://www.epic.org/#about> (last visited Nov. 1, 2000).

## 2000] SYMPOSIUM - DATA PRIVACY &amp; THE FIRST AMENDMENT 63

And fourth, what, and how frequent are the abuses, damages, injuries, or consequences from that free flow?

Now, as we have discussed today in numerous examples, we have a wide variety of federal and a growing number of state laws governing these areas: the Fair Credit Reporting Act,<sup>15</sup> the Online Children's Privacy Protection Act,<sup>16</sup> the Deceptive Mail Enforcement Act,<sup>17</sup> the Financial Services Modernization Act,<sup>18</sup> telemarketing sales rules - the list goes on and on and on. At the state level, I think we are up to ten states now, or maybe twelve as of this writing, that have "do not call" solicitation laws on the books.<sup>19</sup> We also have a variety of other state legislative issues dealing with specific kinds of industry data.

Now, as we all know, the law does not prevent the misuse or abuse of data from occurring. However, I urge anyone who is considering legislation, to review current laws and again look at what is working and what is not, because this provides valuable insight into the practical implementation of what we hope would become legal, or from a constitutional standpoint, permissible.

For example, let's take a look at what appears to be a rather simple problem to solve, and that is the desire of consumers to not receive unsolicited telemarketing calls during the dinner hour. Now, we have the Telemarketing Sales Rule that governs telemarketing at the federal level,<sup>20</sup> we have dozens of states that have "do not call" lists,<sup>21</sup> and yet we are still getting, myself included, telemarketing calls.

The Federal Trade Commission has said, "we have a problem," so they have formed a task force to study whether the law in its current form is effective or not.<sup>22</sup> I think what you will find when their study is complete is that there are two fundamental

---

<sup>15</sup> 15 U.S.C. § 1681 (1994).

<sup>16</sup> 15 U.S.C. §§ 6501-6505 (1999).

<sup>17</sup> Deceptive Mail Prevention and Enforcement Act, 39 U.S.C. §§ 3016-17 (1994).

<sup>18</sup> Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

<sup>19</sup> See, e.g., ARIZ. REV. STAT. ANN. § 44-1278 (West 1999), NEB. REV. STAT. § 86-1212(2) (1999), 2000 ME. LEGIS. SERV. Ch. 694 (West), R.I. GEN. LAWS § 5-61-3.5(a) (1999), HAW. REV. STAT. ANN. § 481P-4(11) (Michie 1999).

<sup>20</sup> 16 C.F.R. § 310 (1999).

<sup>21</sup> See *supra*, note 19.

<sup>22</sup> See *FTC Seeking Public Comments on Telemarketing Sales Rule*, available at <http://www.ftc.gov/opa/2000/02/tsr.htm> (last visited Nov. 1, 2000).

components to the law as it is written which make it ineffective. These components may make the law constitutional, but ineffective, and therefore the law does not solve the problem it was intended to address.

First, most consumers are not aware of the Telemarketing Sales Rule;<sup>23</sup> therefore, they do not even know to invoke it. Second, there are a number of exclusions<sup>24</sup> and, unfortunately, a lot of the excluded categories are those that are the most abused.

This is another example, as we heard from our keynote speakers, where we have an issue of states' rights versus federal rights. I think it is going to be an issue that will continue to arise as we move forward with this discussion, and with possible legislation.

From an industry standpoint, we would certainly prefer to have a national "do not call" list rather than fifty different states with fifty different sets of slightly different rules. I think you would find that the industry would be rather receptive to that, even though it may not practically be something that we can hope for.

Now, in addition to reviewing the current laws and understanding what is working and what is not, it is also important to look at self-regulation. We have talked quite a bit about that today. There are a rapidly growing number of initiatives dealing with a variety of ethical business practices. There are a number of coalitions that are being formed, where there is not an industry association in place, to take on this specific issue, as was discussed with the network advertisers.<sup>25</sup>

Now, I do not know that I want to go back and dissect the history of self-regulation. I think it is much like the history of the Internet, and is somewhat immaterial at this point in time. What we need to do is look at what is happening now and how we are going forward.

Steve Emmert brought up the Individual Reference Services Group ("IRSG"), which is a coalition that was formed in 1997 to deal with personal information that was used for look-up identification-and-verification services.<sup>26</sup> It has been a very

---

<sup>23</sup> 16 C.F.R. § 310 (1999).

<sup>24</sup> See 16 C.F.R. § 310.6 (1999).

<sup>25</sup> See *infra* notes 26 – 30 and accompanying text.

<sup>26</sup> Individual Reference Service Group ("IRSG") is a coalition of fourteen leading

effective group and has had very, very positive results.

The Direct Marketing Association (“DMA”) has instituted its Privacy Promise and made it a condition of membership as of last year,<sup>27</sup> and has actually kicked a few members out for violating the guidelines that promote the concepts of notice and choice.<sup>28</sup>

The Online Privacy Alliance was a group of large companies involved in specific online activities that came together two short years ago to try and set some standards.<sup>29</sup> The group was a driving influence behind the statistics that Peter Swire shared with you, driving privacy policies from the fifteen or sixteen percent level in 1997 to the over-sixty-five percent level last year.<sup>30</sup>

I think, as we have talked about the network advertisers, it remains to be seen what the policy will be, but they have certainly responded quickly and with a great deal of commitment to develop some industry self-regulation.

A central theme throughout all of this, which has been brought up in the framing comments from Bob in our previous panel,<sup>31</sup> is that there are fundamental concepts of notice, choice, security, and data accuracy, that continue to be very consistent and prevalent. I think if you look at these principles and these concepts, you will

---

information industry companies who have pledged to adopt self-regulatory principles governing the dissemination and use of personal data. See Individual Reference Services Group, available at <http://www.irsg.org> (last visited Nov. 1, 2000); see also Individual Reference Services Group, *White Paper* (outlining the benefits of individual reference services), available at [http://www.irsg.org/html/white\\_paper.htm](http://www.irsg.org/html/white_paper.htm) (last visited Nov. 1, 2000) [hereinafter IRSG White Paper].

<sup>27</sup> The Privacy Promise is a public assurance that all members of the DMA will follow certain specific practices to protect consumer privacy. See *Privacy Promise Member Compliance Guide*, available at <http://www.the-dma.org/library/privacy/privacypromise.shtml> (last visited Nov. 1, 2000).

<sup>28</sup> See DMA, *Privacy Promise Member Compliance Guide, Step 2* (stating that a DMA member that does not follow the Promise may be subject to “censure, suspension, or expulsion from the DMA, and publicity to that effect”), available at <http://www.the-dma.org/library/privacy/privacypromise2.shtml> (last visited Nov. 1, 2000).

<sup>29</sup> See ONLINE PRIVACY ALLIANCE, *Guidelines for Online Privacy Policies*, available at <http://www.privacyalliance.org/resources/ppguidelines.shtml> (last visited Nov. 1, 2000). These guidelines include the adoption and implementation of a privacy policy, notice and disclosure, choice and consent, data security, and data quality and access. *Id.*

<sup>30</sup> See *Online Privacy Alliance Says Web Sweeps Confirm Significant Progress in Privacy Self-Regulation*, at <http://www.privacyalliance.org/news/05121999.shtml> (May 12, 1999); *Online Privacy Alliance Encourages Businesses to Post Privacy Policies*, (reporting on OPA’s efforts to increase the number of e-commerce companies posting privacy policies), at <http://www.privacyalliance.org/news/02021999.shtml> (Feb. 2, 1999).

<sup>31</sup> See *infra* pp. 20-28.

see them played out, maybe in slightly different forms, within industry guidelines, but the consistency of the principles is there.

So, I think it is fair to say that yes, there is a conflict between privacy and commercial free speech, and it is having a major impact on industry. It is focusing the attention where the attention needs to be focused, and, from our perspective, it appears to be working very well.

