

DECLARATION OF PETER P. SWIRE

I, Peter P. Swire, do hereby declare and say:

1. I am Professor of Law at the Moritz College of Law of the Ohio State University. From 1999 until early in 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. My curriculum vitae is provided as an attachment.

2. Based on my experience as a government official and a professor, Congress had a rational basis – indeed a compelling basis – for drawing a line between material stored on an ISP server, and material stored in the home. This case is about the ability of consumers to expect privacy when they do not store material on an ISP server but merely use the conduit functions provided by Internet service providers. Most notably, given the technology of 1998, Congress wished to assure individual privacy when using e-mail or browsing the web.

3. In our legal culture, nothing is more fundamental than the distinction between scrutiny of activities carried on in public and scrutiny of activities carried on in the home. Stronger protections consistently are provided, in both constitutional and statutory law, for activities of the second kind. Notably, under the Fourth Amendment, activities carried on in the home enjoy the strongest possible presumption that the persons have a reasonable expectation of privacy. As the U.S. Supreme Court made clear in *Kyllo v. United States*, 533 U.S. 27 (2001), the expectation of privacy in a person's home is so strong that a search warrant is required even for non-intrusive technologies, such as thermal imaging devices, that can be placed on public property and aimed at outside areas of a house. By contrast, documents and other materials that have been entrusted to third parties enjoy no comparable privacy expectation. *United States v. Miller*, 425 U.S. 435 (1976).

4. Similarly, the First Amendment imposes a heavy burden of justification on scrutiny of materials that are read or viewed in the home. Even the private viewing of obscene materials, which in themselves enjoy no First Amendment protection, may not be criminalized

because “the justification for ... statutes regulating obscenity ... do not ... reach into the privacy of one’s own home.” *Stanley v. Georgia*, 394 U.S. 557, 566 (1969).

5. At the time the DMCA was enacted in 1998, the dominant uses of the Internet from home were e-mail and surfing on the World Wide Web. Congress simply did not intend the subpoena provisions in the DMCA to be triggered by home use of e-mail or web surfing. Based on my own experience in government, including with the outcry over e-mail surveillance by the FBI’s Carnivore program, I do not believe that Congress in the DMCA was authorizing a private party to force an ISP to reveal the identity of senders of e-mails and surfers of web sites. *See, e.g.,* Stephen Labaton, *The Nation: Learning to Live with Big Brother*, N.Y. Times, July 23, 2000, at Sec. 4, p. 3 (describing Carnivore controversy). Yet that is precisely the result of permitting Section 512(h) subpoenas to apply to the conduit activities of Section 512(a).

6. The scope of subpoenas that could be tied to conduit activities is vast. In a computerized world where people constantly create documents, images, sounds, and other files, the amount of material subject to copyright is enormous and increasing. Given its technology virtually every act on the Internet requires the making of copies, including “reading” a web site and sending or receiving an email. Further, there are often different rights holders for the multiple rights granted by copyright law. *See* Mark A. Lemley, *Dealing with Overlapping Copyrights on the Internet*, 22 Dayton L. Rev. 547 (1997). Given the minimal showing required for “good faith” subpoenas under Section 512(h), the scope for arguably valid subpoenas increases further. The amicus briefs cite numerous examples of questionable and potentially abusive subpoenas. Other questionable Section 512(h) subpoenas could easily be conceived, such as a person claiming copyright infringement (*e.g.,* of a person’s writing or statement) when in fact they are seeking to discover the identity of a person they accuse of defamation. The identity of individuals subject to a defamation claim today must go through the John Doe process, but a critic that cites to some actual text attributed to another person might now be subject to a “good faith” Section 512(h) subpoena.

