Maine Law Review

Volume 54 | Number 1 Article 5

January 2002

Internet Privacy Law, Policy, and Practice: State, Federal, and International Perspectives

Rita S. Heimes
University of Maine School of Law

Follow this and additional works at: https://digitalcommons.mainelaw.maine.edu/mlr

Recommended Citation
Rita S. Heimes, *Internet Privacy Law, Policy, and Practice: State, Federal, and International Perspectives*, 54 Me. L. Rev. 95 (2002).
Available at: https://digitalcommons.mainelaw.maine.edu/mlr/vol54/iss1/5

This Panel Discussion is brought to you for free and open access by the Journals at University of Maine School of Law Digital Commons. It has been accepted for inclusion in Maine Law Review by an authorized editor of University of Maine School of Law Digital Commons. For more information, please contact mdecrow@maine.edu.

INTERNET PRIVACY LAW, POLICY, AND PRACTICE: STATE, FEDERAL, AND INTERNATIONAL PERSPECTIVES[1]

Foreword and Afterword by Rita Heimes[2]

Foreword

By the summer of 2000, an estimated 90 million United States citizens used the Internet regularly, at least 69 percent of whom purchased goods and services online.[3] As electronic commerce grew, e-businesses implemented technologies to facilitate the online shopping experience. Such technologies included "cookies," which are small files a website's host computer places on a visitor's hard drive.[4] Cookies allow a website to "remember" information provided by the visitor—such as her password, email address, credit card number, and mailing address—so she does not have to reenter the data on her next visit. They also allow website operators to track a consumer's purchasing habits, monitor how long she views pages on the site, and learn other information about the consumer while she explores the World Wide Web.[5]

Cookies and related technologies enhance and facilitate electronic commerce.[6] They also raise privacy concerns. A 1999 study revealed that 92 percent of consumers were concerned about misuse of their personal information online.[7] News that online advertising giant DoubleClick planned to merge information on Internet users' surfing habits with data collected by an offline marketing firm raised a public outcry. The Federal Trade Commission opened an investigation and DoubleClick

---

1. A panel discussion presented at the second annual conference hosted by the Technology Law Center of the University of Maine School of Law—on June 7-8, 2001. The statements reproduced in this article are the opinions solely of the panelist making them. They do not represent the opinions of the University of Maine School of Law or of the panelists' employers.

2. Rita Heimes is Director of the Technology Law Center and Adjunct Professor of Internet Law at the University of Maine School of Law.

3. *Privacy Online: Fair Information Practices in the Electronic Marketplace Before the U.S. S. Comm. on Commerce, Science, and Transport.*, May 25, 2000 (prepared statement of Robert Pitofsky, Chairman, Federal Trade Commission) [hereinafter May 2000 FTC Report] (citations omitted) *available at* http://www.ftc.gov/os/2000/os/testimonyprivacy.htm.

4. Theodore Grossman and Aaron M. Grossman, *Lifting the Veil on Internet Privacy*, MEALEY'S CYBER TECH LITIGATION REPORT, Sept. 2000, at 44.

5. *Id.*

6. *Id.* at 45.

> Simply put, cookies make the Web work better. Many companies use cookies to provide valuable services to their users. Cookies frequently store passwords so that users do not need to reenter the password every time they visit the site. E-tailers like Amazon.com use cookies to track those items that a consumer has placed in his shopping cart, and even to suggest other items that complement the consumer's preferences.

Id.

7. May 2000 FTC Report.

ultimately dropped its plans.[8]

In Europe, consumer privacy concerns prompted European Union members to adopt a broad Directive on the protection of personal data in 1995.[9] Under the Directive, all Member States of the European Union are required to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[10] The term "personal data" means "any information relating to an identified or identifiable natural person," who is anyone who can be identified "by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[11] Pursuant to the Directive, such personal data can only be collected, stored, retrieved, or used (i.e., "processed") under certain limited circumstances, including with the consumer's express consent.[12]

While the EU established broad standards for individual privacy protection,[13] the United States government focused only on narrow categories of sensitive data. For instance, in 1998, Congress passed the Children's Online Privacy Protection Act (COPPA),[14] aimed at commercial Web sites that collect personal information from children under 13. In 1999, it passed the Gramm-Leach-Bliley Act (GLB),[15] which requires financial institutions to disclose their privacy policies and practices to consumers. Regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA)[16] protect privacy of medical records.[17] Proposals in the United States to regulate more broadly the online collection of personal information, however, have not yet passed into law.[18]

Indeed, the Federal Trade Commission (FTC), which enforces consumer protection laws, initially urged Congress to hold off on broad privacy legislation.[19] The FTC supported self-regulatory measures proposed by commercial website operators and online advertising firms, including principles proposed by the Network Advertising Initiative (NAI), a consortium of leading Internet advertising firms, such as DoubleClick, 24/7 Media, Engage, and related firms.[20] The NAI encouraged e-commerce companies to adopt privacy policies notifying consumers of their information gathering and dissemination practices, and giving consumers a choice to opt-out of those practices. It also encouraged such companies to use

8. John Schwartz, *Tracks in Cyberspace: Giving the Web a Memory Cost its Users Privacy*, N.Y. TIMES, Sept. 4, 2001; *see also* http://www.epic.org/privacy/internet/cookies/.

9. Council Directive 95/46/EC, 1995 O.J. (L281) 31, *available at* http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

10. Council Directive 95/46/EC, art. 1, 1995 O.J. (L281) 31.

11. *Id.*, art. 2(a).

12. *Id.*, art. 2(b), art. 7.

13. *Id.*

14. 15 U.S.C. § 6501 *et seq.*

15. *Id.* § 6801 *et seq.*

16. 42 U.S.C. § 201 *et seq.*

17. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,464 (Dec. 28, 2000) (Department of Health and Human Services' final rule).

18. *See, e.g.*, http://www.cdt.org/legislation/107th/privacy (last visited Nov. 25, 2001).