Now let us move on to discuss the concept of consumer benefit. We tend to focus most of our energies on the damage done to the consumer, not on the benefits they enjoy from the commercialization of data.<sup>32</sup> This is an area that is probably the least well-documented, and certainly the least publicized, of all of the issues surrounding the commercialization of data. I can generally place these benefits in the following categories: lower prices through accurate customer information; more effective marketing; a better understanding of customer needs and wants; reduced debt through better screening of potentially bad or high-risk customers; and more effective collection efforts.<sup>33</sup>

Another benefit is that commercial data collection allows producers to offer products and services to those who would either not have the opportunity to receive them or to those to whom products and services would not be easily available.<sup>34</sup> This includes the handicapped and the elderly especially.<sup>35</sup> Next, It saves consumers time and money.<sup>36</sup> Without information to verify some of the activities that go on, the processes that we have taken for granted do not occur as speedily as they would, and time is money to the consumer. Furthermore, Law enforcement is greatly assisted in locating fugitives, missing children, witnesses and collecting delinquent child support by the commercialization of

---

<sup>32</sup> See F.T.C., Staff Rep., *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, available at <http://www.ftc.gov/reports/privacy/privacy1.htm> (last visited Nov. 1, 2000).

<sup>33</sup> See ACXIAM White Paper, *Beyond Consumer Privacy to Consumer Advocacy*, available at <http://www.acxiom.com/whitepapers/wp-16.htm> (last visited Nov. 1, 2000) [hereinafter Acxiom White Paper].

<sup>34</sup> See Solveig Singleton, *Privacy as Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector*, CATO POLICY ANALYSIS No. 295, Jan. 22, 1998 (arguing that poorly targeted direct mail "lead[s] to fewer, more expensive options for those who shop at home").

<sup>35</sup> See *id.*

<sup>36</sup> See *id.*

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 67

data.<sup>37</sup> Finally, the very information that some say creates fraudulent situations is the same information that we use to verify and to prevent, or at least reduce, the occurrence of fraud.<sup>38</sup>

Now, it should be mentioned that the collection and storage of personal information about consumers is a means that businesses use to improve the relationship they have with these very consumers.<sup>39</sup> If they are doing things with the data that the consumer does not understand or the consumer does not like, then they do not have a very happy customer.<sup>40</sup> So as we have discussed in most of the speeches, the motivation to listen to the consumer's desires and to stop a practice that consumers are uncomfortable with, is very strong.

Finally, before we answer the question of whether more legislation is needed, I want to ask and talk about the issue of damages, injuries, or any other consequences that the consumers might experience from the free flow of information.

It is always frustrating to a responsible information company, such as ours, to read the sensationalist coverage in the press, which is very one-sided, about the potential damages or the potential harm that can come from the free flow of information, and which never goes on to discuss or to mention the benefits that the consumer receives from this free-flow.

The reality of the situation is that it costs a lot of money to store data. It costs a lot of money to keep it current, and if you do not keep it current, it has no long-term value. Businesses are not interested in collecting information or paying for information from companies, such as ours, that they do not have the opportunity to turn into some benefit, either in the relationship with these customers or in driving their own costs down. Now, technological advances have reduced the cost of the collection and storage of data, but it is still very real and not an insignificant portion of anyone's information technology ("IT") budget. Acxiom and our

---

<sup>37</sup> See IRSG White Paper, available at <http://www.irsg.org/html/whitepaper.htm> (last visited Nov. 1, 2000).

<sup>38</sup> See *id.*

<sup>39</sup> See Acxiom White Paper, *supra* note 33.

<sup>40</sup> See *id.* ("By addressing the shopper's privacy concerns immediately and completely – and letting her know that she has the right to correct or delete any erroneous data – the company is able to convert a potentially negative situation into a positive one and solidify its relationship with the consumer.").

customers do extensive cost/benefit analysis to determine whether or not the need to capture end-use data is really there before we embark on such activities. It is never done in a haphazard or whimsical manner.

Finally, every study that I have seen in the last six months says that consumers, in addition to wanting their privacy, also want personalization;<sup>41</sup> they want to be treated not as a mass market, but as an individual.<sup>42</sup> The challenge is, how do we do both?

So what does this all mean to the question: "Is more legislation needed?" We cannot deny that personal information about individuals is out in the marketplace, but if you look at how our economy is performing in the new age and the increasing dependency on the availability of information, one could argue that the benefits are tremendous, particularly when you compare these benefits to other countries where the uses of information are much more restricted.

Now, I would like to talk about the real harm. Are consumers being flooded with unwanted, offensive e-mail, or is it an occasional issue, and driven more so by the fact that they visit a chat room, and by the fact that some piece of information was transferred about them? Are consumers having their identities stolen by tracking what they do on Web sites? Are consumers being stalked, any more than they were before, by information that is available out on the Net?

I think you will find the answer to those questions is that we do not have documented proof that this is what is driving, if there is an increase, some of those activities. And if the documentation

---

<sup>41</sup> See PRIVACY & AMERICAN BUSINESS, *Personalization Marketing and Privacy on the Net: What Consumers Want* (revealing that a majority of Internet users want information that is tailored to their needs and are willing to provide information about their preferences in exchange for personalization), available at <http://www.pandab.org/doubleclicktoc.html> (Nov. 1999). Sponsorship for the survey was provided by DoubleClick, Inc. See *id.*, Executive Summary. See also IBM GLOBAL SERVICES, *IBM Multi-National Consumer Privacy Survey* (finding that in order to successfully conduct business on the Internet, companies must provide personalized service and take proactive steps to ensure privacy), available at [http://www.ibm.com/services/files/privacy\\_survey\\_oct991.pdf](http://www.ibm.com/services/files/privacy_survey_oct991.pdf) (Oct. 1999).

<sup>42</sup> See IBM GLOBAL SERVICES, *IBM Multi-National Consumer Privacy Survey* (finding that companies must provide personalized service and take proactive steps to ensure privacy in order to successfully conduct business on the Internet), available at [http://www.ibm.com/services/files/privacy\\_survey\\_oct991.pdf](http://www.ibm.com/services/files/privacy_survey_oct991.pdf) (Oct. 1999).

exists, I think you will find that the industry, regardless of what segment of it you are in, will respond positively and say, "yes, if the abuses are there, let's do something about it." I think the Children's Online Privacy Protection Act was a very good example of where regulators, legislators, and the industry came together to work out a piece of legislation.<sup>43</sup>

However, if the need, as it is sometimes called, is to protect where there is no real evidence of abuse, only the possibility of abuse, then I would submit that it is prudent for us to wait a little longer. Give businesses a little time to decide what information is important to them, give consumers the time to vote with their pocketbooks by going to the companies who use the practices they trust, and give technology the time to put more choices and controls in the hands of consumers. Give us choices to block those "cookies" if we so choose, to filter out unwanted e-mail if that is what offends us, or to surf the Net anonymously if we really want to take it to that extent. Give consumers the chance to realize the unrealized benefits that this free flow of information will surely bring.

Finally, I would like to just make a comment, because everyone else has, on this issue of "opt-in" versus "opt-out," because it is certainly one that is very heated today.

The historical figures, and they are holding fairly consistent, show us that between five and fifteen percent of the population "opts-out" when given the chance, and between five and fifteen percent of the population "opts-in" when given the chance.<sup>44</sup> Now, what does that tell us about the other seventy to ninety percent? They either do not care, they do not understand, or they do not have the time to deal with the question.

I suggest that, in the absence of hard factual examples of abuse, we should not take away the benefits that seventy to ninety percent are enjoying, and it should not be done under the guise of protecting the consumer from themselves. However, in the specific instances where highly sensitive information, as has been talked about earlier - medical, financial, and so forth - do exist and known abuses are occurring, then "opt-in" should be considered, and is being considered. This was one of the practices that the

---

<sup>43</sup> 15 U.S.C. §§ 6501-05 (1999).

<sup>44</sup> On file with author.

DMA put in place before the government even came out with regulations in the area of medical records.

In conclusion, I would just like to say, to answer the question that was posed to us as panelists, I do not think that we need more legislation now, except in very carefully selected areas where inappropriate use of information can be clearly documented and is repetitive.