7. The potential for bad faith subpoenas, however, is even more vast. Based on my experience with the Internet, we can expect a large and geometrically growing number of abusive subpoenas that will be impossible to distinguish from legitimate subpoenas from copyright holders. For anyone who wants to reveal a speaker's identity, it will be easy to craft a legitimate-looking subpoena that Verizon will be obliged to honor "expeditiously." Many of these abusive subpoenas will come from individuals in the United States. Following the path of Web gambling sites, porn sites, and scam artists, many of the abuses could well come from offshore organizations that are beyond the reach of U.S. courts. The actual obtaining and service of such subpoenas could be done by fly-by-night operators in the United States that would open and then close Post Office boxes as quickly as possible. In short, Section 512(h) subpoenas could well become the New Spam, flooding the in-boxes of ISPs, with legitimate and illegitimate subpoenas jumbled together indistinguishably.

8. Examples of bad faith subpoenas will be as limitless as the imagination of Internet users. The most common use may be by any web site that wants to learn the identity of those who visit its site, just for marketing purposes or for more nefarious reasons, including identity theft, fraud, or stalking. Porn sites, gambling sites or other sites that would cause embarrassment, could track down anonymous surfers and demand payment not to reveal the user's identity under the pretext of enforcing a "copyright" in the content of the site. Private investigators could have a powerful new tool to turn an e-mail address (often with an anonymizing "handle") or a visit to a web site into a person's name and physical address.

9. This flood of subpoenas, unchecked by any judicial supervision, will have a chilling effect on speech protected by the First Amendment, greatly infringing home users' rights to read and write anonymously. Many users will not know how their IP address is turned into a name and address through the subpoena process. Americans will learn, however, that simply surfing the Web exposes them to the possibility of being identified. Americans will learn that

sending an e-mail under a pseudonym can easily become the equivalent of giving out their name and address.

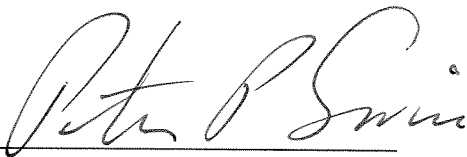
10. In my opinion, Verizon's legal position in this case reflects the policy views of Congress when enacting the DMCA. Congress did create powerful new remedies for information stored at an ISP, where the ISP itself arguably has the ability to take down infringing content after it receives notice of a copyright infringement. Congress did not, however, wish to intrude into the privacy of the home. It did not wish to have unsupervised subpoenas be sufficient to learn the identity of home users innocently surfing the Web or sending e-mails. Once a person's anonymity has been revealed, it cannot be replaced. Given the state of technology in 1998, the DMCA's distinction between conduit and non-conduit functions balanced the policy goal of taking down infringing material with the goals of preserving privacy and freedom of expression.

11. Since the DMCA was enacted, peer-to-peer and other technologies have developed in which the ISP now serves as a conduit. It is possible that Congress will craft new legislation in the future that will seek to restrain copyright infringement in peer-to-peer settings while carefully shielding the privacy and First Amendment rights of Americans engaged in web surfing, e-mail, and related activities. But Congress was contemplating web surfing and e-mail when it created Section 512(a), and the law should be thus interpreted.

12. Based on my expertise as a professor and as the Federal government's Chief Counselor for Privacy, the subpoena provision of Section 512(h), if construed to extend to service provider conduit functions, would be an extreme outlier compared with other privacy-related actions by Congress and the Executive Branch. The DMCA was enacted in 1998, when Congress was busy *increasing* privacy protections in numerous ways. The intrusions into e-mail and web surfing that follow from the RIAA's position are incongruous in light of the consistent and longstanding requirements of greater due process before releasing personally identifiable information in discovery. *See* the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §

6502(b)(2)(E)(iii) (requiring “judicial process”); the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6802(e)(8) (disclosure for financial information “to respond to judicial process”); 45 CFR § 512(e) (2002) (medical privacy rule, approved by both Clinton and Bush Administrations, requiring either court order or notice to the individual and an opportunity to object); Family Educational Right to Privacy Act of 1974, 20 U.S.C. § 1232g(b)(2) (notice and an opportunity to object for student records); Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (strict judicial process before searches of publishers and related First Amendment material); Cable Communications Policy Act of 1984, 47 U.S.C. § 551(h) (discovery only with “clear and convincing evidence”, as well as notice and opportunity to object); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710(b)(2) (showing of “compelling need” and notice and opportunity to object); Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2008(b)(3) (requiring court order); *see also* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 Minn. L. Rev. 1263 (2002) (discussing privacy policy actions in Congress during late 1990’s). To the extent there is any doubt about the proper construction of section 512(h), it should be construed in a way that recognizes the strong Congressional and Executive interest in protecting privacy.