19. May 2000 FTC Report.

20. Press Release, Federal Trade Commission, Federal Trade Commission Issues Report on Online Profiling: Commends Network Advertising Initiative's Self Regulatory Principles (July 27, 2000), *available at* http://www.ftc.gov/opa/2000/07/onlineprofiling.htm. The NAI called for widespread implementation of the fair information practice principles—notice, choice, access, and security—along with a third-party enforcement program for monitoring website owners' compliance with these principles. *Id.*

third-party "privacy seals" certifying good privacy practices as a method of self-enforcement.[21]

By 2000, however, the Federal Trade Commission determined that industry efforts had been insufficient.[22] Only twenty percent of randomly-sampled websites that collected personally identifiable information implemented fair information practice principles, and only eight percent displayed a privacy seal from a certified, third-party privacy seal company.[23] That year, the FTC brought three cases accusing e-commerce firms of unfair or deceptive practices in connection with their posted privacy policies.[24] Among these cases was *FTC v. Toysmart.com*, in which the Commission challenged a bankrupt online toy company's attempts to sell personal customer information because its privacy policy had promised that such information would "never" be disclosed to a third party.[25]

In October 2000, the FTC recommended that Congress enact legislation that would "ensure adequate protection of consumer privacy online."[26] Several bills related to online privacy were introduced in 2001, including proposals requiring that e-businesses provide notice before selling or disclosing personal information and give consumers an opportunity to "opt-out" of privacy policies. Some proposals would create "safe harbors" for members of third-party privacy seal programs and preempt inconsistent state laws.[27]

In June 2001, experts in online privacy law and policy gathered for a conference hosted by the Technology Law Center at the University of Maine School of Law. The conference included a discussion on federal, state, and European privacy initiatives presented by the following panelists: Bryan Harris, former head of the Intellectual Property Division of the Commission of the European Communities and currently an adjunct professor of European Union Law at Franklin Pierce Law Center in Concord, New Hampshire[28]; Laura Mazzarella, attorney in the Division of Financial Practices of the Federal Trade Commission's Bureau of Consumer Protection[29]; Mary Ellen Callahan, associate attorney in the Washington, D.C. office of Hogan & Hartson LLP, practicing in the areas of antitrust, consumer

21. Such privacy seal providers include, for example, TRUSTe, which the FTC recently officially approved as a "safe harbor" program under COPPA. Press Release, Federal Trade Commission, TRUSTe Earns "Safe Harbor" Status: Program Will Promote Children's Online Privacy Protection Act Compliance, (May 23, 2001), *available at* www.ftc.gov/opa/2001/05/truste.htm.

22. May 25, 2000 FTC Report.

23. *Id.*

24. *Recent Developments in Privacy Protections for Consumers, Before the Subcomm. on Telecomm., Trade and Consumer Pro., of the House Comm. on Commerce,* 106th Cong. Oct. 11, 2000 (prepared statement of Robert Pitofsky, Chairman, Federal Trade Commission) [hereinafter October 2000 FTC Report]. The cases included claims based on the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices." 15 U.S.C. § 45.

25. Federal Trade Comm'n v. Toysmart.com, No. 00-11341-RGS (D. Mass., filed July 10, 2000); *see also*, Press Release, Federal Trade Commission, FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors (July 10, 2000), *available at* http://www.ftc.gov/opa/2000/07/toysmart.htm.

26. October 2000 FTC Report.

27. For a summary of legislation related to online privacy proposed in 2001, see the website of the Center for Democracy and Technology *at* www.cdt.org/legislation/107th/privacy.

28. Mr. Harris is also the Chairman of the Research Committee of the Academy of Applied Science in Concord, New Hampshire, with responsibility for the Patent, Trademark and Copyright Research Foundation. He is the former head of the European Economic Community delegation at meetings of the World Intellectual Property Organization and former head of the EEC

protection, and litigation[30]; and James Tierney, former Attorney General for the State of Maine and currently a Fellow with the Cyberspace Law Institute.[31] Susan Richey, Professor of Law at Franklin Pierce Law Center,[32] moderated the discussion. This Article reproduces the panelists' remarks with only minor editing to fit the publication format.

Discussion

Professor Susan Richey: Today, we are going to explore many of the privacy concerns that have been raised due to the incredible ease and the amazing speed with which vast amounts of private information can be processed, retrieved, and disseminated through the Internet. Due to the global nature of the medium of the Internet, it becomes very clear that privacy concerns are not purely domestic. They have been the source of discussion among the worldwide community, in the halls of our Congress, closer to home, among those who make and enforce the laws in our fifty states, as well as in the larger business community. So, today, this panel is going to make an attempt to at least outline those concerns, but I think, more importantly, from your perspective, we are going to talk about the various responses that have been formulated to try and address these very real concerns of privacy.

Without further ado, I am going to turn this over to the panel. We will start with Ambassador Harris.

Ambassador Harris: Professor Richey, Ladies, and Gentlemen, I think George Orwell has nothing on what we are facing in perhaps 2084 or even sooner than that. I am going to be very brief and say how, if at all, privacy problems have been addressed in the European Union. I say "if at all" because you may listen to a very short speech on my part since, in my view, the problem has not really been ad-

---

delegation to the Diplomatic Conference on the Revision of the Paris Convention, with rank of ambassador. Mr. Harris played a major part in drafting the Misleading Advertising Directive, the Trade Mark Directive, the Council Decision on Compulsory Licensing of Patents, and the Community Trademark Regulation. He also initiated the Community's copyright policy and the drafting of the EC Commission's Green paper on Copyright.

29. Ms. Mazzarella was a staff author of the Federal Trade Commission's 1999 and 2000 reports to Congress on Online Privacy, and lead counsel in *Federal Trade Commission v. Toysmart.com.* She heads the Division's efforts in enforcing the "pretexting" prohibitions of the Gramm-Leach-Bliley Act. Prior to joining the Commission staff, Ms. Mazzarella practiced law in San Francisco, California, focusing on intellectual property and trade secrets litigation.

30. At Hogan & Hartson, Ms. Callahan represents clients before the Antitrust Division of United States Department of Justice, the Federal Trade Commission and state Attorneys General in investigations regarding possible violations of antitrust and consumer protection laws. She has assisted consumer-oriented, health Web sites and network advertising companies to develop self-regulatory standards to govern their information collection and privacy practices. Ms. Callahan has also worked at the Congressional Research Service of the Library of Congress as part of the Special Task Force on the Development of Parliamentary Institutions in Eastern Europe.

