PRIVACY LAW SCHOLARS CONFERENCE

PLSC

GW LAW SCHOOL - BERKELEY LAW

OVERVIEW SPONSORS PAPERS SCHEDULE PARTICIPANTS

The 1st Annual

Privacy Law Scholars Conference

June 12-13, 2008

The George Washington University Law School

Washington, DC

Berkeley Law School and **The George Washington University Law School** have joined forces to launch the first annual Privacy Law Scholars Conference (PLSC). The PLSC aims to assemble a wide array of privacy law scholars and practitioners from around the world to discuss current issues and foster greater connections between academia and practice. It will bring together privacy law scholars, privacy scholars from other disciplines (economics, philosophy, political science, computer science), and practitioners (industry, legal, advocacy, and government). Our goal is to enhance ties within the privacy law community and to facilitate dialogue between the different parts of that community (academy, government, industry, and public interest).

The PLSC will be an annual event, alternating between Berkeley and GW Law Schools.

Hosts: The Berkeley Center for Law & Technology and the GW Law School Intellectual Property Law Program

Organizers: **Daniel Solove** and **Chris Hoofnagle**

Co-chairs: Pamela Samuelson, Orin Kerr, Paul Schwartz, Peter Swire, and Deirdre Mulligan.

Participants: A list of participants is below. Click here to download a file of bios for each participant.

Location & Directions: The conference will be held in three rooms at GW Law School -- Faculty Conference Center (FCC), Student Conference Center (SCC), and the Great Room (GR). Breakfast will be in the FCC on both days -- beginning at 8 AM on Thursday, June 12 and 9 AM on Friday, June 13. Please be sure to arrive prior to 8:45 AM on Thursday, June 12 and 9:30 AM on Friday, June 13, as afterwards, the conference will be divided into the three rooms above.

GW Law School consists of many buildings joined together, with many entrances. The best entrance is **716 20th Street** (between H and G streets). Click here for a map. This entrance is mid-block and has full glass doors with the number 716 on the glass above the doors. There are a few entrances on this block, so be sure to enter the one with the number 716. After you enter, take the gold elevator to the 5th floor (where the FCC is located). You'll see a check-in table as you exit the elevator.

SPONSORS

back to top...

The organizers of this conference thank the following sponsors for their generous support:

- **Proskauer Rose, LLP**
- **ChoicePoint**
- **AT&T**
- **IBM**

PAPERS

back to top...

Paper titles, authors, and abstracts are listed in the schedule below. There will be 4 groupings of concurrent workshops.

Prior to the conference, please select the workshop you want to attend (A, B, or C) within each of the 4 groupings. Groups 1 and 2 will be on Thursday, June 12. Groups 3 and 4 will be on Friday, June 13.

Please download one paper (A, B, or C) for each of the four groups. You should download and read 4 papers in all. Participants are expected to have read the papers in advance of the conference so that discussions can launch quickly into the issues.

You can certainly download and read more of the papers if you desire.

	A	B	C
Group 1 (June 12, 2 – 3 PM)	Christine Jolls **Privacy, Rationality, and Consent**	Aaron Burstein **Toward a Culture of Cybersecurity Research**	Peter Swire & Cassandra Butts **The ID Divide**
Group 2 (June 12, 3:30-4:30 PM)	Orin Kerr **The Case for the Third Party Doctrine**	Amy Gajda **Privacy, Ethics, and the Meaning of News**	Alessandro Acquisti & Ralph Gross **Inferring Private Data from Publicly-Available Sources**

			(please email Prof. Acquisti for a copy of his paper by clicking here)
Group 3 (June 13, 9:30 – 10:30 AM)	Paul Ohm **The Thin Line Between Reasonable Network Management and Illegal Wiretapping**	Neil Richards **Intellectual Privacy**	Lauren Gelman **Privacy, Free Speech, and "Blurry Edged" Social Networks**
Group 4 (June 13, 11 – 12 AM)	Danielle Keats Citron & David Super **Cyber Civil Rights**	Deirdre K. Mulligan & Joseph Simitian **Creating a Flexible Duty of Care to Secure Personal Information**	Peter Winn **On-Line Access to Court Records**

SCHEDULE

back to top...