I declare under penalty of perjury that the foregoing is true and correct. Executed on January 30, 2003.

A handwritten signature in cursive script, reading "Peter P. Swire", is written over a horizontal line.

Peter P. Swire

Attachment

PETER P. SWIRE

Professor of Law
Moritz College of Law
The Ohio State University
55 West 12th Ave.
Columbus, OH 43210

phone: (240) 994-4142
e-mail: peter@peterswire.net
web: www.peterswire.net
(Note: I reside in the Washington, D.C. area)

EMPLOYMENT

Professor of Law, Moritz College of Law of the Ohio State University, and Director of its Washington, D.C. summer law school program. Teaching at Ohio State, 1996 to April 1999, January semester 2001, fall semester 2002 and following. Promoted from Associate Professor to Professor in 1998.

Research focus on law of cyberspace, privacy, and computer security. Courses taught in those areas as well as corporations, torts, banking regulation, and other subjects. Editor, Cyberspace Law Abstracts of the Social Science Research Network (with Lawrence Lessig).

Consultant, Morrison & Foerster, LLP, Washington, D.C., 2001-present, on privacy, cyberspace, and related topics.

Chief Counselor for Privacy, Executive Office of the President of the United States, Office of Management and Budget. March, 1999 to January, 2001. Responsible for coordinating Administration policy on public- and private-sector uses of personal information, and served as point of contact with privacy and data protection officials in other countries. White House Coordinator for HIPAA medical privacy regulation; Coordinator, White House Working Group on legislative proposal to update wiretap and electronic surveillance laws; Member, White House Electronic Commerce Working Group; Member, Working Group on Unlawful Content on the Internet. Substantial work on computer security, financial privacy, and other topics.

Visiting Professor, George Washington University Law School, 2001-2002. Associate Professor, University of Virginia, School of Law, 1990-1996.

Associate, Powell, Goldstein, Frazer & Murphy, Washington, D.C., 1986-1990. Advocacy practice before Congress and agencies, on banking, environmental, high-technology and other issues.

Judicial clerk, to the Honorable Ralph K. Winter, Jr., United States Court of Appeals for the Second Circuit, 1985-86.

EDUCATION

Yale Law School. J.D. 1985; Senior Editor, Yale Law Journal; Program of Doctor of Civil Laws

(Law and Political Theory).

Université Libre de Bruxelles, Belgium. Rotary International Fellowship, 1980-81. Student, in French, at the Institute of European Studies and in Economics.

Princeton University. A.B. 1980, summa cum laude, from the Woodrow Wilson School of Public and International Affairs, with Concentration in Economics; Phi Beta Kappa.

BOOK PUBLICATION

Peter P. Swire & Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive (Brookings Institution Press, 1998).

ACADEMIC PUBLICATIONS

"Efficient Confidentiality for Privacy, Security, and Confidential Business Information," Brookings-Wharton Papers on Financial Services (forthcoming, 2003).

"Trustwrap, Or Why Electronic Commerce is Like a Bottle of Tylenol," Hastings L.J. (forthcoming, 2003).

"The Surprising Virtues of the New Financial Privacy Law," 86 Minn. L. Rev. 1263 (2002). 2002).

"Security and Privacy After September 11: The Health Care Example," 86 Minn. L. Rev. 1515 (2002) (with Lauren Steinfeld).

"Financial Privacy and the Theory of High-Tech Government Surveillance," 77 Washington U. L.Q. 461 (1999) & Brookings-Wharton Papers on Financial Services.