What we do need is for all involved - businesses, legislators, regulators, and the consumers - to keep a close focus on the privacy principles that the industries have adopted thus far - notice and disclosure, choice, security, access, and quality - and use them to help continue to refine the business practices that we see work and to identify and change those that we see do not work.

In addition, we should be more aggressive in educating the consumers and making sure they understand the choices that exist for them. I believe a strong commitment to these principles will ensure that the consumer enjoys the maximum degree of safety and protection, while also providing the maximum benefit possible from a healthy information-based economy.

Thank you.

MR. HENDRICKS: Thank you, Joel. Thanks for the invitation. A quick salute to the excellent work that the *Fordham Intellectual Property Journal* has put into this. It is a top quality program, having Joel Reidenberg, Paul Schwartz, and Peter Swire, truly the leading professors in North America on this issue, and internationally respected. And I think I have told you before, Joel, that when I grow up, I want to be a professor too.

A few months ago, I actually wrote to Acxiom. I do not know if you are in charge of the system, but it worked very well. I immediately got the brochure back. It was very clear and very easy. I have not bothered to "opt-out" yet, but it was nice to see that your system worked. So I wanted to say something nice.

MS. BARRETT: Thank you.

MR. HENDRICKS: I was more interested in the article in the *Washington Post* recently, which discussed a system which I

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 71

believe Acxiom is associated with.<sup>45</sup> Anytime you call an 800 number you cannot use blocking technology like you can with a local phone number, where you can use \*67 or you have your line blocked. The 800 numbers are part of ANI<sup>46</sup>, which is considered a different brain of the beast, so your blocking does not work there, and automatic number identification will capture your number. This system, if I remember correctly, which Acxiom is a part of, has captured and stored some 20 million unlisted phone numbers in the Acxiom database.

A *Washington Post* reporter, Robert O'Harrow, quoted Acxiom as stating its belief that if you called an 800 number of a commercial enterprise that was part of their network, you were basically "opting-in" and agreeing to have your unlisted phone number go into Acxiom's database, where it could later be resold.<sup>47</sup> I do not agree with that point of view, but it is an issue we might be able to discuss later.

I am interested in history. You heard about LEXIS-NEXIS<sup>48</sup> and you heard about the IRSG Principles.<sup>49</sup> So much of what industry is doing is to avoid legal rights for individuals – they are advocating against legislation and instead for voluntary "opt-outs." What happened with LEXIS-NEXIS is that, all of a sudden, there was almost a disinformation campaign on the Internet, where some people were lighting up the Internet with another version of "hack attacks."<sup>50</sup> Back in 1997, I think, they were saying: "LEXIS is selling your social security numbers all over the place; they have got this data on you; it is the P-track system." Some of what they were saying about LEXIS-NEXIS was not accurate. I think some 40,000 people "opted out," or contacted LEXIS-NEXIS with e-mail saying, "get me out of your system," and congressmen were actually starting to get mail from constituents. That is what

---

<sup>45</sup> Robert O'Harrow Jr., *A Hidden Toll On Free Calls: Lost Privacy; Not Even Unlisted Numbers Protected From Marketers*, WASH. POST, Dec. 19, 1999, at A1.

<sup>46</sup> Automatic Number Identification. Automatic Number Identification is a function by which the directory number of a calling unit is automatically obtained. This function allows businesses to compile and store lists of consumers' telephone numbers.

<sup>47</sup> See O'Harrow, *supra* note 45.

<sup>48</sup> See *infra* p. 41.

<sup>49</sup> See *supra* note 26 and accompanying text.

<sup>50</sup> See Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 551, 564 (1999); Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 221 n.312 (1999).

brought together the IRSG Group, so they could create a voluntary program approved by the FTC and thereby avoid legislation.

LEXIS-NEXIS was very upset about this situation because they were being inaccurately portrayed by bad information going through electronic information systems. I agree that is wrong, but at least LEXIS-NEXIS now knows how consumers feel, because that is what is happening with a lot of the information systems that have information on consumers.

The issue today is First Amendment and privacy.

Let me tell you a little bit about myself. My name is Evan Hendricks. I write *The Privacy Times*. It is a newsletter. We have a Web site at [privacytimes.com](http://privacytimes.com). In January we started our twentieth year. So I am sort of the “lonely pamphleteer” trumpeted by the Supreme Court.<sup>51</sup> Because of the First Amendment, I exist, and so, I am an ardent First Amendment advocate.

Part of my newsletter covers the Freedom of Information Act (“FOIA”).<sup>52</sup> In 1982, when the Reagan Administration wanted to gut the Freedom of Information Act,<sup>53</sup> I was on the front lines with many of the public interest groups documenting what the public had learned through the Freedom of Information Act. So I also am very much an open government advocate.

And so, as a beneficiary of the First Amendment, as someone who has followed these debates, I feel I can say with a certain amount of authority and certainty that most of the arguments about the First Amendment clashing with privacy, or that because of the First Amendment we cannot pass laws to protect the privacy of personal data, are bogus. So, Joel, your opening remarks to me were not very controversial; they were common sense.

So I draw the line that there is no First Amendment right to traffic in your personal data. As Deirdre said, you have a personal right to say something to somebody; you have a personal right to mail something to somebody; to publish something and pass it out

---

<sup>51</sup> See *Branzburg v. Hayes*, 408 U.S. 665, 704 (1972) (stating that “liberty of the press is the right of the lonely pamphleteer who uses carbon paper or a mimeograph just as much as of the large metropolitan publisher who utilizes the latest photocomposition methods”).

<sup>52</sup> 5 U.S.C. § 552 (1994).

<sup>53</sup> See Andy Blum, *FOIA's Use Gets Harder Over Time*, NAT'L L.J., July 20, 1992, at 36.

in the street; you have the First Amendment right to communicate in any way that you want.<sup>54</sup>

For instance, there was a case where a woman needed to call one of her colleagues at home, and she calls, and this voice quietly answers the phone, much like our discussions this afternoon. The woman says, "Hello, is your mother there?" The child's voice says, "Yes, but she is very busy right now." Then she said, "Well, is your father there?" "Yes, he is very busy too." Then she said, "Is there any other adult I can speak to in the house." "The police are here but they are very busy too." Finally she said, "Look, your Mom and your Dad are busy, the police are there, they are all too busy to come to the phone. What are they doing?" "They are looking for me."

I feel that these are the sort of structures or systems that we are building now between Internet commerce and the government to put consumers under surveillance so that they can know you better and serve you better or to administer their government programs better. But the reaction of individuals is very much like the child hiding in the closet. Already, we are seeing individual countermeasures, people giving false data. And so, as I said, to protect your privacy in a situation where you do not have legal rights, you almost have to act like an undercover operative.

Now, we already have privacy law. We have the Video Rental Law.<sup>55</sup> You might remember Judge Bork, who was nominated for the Supreme Court.<sup>56</sup> Our *City Paper* reporter (the *City Paper* is the give-away paper in D.C.) was standing at a video counter and talking with the clerk, and the clerk said, "Hey, Judge Bork, the guy who is getting all this fire through the nomination, gets his videos here." The reporter said, "Well gosh, can you show me what he has taken out?" The clerk gave him a list of what Judge Bork had rented, and he wrote an article about how Judge Bork likes B movies, detective movies, et cetera<sup>57</sup>—none of the themes from the Clarence Thomas hearings.

---

<sup>54</sup> See *infra* p. 33.

<sup>55</sup> Video Privacy Protection Act, 18 U.S.C. § 2710 (1994).

<sup>56</sup> See David Johnston, *Reagan Hints at Bork Nomination Strategy*, N.Y. TIMES, July 5, 1987, at A14.

<sup>57</sup> See Berman & Mulligan, *supra* note 50, at 578 n.76.