31. Mr. Tierney also served a term as Speaker of the Maine House of Representatives. He currently consults and lectures on a variety of Internet-related legal matters confronting policymakers and state attorneys general, including online privacy issues. In 2000, he served on the Federal Trade Commission Advisory Committee on Online Access and Security.

32. Ms. Richey's courses include: Advertising Law Compliance, Trademarks and Deceptive Practices, Federal Trademark Registration Practice, Copyright Law, Information Technologies, and Introduction to Intellectual Property. She also taught "Privacy and the Internet" at the University of Maine School of Law in the summer of 2001.

equately addressed. I will give you my reasons why very concisely. There are some preliminary points that I have to make in order to put the subject in its proper perspective.

First of all, there are constraints on European Union legislation. In legal terms, all the legislation has to be *intra vires*, and *intra vires* means, in practice, that the legislation must be directed mainly towards the principal objects of the European Union. The principal objects are, above all, the creation of a barrier-free Europe. So, you do not have legislation in Europe at the European Union level on the pure merits of the subject. It has to be related to the question whether that legislation is going to promote free movement of goods and services. This is so important because you cannot, in Europe, simply legislate on copyright, or databases, or privacy, without evaluating the extent to which it promotes the free movement of goods and services within the European Union. That is quite a big constraint in many respects.

A second point is that there is no European Union law in the area of Internet privacy. This is because, instead of creating European Union law in this field of privacy—and the same goes to some extent but not entirely for intellectual property—instead of creating a special law, the national laws of the fifteen member states are harmonized. That is not quite the same thing as creating a European Union-level law. They are harmonized and, all being well, they are very similar, but not necessarily, for two reasons. One is that it is now member-state law that counts in the field of privacy, and secondly, the member states have an odd habit of legislating in a very different way, even though it may be in accordance with harmonization directives. So, that is a terribly important proviso to any general references to European law as such.

There are positive obligations on the European Union. I have referred to them as constraints. Well, in a sense that is so, but in another sense, they are not constraints at all. In Title I, Article 6 of the Treaty on the European Union, there is a provision that the Union shall respect fundamental rights as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (not a European Union document), and as they result from the constitutional traditions common to the member states as general principles of community law.[33]

That leads to what the European Convention on Human Rights actually says about privacy. Article 8 of the European Convention says everyone has the "right to respect for his private and family life, his home, and his correspondence," and

> [t]here shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and as necessary in a democratic society in the interests of national security, public safety or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[34]

So, those are the parameters within which the European Union has to work.

I have another point, generally, on European Union legislation, or rather, on attitudes to regulation. I think that this is best expressed in a recent speech given in

33. Treaty on European Union, May 1, 1999, t.t. I, art. 6, *available at* http://europa.eu.int/abc/treaties/en/entr2b.htm#1Z.

34. Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocol No. 11, art. 8, ¶¶ 1-2, *available at* http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

Brussels by one of the members of the European Commission who addressed a breakfast meeting held by one of my old friends in Brussels and who said in relation to the problem of governance and the global economy, "We need rules and regulations to manage the economic process of globalization and establish well-functioning legislative groups." I want just to emphasize that that is very much a European approach to these problems. This is an extreme case of seeking a regulatory answer to every problem.

There are three directives that have a bearing on the problems we are discussing in this conference. The first of them relates to the legal protection of databases. This was set very much in the context of intellectual property rights. Let me just very briefly read you an extract from the preamble to that directive on the harmonization of the legal protection of databases. "[C]opyright protection for databases exists in varying forms in the Member States according to legislation or case law, and if differences in legislation in the scope and conditions of protection were made between the Member States, such unharmonized intellectual property rights can have the effect of preventing the free movement of goods or services within the Community."[35] So, you see where the directive is angled. The same is true of the privacy directives.

The first one is concerned with privacy in general. It is a long directive and it is headed, "Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data."[36] Notice, once again, "the free movement of such data" appearing prominently.

There is a second directive that is concerned with protection of privacy in telecommunications. I will mention it just to state that the two directives together are the present legal framework for the European Union and between them they are, I suspect, totally inadequate to deal with the problems of the Internet as such. The second directive, on telecommunications, does not make any reference, even indirectly, to the Internet. It has been a question of lawyers doing their utmost to interpret the individual words of the telecommunications directive in such a way that the Internet is included. To some extent, they have succeeded, but not entirely. There is a gap between legislation and technical matters that is present in the concept of telecommunications in 1997, when the directive was adopted (probably drafted ten years earlier), and the technical situation that has arisen since then. So I am not going to speak too much about that telecommunications directive except to say that some lawyers are seeking to link it to the general directive on privacy and to hope that somehow or another it applies to the Internet.

Very briefly, much of the preamble to the general privacy directive is sheer verbiage. For example, it states that "data processing systems are designed to serve man." What about woman, if it comes to that? I mean, that sort of generalization, though wonderful, is not terribly helpful when it comes to legal application and the cause. Actually, the preamble to a directive is part of the law, so the preamble can be cited in cases and very often is. I think it is probably best to get to the real terms of the directive. In the second and subsequent recitals to the preamble, you have the explanation of the scheme.

---

35. Council Directive 96/9/EC, 1996 O.J. (L376) 1, *available at* http://europa.eu.int/ISPO/infosoc/legreg/docs/1969ec.html.

36. Council Directive 95/46/EC, 1995 O.J. (L281) 31, available at http://www.ensi.net/odo/akty/dysekywa%209546.htm

> [D]ata processing systems must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion, and the well being of individuals. [T]he establishment and functioning of an internal market in which the free movement of goods, persons, services, and capital is ensured require not only that personal data should be able to flow freely from one member state to another but also that the fundamental rights of individuals should be safeguarded.[37]

So, in other words, free movement first, then the safeguarding of the privacy rights. Increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity. The progress made in information technology is making the processing and exchange of such data considerably easier.

Well, all that sort of stuff is very important and very relevant but a little bit imprecise, so what about the really fine print of the directive? Well, first of all, you do have in Article 1 some useful definitions of privacy and of the various concepts that go towards the operation of the directive in practice. And you do have also, in the early revisions of the directive, some quite useful material on what is meant by "processing" of personal data. That is quite important, I think. It means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, locking, erasure, or destruction,"[38] which sounds pretty comprehensive to me.