"Of Elephants, Mice, and Privacy: International Choice of Law and the Internet," 32 The International Lawyer 991 (1998).

"The Uses and Limits of Financial Cryptography: A Law Professor's Perspective," chapter in the proceedings of Financial Cryptography '97 (Springer-Verlag, 1997).

"Markets, Self-Regulation, and Legal Enforcement in the Protection of Personal Information," U.S. Department of Commerce, Privacy and Self-Regulation in the Information Age (1997).

"The Race to Laxity and the Race to Undesirability: Explaining Failures in Competition Among Jurisdictions in Environmental Law," Yale Law & Policy Rev./Yale J. on Regulation, Symposium: Constructing a New Federalism 67 (1996).

"Equality of Opportunity and Investment in Creditworthiness," 143 U. Pa. L. Rev. 1533

(1995).

"The Persistent Problem of Lending Discrimination: A Law and Economics Analysis," 73 Tex. L. Rev. 787 (1995).

"Safe Harbors and a Proposal to Improve the Community Reinvestment Act," 79 Va. L. Rev. 349 (1993).

"Bank Insolvency Law Now That It Matters Again," 42 Duke L.J. 469 (1992).

Litan, Swire & Winston, "The U.S. Liability System: Background and Trends," in *Liability: Perspectives and Policies* (Brookings, 1988).

Note, *The Incorporation of Independent Agencies Into the Executive Branch*, 94 Yale L.J. 1766 (1985).

Book Review, 1 Yale J. L. & Pol'y 417 (1983) (reviewing Jerry L. Mashaw, *Bureaucratic Justice: Managing Social Security Disability Claims*).

OTHER WRITINGS

Eisenach & Swire, "Ensuring Privacy's Post-Attack Survival," www.zdnet.com, Sept. 11, 2002.

Podesta and Swire, "Speaking Out About Wiretaps," *Wash. Post*, Aug. 30, 2002, at A23.

"Privacy and the Homeland Security Department," Testimony before a subcommittee of the House Judiciary Committee, July, 2002.

Comments submitted to the U.S. Department of Health and Human Services on medical privacy regulation, March, 2002.

"Privacy and the Future of Justice Statistics," *Proceedings of a National Conference on Privacy, Technology, and Criminal Justice Information*, SEARCH -- The National Consortium for Justice Information and Statistics (2001).

"If Surveillance Expands, Safeguard Civil Liberties," *Atlanta Journal Constitution*, October 21, 2001.

"Administration Wiretap Proposal Hits the Right Issues But Goes Too Far," *Brookings Terrorism Project Website*, October 3, 2001.

"Cato Privacy Paper Not Persuasive," available at Swire web site, August 10, 2001 (critiquing Tom Bell, "Internet Privacy and Self-Regulation: Lessons from the Porn Wars").

"New Study Substantially Overstates Costs of Internet Privacy Protections," available at Swire web site, May 9, 2001 (critiquing Robert Hahn, "As Assessment of the Costs of Online Privacy Protection").

"Peter Swire on Privacy, Pay Phones, and Strong Crypto," Electronic Banking Law and Commerce Report, April, 2001, p. 1 (interview on financial privacy).

Comments submitted to the U.S. Department of Health and Human Services on medical privacy regulation, April, 2001.

"Privacy is Peter Swire's Domain: Behind the Scenes He's President's Go-to Guy," by Elizabeth Weise, USA Today, June 7, 2000, Life Section, p. 1 (press profile).

Comments submitted to the U.S. Department of Commerce on the proposed safe harbor for transborder data flows, December, 1998.

"The Great Firewall of Europe," CIO Magazine, Feb. 15, 1998, at 26.

"Invasion of the Space Alien Movies," Ohio State Hearsay, Sept. 1997.

"The Consumer Credit Reporting Reform Act and the Future of Electronic Commerce Law," Electronic Banking Law & Commerce Rep., Nov./Dec. 1996.

Testimony before the U.S. Senate Banking Committee, concerning proposed reform of bank insolvency laws, June, 1995.