But this story hit close to home in Congress and they moved quickly to enact the Video Rental Protection Law.<sup>58</sup> That law makes it clear there is no First Amendment problem. The law says that you cannot look at a record of what videos someone checks out from Blockbuster and you do not have any First Amendment right to do so.<sup>59</sup> The statute makes it clear you have a right of privacy in that information,<sup>60</sup> you have a right of privacy in cable TV,<sup>61</sup> you have a right of privacy in credit reports.<sup>62</sup> We have a list of laws which give individuals rights to privacy.

But, we also have some major gaps. For example your medical records or financial records are not adequately protected in law; similarly your employment records, like your general Internet e-commerce records - like all the most important records that really count and are becoming central in the Information Age - are not adequately protected by law.

And so we talk about “opt-in” versus “opt-out.” I am not as concerned about that issue. I think the issue has to be, what is our goal? Our goal is to protect privacy based on informed consent. All law is based on informed consent and so too should privacy law, especially in the Information Age, and it should be based on a purpose test.

You’ve heard about Fair Information Practices. Right at the heart of Fair Information Practices is the principle that information collected for one purpose cannot be used for another purpose without your knowledge and consent.<sup>63</sup> That test works very well. Depending on the context, you can never reach 100 percent, but to

---

<sup>58</sup> *See id.*

<sup>59</sup> 18 U.S.C. § 2710(b)(1) (1994) states that “[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person . . . .” Personally identifiable information is defined to include “information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.” 18 U.S.C. § 2710(a)(3) (1994).

<sup>60</sup> *Id.*

<sup>61</sup> *See* Cable Communications Policy Act, 47 U.S.C. § 551 (1994) (providing that “a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned”).

<sup>62</sup> *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994).

<sup>63</sup> *See* FEDERAL TRADE COMMISSION, *Privacy Online: A Report to Congress* at 7-11, available at <http://www.ftc.gov/reports/privacy3/priv-23a.pdf> (June 1998).

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 75

the extent that you are close to that shows the extent that you are protecting privacy.

There are societal benefits. Ironically, a societal benefit is the free flow of information, which is what led the European Commission in the Community to enact the Data Protection Directive.<sup>64</sup>

Let us go back to your privilege between attorney and client. The confidentiality privilege is not so they can hide in the closet. The confidentiality privilege is so the client feels free to tell everything to the attorney, because only when the attorney knows everything can that attorney make a judgment as to how to proceed and to serve the client's interest. So it is the privilege of confidentiality that allows for the free flow of information, which allows for the goal of adequate representation of the client. The same with doctor and patient, and with clergy and parishioner.

You can apply that same model to society, especially in the Information Age. The knowledge that your information will only be used for the purposes for which you gave your informed consent will encourage you to participate in those systems, in the democracy, in the economy, and if something goes wrong you have a remedy. That is where we are going to go someday. It is just a question of how long it takes us to get there. So, there are societal benefits.

Ultimately, privacy is for individuals, and privacy, I am convinced, is emerging as the most important human right of the Information Age.

Now, what is the history of law? The history of law in society really is a march toward greater rights for individuals. In feudalism, the lords had all the rights. Then we moved into industrial capitalism, and that change in the economic system led to a change which gave people more legal rights. Slavery was a form of feudalism, and there were people who defended slavery as necessary and some sort of natural law, but slavery eventually gave way to its abolition and to creation of more individual rights. There was a time in this country when only property owners had

---

<sup>64</sup> See Janis L. Gogan, *Next Up: European Privacy – Oct. 24 Marks The Beginning Of Europe's New Rules On Privacy. Is Your Business Ready?*, INFORMATIONWEEK, Sept. 28, 1998, at 177.

the right to vote, then there was a time when only men had the right to vote, and then finally they gave women the right to vote. And then we had the civil rights movement. These have been the great movements for human rights in North America. Even the environment, to some extent, gave individual rights to people.

In all those cases, none of those rights came without struggle, and I think this will be true for privacy as well. This is because in my historical examples there were entrenched interests that were trying to defend feudalism, slavery, stop integration in North America, and prevent the establishment of civil rights, just as now there are entrenched interests that do not want individual Americans to have legal rights to privacy.

That is why our discussion of the benefits of commercial free speech is quite relevant here, because I think commercial free speech, including campaign contributions, is clearly protected under the Constitution. This is a political area. There is a lot of campaign money flowing on this issue, and I promise you it is having an influence. Politicians have to do an interesting dance. They can not be “bad” on privacy. Some might want to move ahead, but if they somehow play their cards wrong, either they will not get the campaign contributions that they need or their opponent will get them, and you have got to be able to buy television air time for commercials. This is a significant factor in the dynamics of this issue.

It is interesting to me when the commercial sector talks about the benefit to the individual. What they are saying is that, “we will decide for you.” If this is to the people’s benefit, then tell them about it and let them consent to it. But what the commercial sector is saying is, “we will decide what is to your benefit.” I think that is an interesting twist on Big Brother, when organizations are deciding for the individual what is to their benefit.

In the past, I think that kind of attitude - organizations dictating to individuals what is to their benefit - is a form of arrogance, and I think history has shown us that the downfall of power is arrogance. I think that is why we are on very familiar historical ground, which makes it such an interesting time.

Thank you.

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 77

MS. SINGLETON: If you look out at the field of American jurisprudence, what you see is a lot of sacred cows lying around in a field. Some of these cows have a "Constitution" label on them, and some of them say "Privacy," and some of them say "Free Speech," and so on. Now, most people are wandering around in the field looking at the details of the cows, examining an eyelash or picking up a tail or a hoof or something, but every now and then, one of the cows will get up and give one of the other cows a good kick, and then all the cows kind of move around and it actually gets pretty interesting for awhile. I think this is something that has the potential to happen with the conflict between privacy and the First Amendment.

I would like to begin by outlining the issue as a general philosophical matter - from a philosophical standpoint rather than a litigation standpoint. When you are considering regulation of private sector exchanges of data about consumers, the issue becomes should the government stop businesses from communicating truthful information about real people and real events as a general matter?

As a general matter, in human life, the default rule is that we are free to make observations about one another and learn about one another. There are exceptions to that general rule of freedom of information we have created in special contexts. Some of those are medical privacy, attorney-client privilege, and so on. In those situations, an expectation of privacy has developed over the years as a result of industry custom, as businesses learn what they need to do to gain people's trust, and ultimately those expectations, formed from the bottom-up, get built into statutes.

Another example of an exception where we have created walls on information is copyright. Essentially though, copyright applies to a pretty limited array of information. And there is a fundamental constitutional principle that you cannot copyright facts and ideas.<sup>65</sup> So in many ways, copyright is a very limited concept.

Defamation is another example of a sort of property right in

---

<sup>65</sup> See, e.g., *Harper & Row, Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 556 (1985) (citing 17 U.S.C. § 102(b)); *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 344-345 (1991).

information, and that is limited by our understanding of the First Amendment.

Now, a lot of these informational walls, particularly copyright and defamation, are problematic when it comes to the Internet, because that is an environment the entire purpose of which is to lower the cost of transmitting information. One sees a lot of enforcement problems arising in this context. On the Internet, it begins to look like the concepts of defamation and copyright start to erode and change very quickly.

As a general matter, when you are creating property rights in information, you are doing a very difficult thing, and something that is traditionally limited to narrow exceptions. The default rule remains the freedom of information.

Now, if we think about creating property rights in personal information - essentially, a system under which personal information is regulated - we are talking about suddenly moving a lot of facts about people, and analysis of those facts as well, out of the realm of shared information and into the realm of regulated information. If we are going to do that, we should be very, very careful, because it is a much more radical thing than has heretofore been attempted in delineating property rights in information.

Now, I am going to switch tracks and talk a little bit about two of the issues that have arisen in the rather sparse case law concerning the conflict between the commercial speech doctrine and privacy.

There are two questions that have come up in the very few cases that have arisen so far. The first is the question of whether exchanges of data about consumers between businesses is in fact commercial speech, or whether it is ordinary speech.

Now, in some cases, information that a company collects about consumers is clearly going to fall within the standard definition of commercial speech if it is closely tied to something that we would recognize as advertising or solicitation. In other cases though, if information is exchanged between two businesses or is being used within a company, then you suddenly have something that does not look very much like what has traditionally been recognized as commercial speech.