Thursday, June 12, 2008

8 AM – 8:45 AM
Location: FCC

Breakfast

8:45 AM – 9 AM
Location: FCC

Introductory Remarks

9:15 AM – 10:45 AM
Location: FCC, SCC, and GR

Concurrent Roundtable Discussions: Academy

A discussion of scholarship and teaching in the academy. What issues are hot right now? Any challenges or new ideas for teaching privacy course and seminars? Where is the field heading? What direction should scholarship be heading toward? What ideas would scholars like to see adopted and used by business, government, and the public interest? What issues would practitioners like to see academics address?

10:45 AM – 11:05 AM

Break

11:05 AM – 12:30 PM
Location: FCC, SCC, and GR

Concurrent Roundtable Discussions: Practice

What issues are practitioners and advocates concerned about? What privacy issues are government officials dealing with? What are the important areas of concern right now? What are the challenges of privacy practice? What advice should academics give students who want to work in the field?

12:30 PM – 2:00 PM

Lunch

2:00 PM – 3:00 PM

Paper Workshops Group 1

Concurrent Sessions

Please plan to attend one of the following three workshops.

Prior to the conference, please download and read one of the following papers – A, B, or C.

WORKSHOP A
Location: FCC

Privacy, Rationality, and Consent
Christine Jolls
Yale Law School

The relationship between privacy rights and consent has been at the heart of privacy debates for decades. Prominent theorists have placed consent at the core of their definitions of privacy, and at the level of doctrine the traditional common law approach has viewed consent as a categorical defense to claims of privacy invasion. But both the theorists and the traditional common law approach are focused on circumstances quite different from the highly *relational* contexts in which questions of privacy and consent often arise today. In the workplace and other such relational contexts, predictable human failures of rationality frequently undermine the normative force of consent. While blanket in-advance consents are often sought, and received, for privacy invasions that might (or might not) materialize down the road, failures of rationality are a serious concern in these contexts. Interestingly, the common law of workplace privacy seems to reflect an implicit awareness of these failures of human rationality, as the legal force of consent is often blunted in just the contexts in which failures of rationality are most likely. In this sense the common law of workplace privacy can be said to track other common law rules, in areas ranging from tort law to corporate law to patent law, that are believed to reflect an implicit behavioral rationality.

WORKSHOP B

Location: SCC

Toward a Culture of Cybersecurity Research
Aaron Burstein
U.C. Berkeley Law School

Research being conducted by computer scientists offers great promise in improving cybersecurity threats in the short and long term. Progress in cybersecurity research, however, is beset by a lack of access to data from communications networks. Legally and informally protected individual privacy interests have contributed to the lack of data, as have the institutional interests of organizations that control these data. A modest research exception to federal communications privacy law would remove many of the legal barriers to sharing data with cybersecurity researchers. This reform would also counter many of the non-legal objections, such as cost and user backlash, that network providers cite as reasons not to share data with researchers.

WORKSHOP C
Location: GR

The ID Divide
Peter Swire & Cassandra Butts
The Ohio State University Moritz College of Law

This report examines how a next Administration should approach the complex issues of authentication and identification, for issues including: national and homeland security; immigration; voting; electronic medical records; computer security; and privacy and civil liberties. For many reasons, the number of ID checks in American life has climbed sharply in recent years. The result, we conclude, is what we call the "ID Divide."

The ID Divide is similar to the "Digital Divide" that exists for access to computers and the Internet. The Digital Divide matters because those who lack computing lose numerous opportunities for education, commerce, and participation in civic and community affairs. Today, millions of Americans lack official identification, suffer from identity theft, are improperly placed on watch lists, or otherwise face burdens when asked for identification. The problems of these uncredentialed people are largely invisible to credentialed Americans, many of whom have a wallet full of proofs of identity. Yet those on the wrong side of the ID Divide are finding themselves squeezed out of many parts of daily life, including finding a job, opening a bank account, flying on an airplane, and even exercising the right to vote.