"Bank on Streamlined Regulation," Wall St. J., Nov. 21, 1994, at A16.

"Jonah, the Bible, and Environmental Values," Va. L. Weekly, Sept. 23, 1994, at 1.

"Lifting CRA's Threat to Mergers," American Banker, Jan. 5, 1993, at 4.

"Good Old Days Disappear in Banking Regulation," Va. L. Rept., Summer, 1991, at 21.

Eizenstat & Swire, "Try Efforts That Are Neutral of Race, Too," Los Angeles Times, Feb. 14, 1989.

"Tropical Chic", The New Republic, Jan. 30, 1989.

Lazarus & Swire, "Reactionary Activism", The New Republic, Feb. 22, 1988.

PROFESSIONAL ACTIVITIES AND HONORS

Reporter, Committee on Technology and Privacy, The Constitution Project: The Liberty and Security Initiative, 2002-present.

Editor, Cyberspace Law Abstracts of the Social Science Research Network, www.ssrn.com 1998-1999, 2001-present (on leave while in government).

Chair, Experts Group of the Center for Democracy and Technology, to analyze policy and legal issues concerning Internet privacy, 2001-present.

Consulting Expert, Organization for Economic Cooperation and Development, on project for assessing fair information practices for genetic information, 2001-present.

Advisory Panel, Council of State Governments Project on Internet Privacy in the States, 2001-present.

Distinguished Privacy Leadership Award, presented by Privacy & American Business, November, 2000.

Consulting expert, U.S. Department of Commerce, to lead inter-agency delegation to five European countries for research concerning the safe harbor principles for transfers of data between the European Union and the United States, 1998-1999

Consulting expert, Center for Legal and Social Research (headed by Dr. Alan Westin), on Model Contracts Project for Transborder Data Flows, 1998-1999.

Named Ameritech Faculty Fellow for 1997-99, in competition within Ohio State University. for project on "The Role of Law in Assuring Financial Privacy."

Editorial Advisory Board, Electronic Banking Law & Commerce Report, 1997-1999.

Secretary, American Association of Law Schools Section on Defamation and Privacy, 1998-99.

Chair, American Association of Law Schools Section on Financial Institutions and Consumer Financial Services, 1995-96; Program Chair, 1994-95; Secretary, 1993-94.

Research award from Bankard Fund for Political Economy, University of Virginia, 1992-93. research award for work in the area of banking regulation.

Associate Director of Studies, The American Agenda (assisted on domestic and economic policy issues in preparation of bipartisan report to President-elect), June-November 1988.

SPEECHES AND WORKSHOPS (through April, 2002)

“Security and Privacy in Health Care”, Fourth HIPAA National Summit, Washington, D.C., April, 2002.

Panelist, “New Issues in Medical Privacy”; Moderator, “National ID Cards” at the Computers, Freedom, and Privacy 2002 Conference, San Francisco, April, 2002.

Panelist, "Privacy After September 11: An Experts' Roundtable", Privacy & American Business Conference on Managing the New Privacy Revolution, Washington, D.C., March, 2002.

"Privacy and National Security After September 11", Library of Congress Conference on Homeland Security: The Impact of Policy Changes on Government Information Access, Washington, D.C., March, 2002.

"Privacy and the Law After September 11", Capital Law School Faculty Workshop, Columbus, March, 2002.

Plenary speech, "The Implications of September 11 to Healthcare Privacy and Security", HIPAA Summit West II, San Francisco, March, 2002.

Panelist, "Solving the Privacy Puzzle: Competition and Consumer Protection Perspectives", The Conference Board 2002 Antitrust Conference, New York, March, 2002.

Panelist, "Individual Privacy and Public Safety: Reconciling Competing Human Values" Scientific American Summit on Privacy, Security, and Safety: Preserving an Open Society in an Age of Terrorism, New York, March, 2002.