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 79

So far, there is very little solid analysis of this question in the case law. To give you an example, there was one case, the *Los Angeles Police Department v. United Reporting* case,<sup>66</sup> where a company was in the business of selling many units of information, which were essentially sentences in the form of, “X was arrested on the following date.” The Court asked whether this type of speech was commercial speech and decided this issue in about a paragraph.<sup>67</sup> It said, to paraphrase, “Well, this has got to be commercial speech because it is being sold and the sentences are not very long and do not contain very much information.”<sup>68</sup>

Now, I think all of you can find reasons why those two criteria are not very good ways of selecting out commercial speech. What may have been going on in the Court’s mind was something along the lines of, “Well, it is a commercial actor; therefore, what they do must be commercial speech.” But that is not the traditional commercial speech analysis at all. So, I think that the question of whether and when the sale of factual information is commercial speech is an issue that the courts will continue to grapple with.

The second issue that has come up in the case law, is the question of the strength of the government’s interest in regulating privacy. Under the commercial speech test, regulation needs to be a “substantial interest” to pass First Amendment scrutiny.<sup>69</sup>

Now, if all the legislature had to do, when faced with the substantial interest test, is recite vague things about privacy and talk about *Roe v. Wade*<sup>70</sup> and the Fourth Amendment and so on, given that constitutional privacy is quite a different problem from privacy issues that arise in marketing, it would basically gut constitutional protections. So, when we have a stated legislative

---

<sup>66</sup> *Los Angeles Police Dep’t v. United Reporting Publ’g Corp.*, 528 U.S. 32 (1999), *rev’g* *United Reporting Publ’g Corp. v. Cal. Highway Patrol*, 146 F.3d 1133 (9th Cir. 1998), *aff’g* *United Reporting Publ’g Corp. v. Lungren*, 946 F. Supp. 822 (S.D.Cal. 1996).

<sup>67</sup> *See* *United Reporting Publ’g Corp. v. Cal. Highway Patrol*, 146 F.3d 1133, 1136-1137 (9th Cir. 1998).

<sup>68</sup> *See id.* (holding that United Reporting did nothing more than sell arrestee information to clients, a pure economic transaction which falls within the core notion of commercial speech).

<sup>69</sup> *See* *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm’n of N.Y.*, 447 U.S. 557, 566 (1980); *see also* *Greater New Orleans Broad. Assn. v. United States*, 527 U.S. 173, 178 (1999).

<sup>70</sup> 410 U.S. 113 (1973).

interest in protecting privacy, we need to look pretty closely at it to examine it for real substance.

So far, the cases and regulations that have been considered in the cases have not gotten very far with this analysis. At least one court has looked at the issue, broken it down, and said: “Okay, when we’re considering this use of information for marketing, it is not the same thing as when we consider a police search under the Fourth Amendment.”<sup>71</sup> This court has separated out the different types of privacy interests at stake.<sup>72</sup> This analysis is along the right lines. That kind of precision in distinguishing constitutional privacy cases, from cases where there is no state action in collecting the information, is what courts will continue to look for in defining the state’s interest in cases addressing a free speech versus privacy conflict.

Now, as a general rule, companies moving information around to sell things to consumers, develop products, or start a business, as a general matter do not harm consumers; although, they may annoy them. Therefore the government’s interest in regulating privacy is not very strong.

Because of the key role that information exchange plays in letting small companies get a foot in the door when competing against large companies, in starting new business, in developing new products, and so on; these cases, where you consider the constitutionality of private-sector regulation, are going to test a main presumption underlying the commercial speech doctrine today. That presumption is that “Economic Man” is somehow a fundamentally different and less important creature than “Artist Man” or “Journalist Woman.”

Because of the difficulty in showing harm to consumers and of cabining all data flows as commercial speech, I anticipate private regulation running into considerable difficulty in the courts on free speech grounds.

Thank you.

---

<sup>71</sup> U.S. West, Inc. v. FCC, 182 F.3d 1224, 1234-35 (10th Cir. 1999).

<sup>72</sup> *See id.*

MR. SOBEL: Thank you.

It is always a challenge to be the last speaker following ten speakers who have done a very good job of covering a lot of ground. So, I am going to have some trouble breaking new ground here, but I will do my best. I will also try to respond to some of the points that have been made in the preceding comments.

Let me say a little bit about my credentials, which are somewhat similar to the ones that Evan Hendricks told you about. I am also a long-time defender of the First Amendment. Among other things, I was co-counsel in *Reno v. ACLU*,<sup>73</sup> the Supreme Court case that struck down the Communications Decency Act,<sup>74</sup> and my organization has a very strong commitment to protecting free speech and the First Amendment on the Internet.<sup>75</sup> So, I come at this issue as both a privacy advocate and a free speech advocate.

I am also very much committed to the availability of information and public access to government information. I have been a Freedom of Information Act ("FOIA") litigator for twenty years, so my impressions of the privacy issue and the balancing that takes place, has been formed by the FOIA process and by the case law that has been developed under the Freedom of Information Act.<sup>76</sup> Under two of the exemptions to the FOIA, there is in fact a very well-developed balancing test between the need for public disclosure of information on the one hand, and the protection of personal privacy on the other.<sup>77</sup> So, I see myself coming to the issue of the First Amendment versus privacy as someone who has sensitivities on both sides of that apparent conflict.

Having said that, I, for the last several years, having heard the First Amendment arguments that have been put forward, am not convinced. I do not see a serious First Amendment impediment to the privacy legislation that exists and the privacy legislation that many of us believe is necessary to address the practices that we are seeing increasingly on the Internet. I think the Internet is driving a

---

<sup>73</sup> 521 U.S. 844 (1997).

<sup>74</sup> The Communications Decency Act ("CDA") was part of the Telecommunications Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 56, 137 (codified as amended at 47 U.S.C. § 230 (Supp. III 1997)).

<sup>75</sup> See *About EPIC*, at <http://www.epic.org/#about> (last visited Nov. 1, 2000).

<sup>76</sup> 5 U.S.C. § 552 (1994).

<sup>77</sup> See *Dep't of the Air Force v. Rose*, 425 U.S. 352, 372 - 374 (1976) (citing H.R. REP. NO. 1497, p. 11 and S. REP. NO. 813, p. 9).

fresh look at this issue, and I believe a reasonable First Amendment analysis should not interfere with providing meaningful legal rights and remedies to consumers.

I have listened to the First Amendment arguments and I don't see, for instance, why similar arguments could not be made with respect to the federal wiretap law, which was amended in 1986 to apply to e-mail and other electronic communications.<sup>78</sup> Why, for instance, is there not a First Amendment problem with the government saying that I cannot intercept and disseminate your telephone private communications or your e-mail communications? What if the same information that a Web site collects about me was contained in a telephone conversation? Suppose I was calling a friend and I was listing the Web sites that I like to visit and describing the particular material that I have accessed on the Internet? Why is there a philosophical difference between the information being intercepted without my knowledge in a telephone conversation or an e-mail message and being compiled by a Web site without my knowledge?

So, I do not see a significant distinction between the wiretap context, which I think all of us readily acknowledge is an appropriate governmental regulation of conduct, and similar controls on the surreptitious collection of information on the Web. In a moment, I am going to talk a bit about the DoubleClick situation.<sup>79</sup> I think it demonstrates that information is in fact being collected without the knowledge or consent of most individuals, much as it might be in an intercepted phone conversation.

What about the FTC Act itself,<sup>80</sup> which is currently being put forward as the existing source of privacy protection that the federal law provides to consumers? These are the protections that are frequently pointed to, specifically the FTC's jurisdiction over unfair and deceptive trade practices. Why is there not a First Amendment problem with that? What constitutes an unfair trade practice? It is not necessarily fraudulent behavior. It does not necessarily involve anything other than accurate information about individuals, but just being used and manipulated in ways that the Commission might determine to be unfair. If that structure is

---

<sup>78</sup> The Electronic Communications Privacy Act of 1986, Pub. L. No 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

<sup>79</sup> See *infra* notes 81-86 and accompanying text.