But of course, when it really comes down to the practical facts, what it amounts to is this: The member states have to implement a system by which privacy is protected, and the directive gives what can only be called an outline of the law. It does not specify the details. Some member states already had data protection systems and laws in force. The United Kingdom was, for example, presented with some difficulties in implementing the directive, whereas, Greece, which had no previous laws on the subject, was able to implement the directive practically overnight, simply adopting similar terms. But the fact is, even that directive of 1996 has not been fully implemented by the member states. I have found from the Internet a short statement to say that the Commission of the European Communities has opened legal proceedings against four of the member states for not having done anything to implement the directive. So, we are in a difficult position there.

As for jurisdictional issues United States companies face with relation to the EU and Canada, this is one area in which it is not entirely dependent on what the individual member states have in their legislation. It is a general rule, which is enforceable by administrative means by the Commission of the European Communities. The Commission has the power to determine that a third state—which is the language they use that means any state which is not a member of the European Union and then can therefore include the United States or South Africa or anywhere else—a non-member state has insufficient protection of the data coming into the European Union, then the Commission may require the member state into

37. *Id.*

38. *Id.* at recitals.

which those unprotected data are coming to prohibit the entry of those data. When the Commission has made the determination that certain data are unacceptable because they are insufficiently protected, then the Commission instructs the member state to make the specific prohibition of that flow of information, and that is enforceable by the Court of Justice of the European Communities.

How that is going to work in relation to, for example, a member state that does not yet have the full implementation of the directive is another matter. If I were an unscrupulous advisor of a firm that wanted to send unprotected data into the European Union, I would do what exporters of goods do when they want to export into the European Union and tell them where the soft spots are. These are known to traders. It is known, for example, that if you want to export from Turkey into the European Union certain kinds of denim trousers that are not, in fact, Levi's but bear the Levi's label on them, then you go to Antwerp. That is one of those things we know. By the same token, if there are unprotected data that come from a non-member state, then obviously, and I charge no fee for this advice, you go to one of the member states that has not yet implemented the directive. You might not get away with that, but that is a first course of action. But the point remains, you see, that the Commission is all set to take action from the first of July on this directive, and it has powers to do so, but if, in fact, the directive is not fully implemented in the member states, there are lacunae.

One of the most interesting sources of discussion of the effects, if any, of the directive (and I say "if any" because if they are not even fully implemented in the member state, those effects are pretty limited) and the possibilities for revision of the European Union laws, is a very helpful paper, appropriately entitled "Privacy on the Internet"[39] and published on the European Union's website. This is, in fact, the most useful piece of material on the subject that I have been able to find in the European Union context. Briefly, it has sections on the technical description of the Internet Application of Data Protection Legislation—that, as you might imagine, is a somewhat thin part of the study—Electronic Mail, Surfing and Searching, Publications and Fora, Electronic Transactions on the Internet, Cyber Marketing, Privacy-Enhancing Measures, Conclusions,[40] and a terribly useful Glossary of Terms in which, if you did not quite get the description of a cookie, you can find it here.[41] And there are other useful terms as well. Now, this paper is on the Internet. It is very interesting. It makes up for the fact that I had to be rather short. Thank you.

Professor Richey: Thank you, Ambassador Harris. Ms. Mazzarella.

Ms. Mazzarella: Good morning. I am really happy to be here to share some of the Federal Trade Commission (FTC) staff's views. Of course, I do not speak for the Commission, and I think, at this point, it is pretty difficult to speak for the Commission or any one Commissioner.

The FTC is an independent law enforcement agency founded in 1914. We report to Congress with a broad mandate to promote efficient functioning of the marketplace by protecting consumers from unfair and deceptive practices and also increasing consumer choice through the promotion of competition. We are the

39. Article 29—DATA PROTECTION WORKING PARTY, PRIVACY ON THE INTERNET—AN INTEGRATED EU APPROACH TO ON-LINE DATA PROTECTION, 5063/00/EN/FinalWP37, adopted Nov. 21, 2000 *at* http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37en.pdf.

40. *Id.*

41. *Id.*

nation's only general jurisdiction consumer protection agency. We have jurisdiction over most industries, with some exceptions carved out. The FTC's strategies generally in the consumer protection area are targeted law enforcement, developing policies for global electronic commerce and protecting privacy online, and educating consumer businesses. It is really a three-pronged approach, and all three prongs are important in the overall consumer protection mission.

What I would like to do is talk a little bit about the FTC's role in protecting privacy and also talk about this as a consumer issue. I think we are in agreement, as we have already heard, that privacy is the next big legal issue in the next decade. It is the next technological issue in this decade, and we believe it is also the next big consumer issue. This is an issue that is not just discussed by lawyers and technologists. This is an issue that is making the front page of national newspapers. It is used in national ad campaigns on TV, such as the Earthlink campaign that ran earlier this year. It was also part of the Presidential and Congressional elections as a topic discussed by many candidates. And, of course, privacy protections are becoming an integral part of businesses. It is something that business has to take account of, through the growing matrix of privacy rules, self-regulation efforts, and just keeping up with consumer perception on this issue because a lot of damage can be done to companies' reputations when these stories come out in the news, as they so often do. What has evolved so far, what we have seen in the United States at least, is that Congress has carved out special protections for sensitive information, information about children, about finances, and about health information. That is what we have so far.

In terms of some of the background of the problem and the FTC's involvement, of course, what we have seen is the tremendous growth in Internet use and e-commerce. At the same time, however, sales and ad revenues just have not lived up to expectations, and the question is, why? What is the reason for that? Nobody is suggesting that privacy concerns are the only reason why the revenues and the ad revenues have not been what they were expected to be, but I think it is really important to look at what consumers have to say on this issue. For the past few years, there have been a number of surveys studying consumer attitudes about privacy and asking them about their concerns and what it is that they want. What we find consistently over the years is that Internet users are really concerned about other people getting their personal information. This number does not really change over time, so even as people spend more time on the Internet, and it is no longer a new thing for them, they still are very concerned about what happens with their personal information. They are also concerned about their privacy. When asked, Internet users favor opt-in privacy policies, meaning that they think they should have a choice as to how their information is used. When they give it for one purpose, they want to have a choice about how that information can be used, reused, and disclosed.