Panelist, "Tracking Terror: BioSurveillance and Medical Privacy", Scientific American Summit on Privacy, Security, and Safety: Preserving an Open Society in an Age of Terrorism, New York, March, 2002.

"Trustwrap, or Why E-Commerce is Like a Bottle of Tylenol", Johns Hopkins School of Foreign and International Affairs Conference on New Technologies and International Governance, Washington, D.C., February, 2002.

"The Surprising Virtues of the New Financial Privacy Law", Minnesota Law Review Symposium on Privacy, Minneapolis, February, 2002.

"Security and Privacy After September 11: The Health Care Example", Minnesota Law Review Symposium on Privacy, Minneapolis, February, 2002.

Panelist, "Law and Technology in Cybercrime and Homeland Security," Conference on

Information Technology and Legal Regulation of Carnegie-Mellon University, Pittsburgh, February, 2002.

Plenary Speech, "Privacy and Security Policy in the United States After September 11" and Panelist, "National and International Privacy Policy", Second Annual Privacy and Data Security Summit, Washington, D.C., January, 2002.

Panelist, "Privacy on the Internet", American Association of Law Schools Sections on Civil Rights, San Francisco, January, 2002.

SPEECHES AND WORKSHOPS (in 2001)

"Privacy and Security After December 11," University of Michigan University Lecture Series; American Society of Access Professionals; Ann Arbor & Washington, D.C., November, 2001.

"Privacy and the Internet," Democratic Forum & Institute for Policy Innovation, Dallas, November, 2001.

Panelist, "Civil Liberties in the Internet Age", Yale Law School, New Haven, CT, November, 2001.

"What Should be Hidden and Open in Computer Security: Lessons from Deception, the Art of War, Law, and Economic Theory," Telecommunications Policy Research Conference; Brookings Institution Program on Cyber-Security; and George Washington University Law School Works in Progress, October-November, 2001.

"Security and Privacy after September 11 - the Implications for Healthcare," Third National HIPAA Summit; & Glasser Legalworks Privacy Conference, both in Washington, D.C., November, 2001.

"Key New Surveillance Provisions," Privacy 2001 Conference, Cleveland, October, 2001.

"Telecommunications, Privacy, and Security after September 11", Ohio Telecommunications Associations, Cincinnati, October, 2001.

Workshop leader on *Kyllo v. United States*, George Washington University Law School, August, 2001.

"Why Medical Privacy is Happening Now -- Trust in the Online Environment," Johnson & Johnson Privacy Conference, New Brunswick, New Jersey, July, 2001.

"Medical Privacy in a Broader Privacy Context," Glasser Legalworks HIPAA Conference, Washington, D.C., July, 2001.

Panelist, Democratic Congressional Privacy Summit, U.S. Chamber of Commerce Foundation,

Leesburg, Virginia, July, 2001.

"Maintaining Trust in an Electronic World," International Banking Summer School, La Jolla, June, 2001.

"Medical Privacy in a Broader Privacy Context," HIPAA West Summit, San Francisco, June, 2001.

Panelist, "Untangling the Privacy Tech Tangle," United Health Care Conference, Atlanta, June, 2001.

"Medical Privacy in a Broader Privacy Context," Rx2001 Conference, Los Angeles, May, 2001.

"The Chief Privacy Officer for the U.S. Government," Privacy Officers Association Conference, Washington, D.C., May, 2001.

"Privacy Today and Major Corporations," American Bar Associations Corporate General Counsels Committee, Philadelphia, March, 2001.

"Reflections on the White House Privacy Office," Computers, Freedom, and Privacy, Boston, March, 2001.

"Considering Privacy in Ohio -- What Should (and Should Not) Be Done?" John Glenn Institute, Columbus, March, 2001.

Panelist, "The Promise and Peril of Genetic Information," Spitzer Lecture at the 92d Street Y, New York, February, 2001.

"Internet Privacy," Senate Bipartisan Forum on Technology and Innovation, Baltimore, February, 2001.

"Privacy and the Internet," National Press Foundation Conference on E-Commerce, Pittsburgh, Pennsylvania, February, 2001.