<sup>80</sup> The Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (1994).

appropriate, and if there is a legitimate governmental role in regulating unfair and deceptive trade practices, I don't see why the First Amendment would prevent us from going a step further and regulating many of the activities that do not fall within the unfair and deceptive trade practice regime.

That leads me to a discussion of DoubleClick, which has been talked about a bit today. I would like to discuss it in a little more detail because I think it provides an interesting test case for the adequacy of the current privacy regime we have in the United States.

As I mentioned, the Federal Trade Commission and the FTC Act are frequently pointed to as providing the legal framework for consumer remedies in the privacy realm. My organization last week filed a complaint with the FTC against DoubleClick alleging that DoubleClick's information-collection practices constitute unfair and deceptive trade practices.<sup>81</sup>

DoubleClick, as you might know, is the largest online advertising company.<sup>82</sup> Basically the way they operate is that they place "cookies" on the hard drives of users who visit various Web sites that serve up banner ads that are provided by DoubleClick.<sup>83</sup>

Now, an interesting aspect of this is that the user never consciously deals with DoubleClick. You do not go to the DoubleClick Web site and thereby have a cookie placed on your hard drive. Instead, you go to *The New York Times* Web site, you go to the CNN Web site, and by virtue of receiving the ad that DoubleClick is providing at that Web page, you receive a "cookie" which essentially brands your computer and makes it identifiable to DoubleClick.

DoubleClick for many years has claimed, to anyone who managed to actually visit its Web site, that all of this activity was anonymous, that "cookies" just contained a unique identifier. I would be, for instance, "User 123;" I would not be identified as David Sobel, and DoubleClick provided assurances at its Web site

---

<sup>81</sup> Complaint before the Federal Trade Commission, In the Matter of DoubleClick, Inc, available at [http://www.epic.org/privacy/internet/FTC/DCLK\\_complaint.pdf](http://www.epic.org/privacy/internet/FTC/DCLK_complaint.pdf) (last visited Nov. 1, 2000).

<sup>82</sup> See Bob Tedeschi, *In a shift, DoubleClick puts off its plan for wider use of the personal data of Internet consumers*, N.Y. TIMES, March 3, 2000, at C5.

<sup>83</sup> See *id.*

84                    *FORDHAM INTELL. PROP., MEDIA & ENT. L.J.*    [Vol.11:59

that this information was and would remain completely anonymous.

Significantly, those statements started to change last year when DoubleClick announced its plans to acquire a company called Abacus Direct, which is an offline direct marketing database company.<sup>84</sup> Abacus Direct has a database that contains 88 million consumer profiles that are largely derived from catalog sales.

Many of us in the privacy community who were looking at the proposed acquisition expressed a concern that the Abacus database, the 88 million identifiable profiles, would be married together with the approximately 100 million anonymous online profiles that DoubleClick had compiled over the years. And suddenly, the privacy assurances at the DoubleClick Web site began to get watered down. There was no longer the use of the word “anonymous.” The assurance was no longer provided that this information would be and would remain completely anonymous.

And then, after the acquisition was actually completed last November, DoubleClick announced its plans to in fact begin this process of merging the databases, but with the caveat that this would be done with notice and, as they put it, “choice” on the part of the users who were so identified.<sup>85</sup>

Our complaint to the FTC alleges that this constitutes an unfair and deceptive trade practice.<sup>86</sup> It is unfair because the average user, as I said, never goes to the DoubleClick Web site. The average user, I think, even after all of the controversy and all of the press stories, is probably unaware of the fact that there is a company called DoubleClick and that that company has placed markers on the users’ machines. How can it possibly be characterized as something that is occurring with the knowledge and consent of users? So, our first claim to the FTC is that this scheme, because of its invisibility, is fundamentally unfair.

The deception claim has to do with the company’s earlier assurances that the information would remain anonymous. Now,

---

<sup>84</sup> *DoubleClick to Buy Retailing Data Base Keeper*, N.Y. TIMES, June 15, 1999, at C4.

<sup>85</sup> See, e.g., Will Rodger, *Online Profiling Firms Plan to Police Themselves*, USA TODAY, Nov. 8, 1999, at A2.

<sup>86</sup> See *supra* note 80 at ¶¶ 28-33.

2000] SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT 85

as I said, I suspect that not many of the people who have those “cookies” on their hard drives ever found their way to the DoubleClick Web site and saw that assurance, but to the extent that they did, that constitutes a deceptive trade practice.

This is going to provide an important test case, to see whether the existing remedy that federal law provides, which is the somewhat difficult standard of unfair and deceptive trade practices, really works in the privacy context. In preparing the complaint, I have to say that it really did feel like we were trying to fit a square peg into a round hole because, frankly, the unfair and deceptive trade practice analysis does not always work for a privacy case. In this case, however, I think it does because of the invisibility of the challenged activity.

I think we will have to see what the Commission does with the situation. I am not overly optimistic, frankly. I think the Commission, if they look at this at all, will probably nibble around the edges of it. I think that this is going to provide some baseline data for us to clearly demonstrate the inadequacy of the current legal regime in the privacy realm.

I want to just briefly address the issue of whether or not personal information is property, and whether the individual who the information relates to should have some property right in their personal data.

I will make an observation about the *U.S. West* case,<sup>87</sup> which is in the symposium materials and which has been discussed today. It has not been commented on much in any of the analysis or discussion of the case that I have seen, but if you look at the decision, you will notice that in the Tenth Circuit, *U.S. West* made two claims: First, the company challenged the FCC’s CPNI<sup>88</sup> rules on First Amendment grounds; but the firm also raised a Fifth Amendment claim, saying that the rules required it to obtain the permission of consumers was a “taking” of their property.<sup>89</sup> In other words, the CPNI information, the calling records of the

---

<sup>87</sup> *U.S. West, Inc. v. FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied sub nom. Competition Policy Inst. v. US West, Inc.*, 120 S. Ct. 2215 (2000).

<sup>88</sup> Customer Proprietary Network Information.

<sup>89</sup> *U.S. West*, 182 F.3d at 1230 (“[P]etitioner argues that the CPNI regulations raise serious Fifth Amendment Takings Clause concerns because CPNI represents valuable property that belongs to the carriers and the regulations greatly diminish its value.”).

individual customers, was, according to *U.S. West*, company property.<sup>90</sup>

It seems to me, first of all, that the claim is completely inconsistent with the First Amendment argument, although the court didn't need to get to the Fifth Amendment argument or the property claim because it resolved the case on First Amendment grounds.<sup>91</sup> But I just throw that out because I think if *U.S. West* can claim that customer data is their property, we could certainly envision legislation that would change that presumption and establish that such information is, in fact, the property of the individual to whom it relates. I think that would remove a lot of the First Amendment concerns that have been raised.

Finally, I want to talk a little about "opt-in" and "opt-out" because that has been a major point of discussion today. I think we have to assess the burden placed on consumers in a scheme that requires "opting-out," particularly on the Internet. I think this is the environment in which the inadequacy and the inappropriateness of "opt-out" has really been demonstrated.

What this approach would really require - and I think the DoubleClick case is an interesting example of this - would be for every user at every Web page to read these very difficult and voluminous privacy policies and make copies of them, because they are subject to change, as the DoubleClick case indicates. So the average consumer, who would want to raise some claim against DoubleClick based on a contract theory, for instance, would have to have thought ahead two years ago to make copies of those previous privacy policies. So, there is a real burden involved in saying to consumers, "you have got to read the policy, here is your right to "opt-out;" but, by the way, the policy might change, so you really need to check back periodically to make sure that we are still doing what we said we were going to do six months ago."

And finally on this point, if, as we have heard, the benefits to consumers are so real when personal information is used in the ways that we have been discussing, and targeted advertising is directed to consumers, then I do not understand why industry is so resistant to an "opt-in" model. Make the case, explain to people why it is to their advantage to "opt-in" to an information collection

---

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 87

system. Industry should do very well in that endeavor if, in fact, extensive data collection is something that, as they claim, most consumers want and would find beneficial.