Consumers say that they want Congress to take action. They think it is time for some legislation in this area. They believe it is a major privacy violation for businesses to collect and then supply data about consumers to other companies.

I think consumers really just have no idea what has been going on. Information sharing and collection have been going on for a long time, but I think consumers are finally starting to get some awareness and they do not like it. When they hear that that is what happens, they are quite upset. Interestingly, only six percent

of consumers trust websites with their personal data. We therefore see a lot of concern and fear, and a very major trust gap.

Why is it important? One of the reasons it is important is that it does lead to reduced sales and reduced opportunities for businesses. Nearly two-thirds of Internet users at one point or another have either abandoned a purchase or refused to make a purchase because they were concerned about their privacy and what would happen to their information. And all that, of course, translates into lost sales.

So far, in the United States, there is no single law that governs online privacy rights. What we have is a collection of federal laws and regulations governing specific industries and practices. Companies need to be aware of that. They need to figure out, "Do I fit into a certain sector where I need to worry about specific legislation?" They also need to think about where they do business. The states are growing increasingly active in this area. And of course, if companies do business in Europe, Canada, Japan, Australia—a growing number of international opportunities—they need to be aware of the laws and restrictions that may apply in those regions. In the United States, the only law that is specifically geared to online privacy is COPPA, which applies to information collected from children who are thirteen and under, and it applies if a website is directed to children or if the website actually knows that it has collected information from a child under the age of thirteen. Under Gramm-Leach-Bliley—and I am sure most of you have begun to receive, if you have not already helped to draft, privacy notices from financial institutions—companies must come into compliance by July 1, 2001. The law gave companies eighteen months to get ready to comply with its privacy protections. "Financial Institutions" is defined very broadly under GLB. A lot of companies that do not think they are financial institutions may, in fact, be financial institutions if they have significant activity in finances. So, auto dealerships, for example, who do financing, are covered by the Gramm-Leach-Bliley Act; they need to pay attention to these regulations. GLB requires that notice be provided and consumers have a chance to opt-out of the sharing of their information with unaffiliated third parties. It does apply to online as well as offline communication.

The Fair Credit Reporting Act is probably our oldest consumer privacy statute, which, of course, deals with consumer credit report information and how that can be used and shared. And then we have the Federal Trade Commission Act. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce.[42] So it is a big catch-all consumer protection statute, and it can be and has been used in the privacy area as well.

On the federal level, this is really what we have. There are several different spheres of interest. Towards the end of the last session in Congress, there were a number of privacy bills being introduced. There was a lot of excitement to do something in privacy. It seemed to be a bipartisan issue and right at the end of the summer it seemed that perhaps at least a narrow bit of legislation dealing with what has become known as the Toysmart situation would pass, but it did not. At the beginning of this session, the question was not *whether* there would be privacy legislation. The question really was *when*. It was just a matter of time. It was assumed that this was the year it was going to happen. Then the forces against

42. 15 U.S.C. § 45.

legislation really rallied.

There have been a number of studies done, sponsored by industries, showing that the costs of complying with any regulation in this area would really be exorbitant and put a lot of burden on the new economy, and it seems that the interest has died down. Just this week, the Democrats have taken control of the Senate. We now have Senator Hollings chairing the Commerce Committee. Senator Hollings has been very active in the privacy area, and the legislation that he proposed last year was very protective of consumers and was an opt-in bill and very comprehensive.

At the FTC, just this week, we have a change in command. Chairman Muris was sworn in, and during his confirmation hearing he was asked a lot about privacy and what his views were. He said that this was a very important issue that needed to be studied and that he had no preconceived views as to whether or not there should be regulation in this area. So, it remains to be seen what will happen at the FTC in terms of the FTC's position on whether or not there should be regulation in this area.

As for the Bush administration, I think it is also a little too soon to say. President Bush, very early on, was actually quoted as saying that he believed that there should be opt-in privacy protection, and I do not think we ever heard that said again. But some people have used that to say, "Hey, here is our privacy President, and we are looking for great things from him." So, we do not know what is happening there yet because they have been pretty quiet on the issue.

Of course, there is tremendous activity going on at the state level as well, both with state attorneys general being aggressive using their consumer protection statutes to bring privacy actions, and also with state legislators considering new laws.

Specifically, in the privacy initiative, which began in about 1995, the FTC has conducted a number of workshops and surveys of commercial websites. We have reported to Congress annually from 1998 through 2000, brought a number of enforcement actions, and took steps to try to educate businesses, consumers, and government about the new technology and what it means for consumer privacy. We have also held a number of workshops. Typically, we look for an emerging or hot issue and try to bring a number of different points of view together—the consumer perspective, industry's perspective, the academic perspective—on a number of issues. So, for example, we were talking earlier about cookie technology and web bugs. We held a workshop in November of 1999 on online profiling that got a lot of attention and, I think, helped to educate consumers about what is going on. The most recent one was on data merger and exchange, which was prompted by a new standard that is being developed called CPExchange, which is going to facilitate the intra- and inter-company transfer of information.

We have conducted surveys and made various recommendations to Congress. The most recent recommendation was a majority of the Commission did support legislation in the area of general privacy as well as in third-party profiling. We have also brought some enforcement actions.

I will just talk for one minute, if I may, about the Toysmart case.[43] In that case, a company had a privacy policy that said, "We will never share information with third parties." They started to have financial difficulties, and even before

43. Federal Trade Comm'n v. Toysmart.com, No. 00-11341-RGS (D. Mass., 2000).

they went into bankruptcy, started advertising in the Wall Street Journal and Boston Globe that they were selling off their assets piecemeal. One of the assets available was their customer database. The FTC and in the end, I think, forty-nine or fifty states got involved to block the sale of that customer information. As one of the people who worked on that case, I can tell you I get calls almost every week from a company asking about its privacy policy or wondering if it can sell certain information in bankruptcy. There is now some pending legislation as part of a bankruptcy reform bill. Also, TRUSTE, the online seal program, has issued guidelines for its licensees to follow when they come into a situation of merger, acquisition, or bankruptcy.

In sum, there are many privacy issues that I think we all still need to look at, and I will just end there. Thank you very much.

Professor Richey: Thank you very much.