"Health Privacy as One, Important Privacy Concern," Consumer Summit on Health Privacy, Washington, D.C., February, 2001.

Panelist, "Carnivore and Electronic Surveillance," Ohio University Panel on Ethics and Technology, Athens, Ohio, February, 2001.

"The United States, Privacy, and Data Protection," Dutch Embassy Conference for Science and Technology Counselors, Washington, D.C., January, 2001.

Panelist, "Financial Privacy After Gramm-Leach-Bliley," American Association of Law Schools

Section on Financial Institutions and Consumer Financial Services, San Francisco, January, 2001.

In government service, speeches or presentations to events including:

American Association of Access Professionals; American Bar Association, Committee on Cyberspace; American Bar Association, Corporate Section; American Bankers Association, National Policy Conference & Annual Compliance Conference; American Health Information Management Association Conference; American Medical Association, Presidents' Meeting; American Teleservices Association Annual Conference; Annual Conference of Privacy & Data Protection Commissioners '99 & '00; Aspen Summit '00; Association of American Law Schools, Sections on International and Technology Law; Association for Electronic Health Care Transactions Policy Forum; Cato Institute; Census Bureau, Millennium Lecture Series; Center for Strategic and International Studies (twice); Chief Privacy Officers Conference; Coalition of Service Industries; Computer Systems Security & Privacy Advisory Board; Computers, Freedom & Privacy '99 & '00; Congressional Internet Caucus (twice); Consumer Bankers Association; Critical Infrastructure Assurance Office Conference; Direct Marketing Association (twice); E-Commerce in the Heart of Techtopia Conference; Electronic Commerce Practitioner Institute; Electronic Financial Services Council; Federal Bar Association Banking Law Committee; Federal CIO Council; Fedweb '99; Federal Deposit Insurance Corporation Conference on Financial Privacy; Federal Financial Institutions Interagency Privacy Group; Financial Services Institute; Financial Services Roundtable; Fordham Law Review Symposium on Privacy and the First Amendment; Freddie Mac Policy Conference; Freedom of Information Act Advanced Practitioner Conference; General Accounting Office Executive Council on Information Technology Conference; Genetic Discrimination Information Conference; Georgetown Technology Law Students Conference; Georgetown Law Journal Conference on The Unwanted Gaze: The Destruction of Privacy in America; Glasser Legalworks Financial Privacy Conference; Global Privacy Summit 2000; Health Privacy Information Alert Conference; HIPAA Health Privacy Summit; I-40 Forum on Privacy and Security; IBM Chief Marketing Officers Annual Conference; Identify Theft Summit of the Department of the Treasury; Internet Security, Trust & Privacy Association; Internet Society Conference; Mercatus Center Conference on Privacy and Legislation; Mealey's Internet Law Conference; National Automatic Clearinghouse Association Conference; National Association of State Auditors, Comptrollers and Treasurers Conference; National Consortium for Justice Information and Statistics; National Judicial Conference (committee on privacy and court records); National Press Foundation Privacy Colloquium; National Science Foundation, Computer Science & Telecommunications Board; National Telecommunications & Information Administration Conference on New Privacy Technologies; North American Securities Administrators Association Conference; Ohio Business Privacy Conference; Ohio State College of Law, Conference on ADR and Cyberspace; Online Privacy Alliance; Online Profiling Workshop of the Department of Commerce & the Federal Trade Commission; The Open Group (Internet standards organization) (twice); President's Information Technology Advisory Committee; President's Management Council; Privacy 2000 conference; Privacy & American Business, Annual Conference; Privacy & American Business, Chief Privacy Officers Conference (twice); Privacy Compliance Reporter Conference; Privacy Laws & Business Annual Conference; Progressive Policy Institute; Rx2000 Conference; Securities Industry Association; Stanford Law Review Conference on Internet Privacy; University of California, Berkeley, Conference on Electronic Commerce; U.S. Internet Council; Washington Financial Forum.