Part I of this report describes the background of the issue, including the sharp rise in recent years in how often Americans are asked for proof of identity. Part II examines the facts of the ID Divide in detail. There are at least four important types of problems under the ID Divide:

1. Large population affected by identity theft and data breaches.
2. Growing effects of watch lists.
3. Specific groups disproportionately lack IDs today.
4. The effects of stricter ID and matching requirements.

Part III develops Progressive Principles for Identification Systems. These principles apply at two stages: (1) whether to create the system at all; and (2) if so, how to do it:

1. Achieve real security or other goals.
2. Accuracy.
3. Inclusion.
4. Fairness/equality.
5. Effective redress mechanisms.
6. Equitable financing for systems.

Part IV explains a "due diligence" process for considering and implementing identification systems, and

examines biometrics and other key technical issues. Part V applies the progressive principles and due diligence insights to two current examples of identification programs, photo ID for voting and the Transportation Worker Identification Card.

3:00 PM – 3:30 PM

Break

3:30 PM – 4:30 PM

Paper Workshops Group 2

Concurrent Sessions

Please plan to attend one of the following three workshops.

Prior to the conference, please download and read one of the following papers – A, B, or C.

WORKSHOP A
Location: FCC

The Case for the Third Party Doctrine
Orin Kerr
George Washington University Law School

This article offers a defense of the Fourth Amendment's third-party doctrine, the controversial rule that knowingly revealing information to a third party relinquishes Fourth Amendment protection in that information. Fourth Amendment scholars have repeatedly attacked the rule on the ground that it is unpersuasive on its face and gives the government too much power. This article responds that critics have overlooked the benefits of the rule and have overstated its weaknesses.

The third-party doctrine serves two critical functions. First, the doctrine ensures the technological neutrality of the Fourth Amendment. The third-party doctrine corrects for the substitution effect of third parties that would otherwise allow savvy criminals to substitute a hidden third-party exchange for a previously public act. Second, the doctrine helps ensure the clarity of Fourth Amendment rules. It matches the Fourth Amendment rules for information to the rules for location, creating clarity without the need for a complex framework of sui generis rules.

Finally, the two primary criticisms of the third-party doctrine are significantly weaker than critics have claimed. The third-party doctrine is awkward for reasons of form rather than function; it is a consent doctrine masquerading as an application of the Katz "reasonable expectation of privacy" test. Claims that the doctrine gives the government too much power overlook the substitutes for Fourth Amendment protection in the use of the third parties. Those substitutes include entrapment law, common law privileges, the Massiah doctrine, the First Amendment, internal agency regulations, and the rights of the third parties themselves.

WORKSHOP B
Location: SCC

Privacy, Ethics, and the Meaning of News
Amy Gajda
University of Illinois Law School

Courts, John Marshall famously declared, must "say what the law is." Increasingly, however, courts are also called upon to say what the news is. When subjects of unwanted publicity sue for invasion of privacy or other torts, journalists commonly defend on the ground that the challenged disclosures were privileged as newsworthy. Traditionally, courts minimized constitutional concerns by deferring heavily to journalists' own sense of what qualified as news; that a story made the newspapers or the evening news was itself nearly conclusive that the topic was of legitimate public interest and therefore beyond the reach of tort law. Recently, however, courts have grown decidedly less tolerant. Driven by mounting anxiety over the loss of personal privacy generally and by declining respect for the press specifically, courts are increasingly willing to impose their own judgments about the proper boundaries of news coverage. Ironically, an emerging tool used by courts to police news outlets is journalists' own codes of professional ethics. By measuring editorial decisions against gauzy internal ethics standards, courts give the appearance of deference to the profession while aggressively scrutinizing editorial judgments.