Ms. Callahan: Thank you very much. Laura and I work together a lot but we come at it from slightly different approaches. I, too, get calls from companies asking for help with their privacy policies and wondering what they can do with data. I serve as outside counsel to online companies and to bricks and mortar companies that have online representations, whether they are doing e-commerce or just having a website presence. I also work with coalitions who are interested in creating best practices on the Web and creating self-regulatory regimes that will help provide guidance and guidelines to online companies who want to protect consumers' privacy while also protecting their own businesses. It is a tough balance.

As you have heard, we have a lot of tensions. We have individual privacy concerns, and we have the business model and the interest of a company itself. We have also had the direction of the Internet overall. With all of those competing issues, as an outside counsel, it is at times difficult to promise that a client can or cannot do anything in particular with data. Inevitably, the first request I get is to draft a privacy policy. And my answer is that I cannot. What I can do is find out what the client's business practices and data practices are online, what the marketing people plan to do with the collected information, what the business people plan to do with the information, and what the legal people *think* is being done with the information.

I have noticed that my first contact is usually with the general counsel or with someone in the legal department. They say, "We are never going to sell this information." And that is great if that is, indeed, what the business model is and if that is, indeed, what is going on. But then I talk to the business people, and they tell me they have an agency relationship with another company and are actually currently giving away the information to that company. They wonder if they have to mention that in the privacy policy. Yes, you have to mention that. Then you talk to the marketing people who say, "We want to sell this. We want to sell it now. We want to sell it often. We want to really market the information." So, there are often a lot of different tensions going on within the business itself, and the privacy policy must reconcile that to give an accurate representation of what the company is doing, which represents all of the points of view from the different aspects of the company, in clear language. I think there are people in this room who would say that a lot of privacy policies are not clear, but the intent is to state what you are doing and to state it concisely, but also not to promise that you only share informa-

tion with one, specific agent. Or to give narrow exceptions, such as, "We do one thing with information." And then in two months do something slightly different.

You have got to think about how the business is going to develop without being too broad, so that the privacy policy is not useful, and without being an alarmist by saying, "We are going to sell your information all over the place." Those are the kind of tensions we have to work with.

Working with clients over the past several years, the sophistication level of my clients has risen significantly. Thanks to public disclosures and discussions of privacy matters, and the increase of attention to both personally identifiable information and, to a certain extent, non-personally identifiable information and its uses online and its uses offline, we now have clients who are thinking about these ramifications. Three or four years ago, when I was advising people on privacy policies, and I said, "Disclose third parties, mention that you have maybe a third-party ad server," I was fought tooth and nail on that point. It was very difficult.

Laura and I worked together on the Network Advertising Initiative. This is a group of third-party advertisers who have agreed to require all the companies for whom they serve ads to disclose in their privacy policies their use of a third-party ad server. That is now becoming commonplace, as the third-party ad servers and the Network Advertising Initiative have spent thousands and thousands of hours working with first-party websites to get the disclosure up on the sites to explain what is going on, to try not to make this the amorphous unknown but to disclose what is happening.

Many of my clients want to be good citizens, wanting to engender trust online. They want to be part of what is now a minority, that is what I have been trying to work on with them, both on an individual basis and on a general basis in the coalitions. The client sophistication and the public sophistication on these issues have grown significantly, and the debate changes as the understanding and the technology develop. In Washington, at least, most companies recognize that we currently have very specific legislation engendering sensitive data and its use. That is great. Everyone supports the COPPA, the GLB, and the HIPAA. I think people recognize that going forward, there is going to be more legislation of some sort, whether it is Senator Hollings or Senator McCain who controls the debate. The concerns that people have and what companies are worried about is that legislation will be technologically broad enough to encompass not just the snapshot of today and the cookies that we use today, but to talk about the next step of technology. People want legislation to be broad enough to create clear guidelines and standards without locking companies into a certain technology and protocol.

I think people are also concerned about these self-regulatory regimes that have been created, which are requiring disclosure, contracts, and privacy policies. Ideally, I think that the companies who have worked on them so hard would like them as safe harbors. I am not sure that is going to happen in the network advertising situation, but nonetheless, privacy policies are good benchmarks and bellwethers of what best practices are currently out there. So, in that sense, it is useful for Congress to look at them and to reflect on them.

The third issue that is going to be troubling for businesses and troubling for your clients is the issue of federal preemption. The issue of federal preemption is one that is very near and dear to the hearts of business because right now they have the European Union and the Directive. There is currently something called the

Safe Harbor, which the United States signed with the European Union, and there are now only forty companies who have signed up to be in the Safe Harbor. These companies are essentially saying, "We are abiding by all the issues in the directive. We are agreeing to keep by all of these standards, and we have a third-party auditor who is checking to make sure that we keep personal data in this manner." When the United States and the European Union signed this agreement in 1999, I think a lot of people expected that both offline and online companies were going to jump onboard and say, "If we are in the Safe Harbor, we cannot be prosecuted," because the European Directive says no information can go to anyplace outside the European Union that does not have adequate data protection laws. Apparently, that is us. The United States apparently is bad with data, according to the European Union. Part of it is because of the self-regulatory scheme in the United States, which Laura and I have talked about. And part of it is because we have this data-specific use of information, whether it is financial or health or children.

The EU seems to be saying we need a more regulatory approach, as Ambassador Harris referenced. So, the Department of Commerce thought, if we are going to have this Safe Harbor, everyone is going to sign up for it, and that is the way the data flow is going to continue for multinational business. The way that Safe Harbor was written, it is really geared for online information. It is not geared towards personal information and not geared towards subsidiary information, which are all covered by the European Directive. And so companies are at a loss as to what to do. Do they sign up for the Safe Harbor and kind of flag it to people? Do they meet all of these standards, or do they gamble and hope the European Union does not come after them? Starting July1, 2001, the European Union is going to start to enforce the Directive. But not only will the Directive be enforced, these multinational companies also will have to abide by all the member states' legislation that Ambassador Harris referenced. Companies have to make sure that they are keeping up with the standards.

Furthermore, then, you have got fifty-one (counting my District of Columbia) states legislating on the same issues. Whoever has the most restrictive privacy ordinance becomes the floor. Instead of having the federal legislation be the floor, which is how it is written in HIPAA and GLB, the most restrictive data issues become the floor. It could be very difficult for businesses to understand how to deal with information and know what standard governs.