Thank you.

PROFESSOR REIDENBERG: Thank you.

I think what I am going to do is start by opening it up to see if there are any initial questions.

QUESTION: I have a question, certainly for Solveig and for anyone else on the panel. In the Telecommunications Act,<sup>92</sup> part of the justification behind the CPNI rules<sup>93</sup> was competition. The concern was that local phone companies had a wealth of calling pattern information that would be critical to competitive services, and the new law hoped to encourage market entry for long distance, local, and wireless usage. Congress did not want companies to have an unfair advantage based on all the data they had from what had been a very regulated market.

I think there are some interesting parallels between the CPNI rules and the Financial Services Modernization Act, known as the Gramm-Leach-Bliley Act (“GLB”).<sup>94</sup> GLB sets rules for the use of information inside financial institutions and for the disclosure of information outside the institution. Banks, securities, and insurance companies that used to be separate entities are now going to be merging, and so they will have the benefit of a significant volume of data with few limitations on affiliate sharing, whereas some of the small actors are going to be quite disadvantaged entering these new markets.

So, have you looked at the implications of privacy rules for competition in, as you said, an incredibly information-dependent age?

MS. SINGLETON: Yes, I think privacy rules have a potentially enormous impact on competition. I think that is part of the reason to stay out of the whole business of regulation in that area, because

---

<sup>92</sup> Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, (codified as amended in 15 U.S.C. and in scattered sections of 26 U.S.C.).

<sup>93</sup> *Id.* § 222.

<sup>94</sup> Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999), Pub. L. No. 106-102, 113 Stat. 1338, (codified as amended in scattered sections of 12 U.S.C. and 15 U.S.C.).

88                    *FORDHAM INTELL. PROP., MEDIA & ENT. L.J.*    [Vol.11:59

if you tailor the regulation narrowly enough to target a particular industry sector, or a particular problem, then the economy restructures itself to work around the rules and to get out of the narrow category that has been regulated.

I would generally say that I think on the whole the role that information plays in competition is going to be a tremendously complicated one. There are not a lot of economic studies that have been done on this subject yet.

But I guess I would generally say that, as a general rule, this is a reason to stay away from regulation across-the-board rather than a reason to begin regulation and then expand it to include many different companies.

PROFESSOR REIDENBERG: I think there are many problems with the standard of review of the Tenth Circuit in the *U.S. West* case.<sup>95</sup> The court might not even get to the privacy issue on appeal.

If I might add a couple of footnotes to that, in the Tenth Circuit *U.S. West* case,<sup>96</sup> there has been a petition for rehearing *en banc*. I don't know if that has been. . .

MR. SOBEL: It was denied.<sup>97</sup>

PROFESSOR REIDENBERG: I didn't realize that. Has it been appealed to the Supreme Court yet?

MR. SOBEL: No.

PROFESSOR REIDENBERG: Do you know if it will be?

MR. SOBEL: The government is considering it.

PROFESSOR REIDENBERG: Okay.

The other point is, in looking at the Tenth Circuit's opinion, the court criticized the FCC very heavily for not conducting a sufficient inquiry into "opt-in" versus "opt-out."<sup>98</sup> I would certainly concur with Evan. I am not sure what docket the Tenth Circuit was reading because, at least as I read the FCC's docket,

---

<sup>95</sup> *U.S. West*, 182 F.3d 1224.

<sup>96</sup> *Id.*

<sup>97</sup> *Competition Policy Inst. v. U.S. West, Inc.*, 120 S. Ct. 2215 (2000).

<sup>98</sup> *U.S. West*, 182 F.3d at 1238-39.

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 89

there was quite a discussion of the difference between “opt-in” and “opt-out” that the Court seemed to willfully ignore. But, we will see what happens in that case. It is interesting.

The other footnote goes in part to Solveig’s point. The competition implications of fair information practices are certainly significant, and I think in some ways you make the case for having omnibus legislation rather than none at all. If we continue to pursue a targeted approach, as we have done in the United States, I think you are absolutely right that what happens is the law encourages circumvention. For example: “Well, if we regulate it as a video rental service provider under the ‘Bork Bill,’<sup>99</sup> then if I provide video over the Internet, I am not covered.” So, there is an incentive to provide service over the Internet.

There are some other interesting cases involving this competition angle. The credit reporting agencies have been very upset because many of the large credit issuers, the banks such as Citigroup, started to refuse to provide transaction information to the credit reporting bureaus. Credit issuers stopped reporting data such as “John Smith is paying his debt on time.” The reason was that the credit bureaus were turning around and selling these names and addresses to competitors who used this information to make unsolicited offers of credit or insurance. So, credit grantors like Citibank felt these were their best customers; they are paying off their credit debt on time. The credit bureau is going to turn around and help competitors of Citigroup. The competition would try to cherry-pick Citigroup’s best customers and offer them a better interest rate. Citigroup, as a large conglomerate, all of a sudden, had enough information about tens of millions of Americans that they no longer needed the same services of a credit bureau to make decisions about granting credit. So, there are some very significant competition implications that are playing out there.

QUESTION: I want to address this to Ms. Barrett. It seems to me that the constitutional issue in this case is going to be decided by the political consensus that develops in the country. Ultimately, this is not one of those issues which is going to be held up on some

---

<sup>99</sup> Video Privacy Protection Act of 1988, 18 U.S.C. § 2710-2711 (1994). The act was enacted in response to the revelation at the Supreme Court nomination hearings of Judge Bork that a list of his video tape rentals had been procured and made publicly available. *See Video Privacy: “Nonpublic” People Are Even More Important*, WASH. POST., Mar. 6, 1988, at C8.

real constitutional doctrine. I have some sense of what privacy means. I can identify it in terms of the phone calls I get at night and in terms of brochures that come to me that I do not want. But I really have absolutely no sense of what your argument is politically; in other words, how you think you are going to carry the day, other than in the abstract sense of what the efficiencies are or the reduced cost that I may experience. What is the value to me, how you are going to convince me to write a letter to my congressman saying, “do not protect what I perceive as my privacy?”

MS. BARRETT: This is one of the issues that the industry is looking at, because the value to the consumer is not clear public knowledge, and it is in many cases very poorly documented.

I will give you one very specific example of a situation that actually deals with a public record, which is not our forum here, but it is a good one. The property information, the recorded deed of your house, which has been a public record for many, many years, is a very integral part of the mortgage industry. It has been documented that mortgage rates in the United States are approximately two points less than they are in other countries because of the free flow of mortgage information.<sup>100</sup>

Now, I think if the consumer knew some of the real tangible benefits that can result from the free flow of information, they might feel differently about it. However, as an industry, we have not done a very good job of documenting those examples. I think you are going to begin to see more documentation of these benefits as time goes forward.

MR. HENDRICKS: I did not address this because this is not a public records panel, but the purpose test works very well and is the way to guide the use of driver’s records. Right now and historically, driver’s records have been available for any purpose, which is why you get horror stories about stalkers using Department of Motor Vehicles (“DMV”) records.

I don’t think anecdotes should drive our debate, but I think systematically you want to look at a purpose test for property records for property purposes. In half the states, the law is that

---

<sup>100</sup> WALTER F. KITCHENMAN, U.S. CREDIT REPORTING: PERCEIVED BENEFITS OUTWEIGH PRIVACY CONCERNS 4 (Tower Group 1999).

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 91

voting records are only for voting purposes, and not to be used for commercial purposes. You should let the purpose test drive the use of public records.

PROFESSOR REIDENBERG: Let me ask for one more question and then I'll ask a question before we adjourn for cocktails.

QUESTION: I just wanted to ask any of you to comment more about substantive regulation. The discussion today has focused more on self-regulation as the predominant force in the industry. From what I understand, the debate over "opt-in" versus "opt-out" seems to hinge on a debate between the self-regulation versus substantive regulation; substantive regulation being more of the "opt-in" and self-regulation being more of the "opt-out." Can you comment more on substantive regulation?