Those are the questions that are facing my clients and probably your clients as well. I look forward to working in the new environment, but these are the questions that worry me.

Professor Richey: Thank you very much, Ms. Callahan, thank you. All right, Mr. Tierney.

Mr. Tierney: Thank you. In my introduction, unfortunately, Susan left out the two most important parts of my background. One is that I am a proud graduate of the University of Maine in Orono, which is a terrific school and changed my life and changed the life of many of you. I am also a graduate of this law school, of which I am very, very proud. I do not say that just because I am here. I say that wherever I speak on this subject around the country. Indeed, this is the only time I have ever spoken on this subject when I could drive to the site of speech! I am glad to be here, and I am certainly proud of my law school, but when I get done with my remarks, it is entirely possible that my law school will no longer be proud of me.

I hate this subject. I view privacy as an issue that divides people. It does not bring people together. It is mean-spirited. It is narcissistic and assumes threats and fears. It makes people think that people are inside their heads, and that is preposterous. I think it is a bad discussion in the country. I think we should be talking about bringing people together not dividing them apart. If you do not believe me, read Robert Putnam's "Bowling Alone," and you will agree after you read it.

I wish I was exaggerating. I have read for about a year and a half all these treatises about the threats to our privacy. Privacy advocates are divided into two categories: One, I am, and one, I am not. The one I am not is the Ebenezer Scrooge type. These are people who say: "I want to be left alone. Stop knocking on my doors. Stop asking for charitable donations. Get out of my life. Government, do not make me pay my child support. Leave me alone." These are privacy zealots. They are written up very well, and many of them are academics. Indeed, it seems that Dr. Jeffrey Rosen's real fear of privacy intrusions is so great that he wants to dismantle sexual harassment laws. He wants to leave women at risk in the workplace in order to protect all of our privacies. You can read it at length in his book "The Unwanted Gaze." I am not that kind of privacy advocate. I am not an Ebenezer Scrooge privacy advocate.

The second one, however, is the George Bailey view of privacy. Now George Bailey, of course, the hero of "It's a Wonderful Life," had no privacy. He knew everything about everybody in Bellows Falls, Vermont and everybody knew everything about him. And he is our hero. We sit down around the holiday season, and we watch that movie and we remind ourselves of some core American values. So, you might say well, maybe George Bailey does not care about privacy, but I say no. George Bailey cared about safety, and would oppose anyone intruding on people's safe space. He had a safe space in Bellows Falls, Vermont. That is a safe place.

If you are talking about maintaining safe places for us to be intimate and care about each other without unwanted intrusions, then I am one heck of a privacy advocate. That is how I define that term. But you have to be careful when you deal with the zealous privacy advocates because they miss this distinction very, very often.

Now, how are we going to protect ourselves? I think assuming privacy is a "right" is a huge mistake. It is terrific for our profession. You bring in tons and tons of lawyers, and you generate tons and tons of silly things that never get read, never get enforced, never get listened to. Privacy is a value, and values are protected by norms, not by laws and by regulations. It is not a right and the extent to which you try to put traditional legal analysis onto the privacy field you are going to continue to be fail. It is a norm. It is a value. And where this culture goes and where the society goes in large part can be where our privacy expectations go.

I am going to talk briefly about different forms of protection.

First, I think the European Union provides a terrific model for us for protecting people's privacy rights because the value of privacy is much, much higher in the EU, and it is much higher in Canada, than it is in the United States. They care a lot about it. Now, they have negotiated "safe harbors" with the U.S. Department of Justice and the Federal Trade Commission to give American companies a little bit of a break and they are watching very closely. They are waiting to see whether

this Administration in this country is dedicated to privacy protections. If it is not, they will enforce their privacy rules, and if the EU does not enforce, a member state will enforce, and if a member state does not enforce, a particular state in Germany will enforce. And remember, in the world of the Internet, it only takes one enforcement action to shut you down. So, the EU remains a very, very major enforcement protection for us to maintain safe spaces.

Second, our own federal government is—in my opinion—virtually worthless. I am opposed to any federal legislation. I agree with all of the business people who are saying, "Do not pass legislation." Take it from me, this Congress is not going to do anything to help any of us. If it passes a bill, it will be overly regulatory to business and it will be underprotective of any consumers. You can take that one to the bank. The new chairman, Timothy Morris, was very careful in his confirmation hearings and said he does not have any views on privacy. That is correct. He does, however, leave a long history. For example, when I was Attorney General of this state, he was the—are you ready—Director of the Bureau of Consumer Protection from 1981 to 1983 and the Director of the Bureau of Competition from 1983 to 1985. For those of you who remember FTC history, that was in the reign of Jim Miller and Dan Oliver during the Reagan administration in which they regularly appeared on behalf of defendants against state attorneys general when we tried to enforce, not just some law but any law. Last summer, he was litigating on behalf of Publishing Clearing House. Now, you all remember, those are the sweepstakes people. He said nothing they did had violated anybody's laws, but of course he was just a lawyer with a client. You cannot blame him for that, can you?

Okay, so let us look to the new head of the Director of the Bureau of Competition who was appointed last week by Mr. Muris. He is an economist. He cannot say, "I am a lawyer with a client." But he signed an affidavit on behalf of RJR saying that the Joe Camel campaign was not deceptive, was not aimed at kids, and did not do anything to increase youth rates of smoking, in his professional judgment. Now, he is going to be sitting in the head of the Bureau of Consumer Protection judging advertising. Do not worry about the FTC folks if you are representing defendants. They are history, they are toast, they are gone. Do not worry about Congress. They are history, they are toast, they are gone.

Why do you want legislation? Mary Ellen slipped; there is only one reason why they want legislation. They want it to preempt the only people who can protect you. The states and the private bar are the only people outside the EU and Canada who are going to be able to do anything to be able to really protect your rights using existing laws. State Unfair and Deceptive Trade Practice Acts are your best shot at providing consumer protection. You can have the replay of the Toysmart case when people step over the line and the companies will give up because they are not going to be able to sell goods and services.

Now, for my last two minutes, let us talk about a business model. Do not worry, no one out there is trying to invade your privacy unless they can make money. So why is it that we sit here and talk about privacy without talking about the business environment within which the whole thing operates? I mean, maybe there are a few weird cyberstalkers out there who want to read your e-mail, but the real issue is that business wants to invade privacy so they can make money. And you know what? That is a good thing. I want e-commerce to work, and to a certain degree, we all have to give up a little something if Amazon is going to remind my

kids about what they should get me for Father's Day. Somebody is going to have to give up a little privacy along the line. That is not a bad thing. That is a good thing, because I am a Dad. So, I am not against these things. That kind of commerce does not invade my safe place.

I am not coming at this from an ideological perspective, but I want safe places. Safe places could start to disappear. First of all, there is a little gizmo that was put together by a consortium down at MIT, which is going to be embedded in all of our computers or downloaded in our computers. It is supposed to give us the authority to set our own default levels as to what kind of privacy we want. However, the default levels will, of course, be set by the person in the company who owns your operating system. So, I want you to go out and look all across the country and decide which operating system you all have. Ninety-six percent of us have one from one company and it will decide the level of default that you will have, and nobody will ever change that default. In the new Microsoft "Hailstorm" world, the discussion on cookies is irrelevant because you are not going to have cookies anymore. All of the evidence is going to be residing out in Redmond on their servers because you are not going to be able to get to anybody or get back to anybody without going through the hailstorm dot-net. Upon combining the three monopolies—the Office Suite, the browser, and the operating system—you are going to have to have a little passport. You are not going to be able to get on the Internet for free anymore, and when you do, all of the evidence of your online visit will reside in Redmond. Microsoft will or will not decide the level of privacy that we will or will not have as a result, unless you believe that competition is going to arise, and there still is a slim glimmer that if justice prevails in this country, there will be some competition in that field. But you have to look at the business model and the business environment in which this is occurring because the technological results are going to stream by it.

The last point: Privacy policies, forget them. Mary Ellen's law firm promulgated these as the answer to regulation when privacy was hot, which was when a lot of those polls were taken and the FTC wanted it to look like they were going to do something. Privacy policies—have you ever read any? I mean, they are getting longer and longer and longer because Mary Ellen's firm and all of you are making them longer and longer and longer, and way down buried in the deep of them it always says that "we can change this privacy policy whenever we want." There is always a little sentence that exists within it.

So, who cares? The question is, when you log on to a website, have you already authenticated the changes they made to the policy since the last time you logged on? The privacy policy is not a meaningful protection. It never has been. I think it has been a good way to help us define norms, to help spur discussions. I think businesses are more sensitive to privacy concerns because, in their own process, they have had to struggle and work their way through what should or should not be in a privacy policy and what they are really doing with information. I think that has been very positive.

Afterword

The online collection and use of personal information remains an important issue to the Federal Trade Commission, the European Union, privacy advocates, and the public even after the terrorist attacks of September 11, 2001. In an October 4, 2001 statement, FTC chairman Timothy J. Muris noted that "[p]rivacy has become a large and central part of the FTC's consumer protection mission," and pledged to increase the Commission's "enforcement of laws protecting consumer privacy."[44] According to Chairman Muris, the FTC will, among other things, continue to enforce commercial Web sites' privacy promises and "will give priority to complaints that United States companies fail to provide privacy protections they promised under the European Union Safe Harbor Principles."[45]

Chairman Muris did not, however, endorse "legislating broad-based, privacy protections" in the United States.[46] Federal privacy legislation is currently unwise, according to Muris, because no consensus exists about privacy principles, application of access and security rules would vary from business to business, more is at stake than simply online data practices, and legislation might further slow the Internet's already slowing growth.[47] Muris recommended that Congress carefully study whether new privacy laws are required at this time.[48]

The European Union, meanwhile, has been grappling with whether network operators and Internet service providers should be required to retain so-called "traffic data" in light of law enforcement's significant interests in tracking online activities. At an EU Forum on Cybercrime held November 27, 2001, a discussion paper explained the dilemma:

> To investigate and prosecute crimes involving the use of the communications networks, including the Internet, law enforcement authorities frequently use traffic data when they are stored by service providers for billing purposes. Law enforcement authorities fear that this will reduce potential material for criminal investigations and therefore advocate that service providers keep certain traffic data for at least a minimum period of time so that these data may be used for law enforcement purposes.[49]

This suggestion contradicts EU personal data protection directives, which require that traffic data be erased or made anonymous immediately after telecommunications service is provided unless they are needed for billing purposes.[50] The Bush administration apparently favors modifying the EU directives to allow such

---

44. Remarks of FTC Chairman Timothy J. Muris, "Protecting Consumers' Privacy: 2002 and Beyond," The Privacy 2001 Conference, Cleveland, Ohio (October 4, 2001); *available at* http://www.ftc.gov/speeches/muris/privisp1002.htm.

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.*

49. Discussion Paper for Expert's Meeting on Retention of Traffic Data (Nov. 6, 2001), submitted at the EU Forum on Cybercrime, November 27, 2001; *available at* http://europa.eu.int/information_society/topics/telecoms/internet/crime/wpapnov/index_en.htm.

50. *Id.*; *see* Council Directive 95/46/EC, O. J. L 281, 23/11/1995 pp.0031-0050 (*available at* http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html), and Directive 97/66 EC, Official Journal L 024, 30/01/1998 pp.0001-0008 (*available at* http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html).

data tracking, while international privacy organizations have argued against it.[51]

The FTC chairman's current opposition to broad privacy legislation, and the Bush administration's support for increased government access to electronic communications,[52] may stall—if not defeat—proposed federal legislation mandating privacy protections for data collected online. If so, the fate of online privacy may rest with industry's continued willingness to self-regulate through privacy policies, the FTC's efforts to enforce such policies, and possibly with state-level regulation of data privacy practices.

51. Letter from International Privacy Groups to Prime Minister Guy Verhofstadt, President, EU Council of Ministers (Nov. 12, 2001); *available at* http://www.cdt.org/security/011112privacy.html.

52. On October 26, 2001, United States President George W. Bush signed into law the USA Patriot Act of 2001, which, among other things, "[a]mends the Federal criminal code to authorize the interception of wire, oral, and electronic communications for the production of evidence of: (1) specified chemical weapons or terrorism offenses; and (2) computer fraud and abuse." Public Law No. 107-56, H.R. 2975, S. 1510 (Oct. 26, 2001). Bill Summary, Title II.