PROFESSOR REIDENBERG: I think I feel safe in saying the privacy community favors legislation based on the widely accepted fair information practice standards.

This is the law in Europe.<sup>101</sup> Whether the data is government held information or privately held information, citizens have legal rights and citizens have a remedy if personal information is mistreated. Personal information cannot be used for secondary purposes, and governments have an oversight office to turn to if something does go wrong.<sup>102</sup> This is the scheme in the Netherlands, for instance.<sup>103</sup> The Dutch have baseline protections of law, and then ask the different sectors of the economy to come forward and submit their own codes of how the sector can implement the law.<sup>104</sup> Then the Dutch Privacy Commissioner and the various industries go back and forth, finally agreeing on the code for specific sectors of industry.<sup>105</sup>

You have to start with the basic underpinning of rights based on fair information practices, which we already have, to a limited

---

<sup>101</sup> See generally European Union Directive 95/46/EC.

<sup>102</sup> See David Banisar & Simon Davis, *Global Trends in Privacy Protection: An International Survey of Data Protection and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 12-13 (1999).

<sup>103</sup> See Personal Data Protection Act of July 6, 2000, available at [http://www.registratiekamer.nl/bis/top\\_2\\_6.html](http://www.registratiekamer.nl/bis/top_2_6.html) (last visited Nov. 17, 2000).

<sup>104</sup> *Id.* at Art. 25(1).

<sup>105</sup> *Id.* at Art. 25(4).

extent, in laws such as the Fair Credit Reporting Act<sup>106</sup> or the Privacy Act which covers federal agencies.<sup>107</sup>

Simson Garfinkel has a new book out,<sup>108</sup> and there is an article in the current issue of *The Nation*, where he advocates expanding the Fair Credit Reporting Act to apply to everything.<sup>109</sup> These standards work well no matter what the medium, and they are already in place in Europe. These standards represent basic fairness for individuals and ultimately are good for commerce.

MS. SINGLETON: If I could add to that, I think as a theoretical model, self-regulation could take the form of “opt-in” or “opt-out,” as could substantive regulation. The reason that self-regulation has tended to take the form of “opt-out” is that the companies looking at how to develop regulation need something that can work with their existing businesses without having to completely restructure their entire information systems. They are looking at “opt-out” because it is something that, from a business standpoint, is a manageable task.

I might also just comment that even the European law, which is held up as a very conservative law, does not require “opt-in.” “Opt-out” is a permissible form of consent under that law. So it really is not an “opt-in” versus “opt-out” issue when you get to the substantive issue.

PROFESSOR REIDENBERG: I want to ask a closing question that brings us back to a point that Jennifer Barrett started with in her comments, which is, “what are the abuses?” Among her four questions, the last one was, “what are the abuses?” I think this goes to the heart of many of the issues we were talking about today, because the question of whether self-regulation is satisfactory, whether legislation is necessary, and whether legislation could meet the *Central Hudson* test,<sup>110</sup> will hinge on how we define the harm and what we see as the abuse.

---

<sup>106</sup> Fair Credit Reporting Act, 15 U.S.C.A. §§ 1681-1681(u) (2000).

<sup>107</sup> Federal Privacy Act of 1974, 5 U.S.C.A. § 552a (2000).

<sup>108</sup> SIMSON GARFINKEL, *DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY* (O'Reilly & Assoc. ed., 2000).

<sup>109</sup> See Simson Garfinkel, *Privacy and the New Technology: What They Do Know Can Hurt You*, *NATION*, Feb. 28, 2000, at 11.

<sup>110</sup> *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557, 566 (1980) (setting out a four-part test to judge government restrictions on commercial speech).

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 93

My question is, in part, why are we having such difficulty finding the harm? Why is not it that information profiling, in and of itself, is an indignity and a harm that society recognizes? I think when seen in the light of day, there are many companies out there selling the same types of detailed profile information; it is just that they are hidden from public view. And it is the sense that this data is being profiled and sold secretly that I think is, in part, what your question reaches.

So, my closing question is, why do we not define that in and of itself as a harm?

MR. SOBEL: Joel, if I can address that, I agree with that very much. Our perspective on this is that privacy is a fundamental right and there should not be any need to catalog specific harms beyond the violation of a basic right. We do not, for instance, ask: "What is the harm when somebody is denied their right of free speech?" I believe that privacy rights are similar and that they are fundamental human rights and you should not have to put a monetary value, for instance, on what the loss is or specify what the harm is.

But that is not to say that we are not heading for a situation where there are likely to be some very concrete harms in the future. As these databases continue to grow and become more sophisticated and more widely available, I do not think it is beyond the realm of possibility that reference to such databases will become a typical part of pre-employment screening, for instance, or used by insurance companies making decisions whether to insure people.

So, I think we are heading for a situation where there will be many horror stories, but at that point it might be too late. So, to a certain extent, the concern today is anticipatory.

MS. SINGLETON: From my standpoint, human beings have a fundamental right to learn about each other and to communicate what they have learned to other people.<sup>111</sup> There are an awful lot of things that we could outlaw on the argument that they are not consistent with human dignity. There are a lot of things that

---

<sup>111</sup> See generally Solveig Singleton, *Privacy As Censorship: A Skeptical View of Proposals to Regulate Privacy in the Privacy Sector*, CATO POLICY ANALYSIS No. 295, Jan. 22, 1998.

human beings do that are just not that dignified. And yet, I do not really think that a human being is that fragile a creature and that human dignity is that weak a thing that the fact that a company has learned some information about your behavior and has sold it to another company is really a harmful attack on that.

MS. BARRETT: I would comment that I think harm, once you get past the obvious legal abuses - identity theft, stalking, and so forth - becomes a very subjective thing. What I might view as harmful to me versus what Joel or others on this panel, or those of you in the room, might view as harmful would probably be very different. I think that is the difficulty that we face in trying to answer the question.

MR. HENDRICKS: I think that goes for benefits too; that is also subjective. But clearly, there is progress on this, in the sense that harms have been alleged in lawsuits recently filed against DoubleClick,<sup>112</sup> Alexa of Amazon.com,<sup>113</sup> any others?

PARTICIPANT: Yahoo!

MR. HENDRICKS: Yes. How could we forget that? That guy sued Yahoo! because they were standing by their privacy policy and then turned around and sued them for violating people's privacy - Larry Friedman in Dallas.<sup>114</sup> So the courts might be speaking on this sooner than we expect.

However, I think that there is a certain model that we can look at to understand that there is still plenty of freedom within a system of informed consent that respects privacy. I mean, take "The Jerry Springer Show, for instance. Those people spill their guts in front of a national audience, but they give their informed consent to do it and they totally understand the consequences of just hanging themselves out there. That is a system where they are free to be undignified, but they are clearly exercising their rights to free speech and there is no invasion of privacy.

---

<sup>112</sup> Judnick v. DoubleClick, Inc., No. CV 000421 (Sup. Ct. Marin County Cal. filed Jan. 27, 2000).

<sup>113</sup> Newby v. Alexa Internet and Amazon.com, No. C 00 0054 (N.D. Cal. filed Jan. 6, 2000).

<sup>114</sup> See, e.g., Susan Borreson, *Suit Claims Cyber "Cookies" are Poison*, N.Y.L.J., Feb. 15, 2000, at 5; *Yahoo! Faces Texas Suit Over Privacy Concerns*, NAT'L L.J., Feb. 28, 2000, at B9.

2000] *SYMPOSIUM - DATA PRIVACY & THE FIRST AMENDMENT* 95

PROFESSOR REIDENBERG: With that, I would like to conclude the panel and the afternoon and give a thanks and congratulations to the *IPLJ*,<sup>115</sup> and especially to Joshua Sussman who put today's program together. It has really been a terrific and productive session, and I hope this is the beginning of a very long, spirited debate on these issues.

Thank you very much. I hope you will all stay for cocktails.

---

<sup>115</sup> Fordham Intellectual Property, Media & Entertainment Law Journal.