This Article demonstrates the growing threat to press freedom posed by these emerging trends. Part I places the conflict in historical context, showing how evolving legal understandings of privacy and press freedom set the two on course for a modern collision over "newsworthiness," which was resolved initially by deferring to journalists' editorial judgment. Part II explains how recent developments – including growing resort to journalists' codes of professional ethics – have undermined judicial deference to journalism in defining the news. Part III examines the implications of the nascent resurgence of tort regulation of journalism, and Part IV concludes by suggesting that courts return to a more deferential approach in assessing "newsworthiness." Specifically, it suggests that courts should have no power to punish truthful disclosures of private facts if journalists could reasonably disagree about the story's legitimate news value.

WORKSHOP C
Location: GR

Inferring Private Data from Publicly-Available Sources
Alessandro Acquisti & Ralph Gross
Carnegie Mellon University

Please email Prof. Acquisti for a copy of his paper by clicking here.

I will present results from a study of privacy risks associated with information sharing in online social networks. Online social networks such as Friendster, MySpace, or the Facebook have experienced exponential growth in membership in recent years. They are no longer niche phenomena: millions use them for communicating, networking, or dating. These networks are successful examples of computer-mediated social interaction. However, they also raise novel privacy concerns, which this research aims at quantifying. Specifically, I evaluate the risks that personal information (PI) publicly provided on a social networking site may be used to gather additional and more sensitive data about an individual, such as personally identifying information (PII), exploiting the online profile as a 'breeding' document. More broadly, these results highlight the unexpected consequences of the complex interaction of multiple data sources in modern information economies.

4:30 PM – 6:00 PM

Reception

Location: 1st Floor, Burns Hall

Friday, June 13, 2008

9:00 AM – 9:30 AM

Breakfast

9:30 AM – 10:30 AM

Paper Workshops Group 3

Concurrent Sessions

Please plan to attend one of the following three workshops.

Prior to the conference, please download and read one of the following papers – A, B, or C.

WORKSHOP A
Location: FCC

The Thin Line Between Reasonable Network Management and Illegal Wiretapping
Paul Ohm
University of Colorado Law School

AT&T made headlines when it publicly discussed aggressive plans to monitor subscriber communications on an unprecedented scale and for novel purposes. Comcast has examined packets on its network, in order to identify and throttle Bittorrent users. Charter Communications informed thousands of its customers that it would track the websites they visited in order to serve them targeted ads. These may be precursors to a storm of unprecedented, invasive Internet Service Provider (ISP) monitoring of the Internet.

Many consumer advocates have characterized these techniques as violations of network neutrality—the principle that providers should treat all network traffic the same. Trumpeting these examples, these advocates have urged Congress to mandate network neutrality.
Until now, nobody has recognized that we already enjoy mandatory network neutrality. Two forces—one technological, one legal—deliver this mandate. First, up until the recent past, the best network monitoring devices could not keep up with the fastest network connections; inferior monitoring tools have prevented providers from engaging in aggressive network traffic discrimination. These technological limitations have forced an implicit network neutrality mandate.

Second, legislatures have passed expansive wiretapping laws. Under these provisions, so-called network management techniques like those described above may be illegal. By limiting network management, the wiretapping laws mandate a sort of network neutrality. Historically, however, few Internet Service Providers (ISPs) have had to defend themselves against wiretapping charges, but as the implicit, technological network neutrality mandate fades and as ISPs respond by expanding their monitoring programs, the wiretapping laws will soon emerge as significant constraints on ISP activities.

Network neutrality has been debated for years and nearly to death, but the recognition that we already have mandatory network neutrality inverts the debate. ISPs are unable to do some things with their networks, unless and until they can convince Congress and state legislatures to change the wiretapping laws. More importantly, focusing on the wiretap laws freshens the debate, which has always been mostly about innovation, by injecting questions of privacy, surveillance, and freedom.

WORKSHOP B
Location: SCC

Intellectual Privacy

Neil Richards
Washington University School of Law

This paper is about intellectual privacy - the protection of records of our intellectual activities - and how legal protection of these records is essential to the First Amendment values of free thought and expression. We often think of privacy rules being in tension with the First Amendment, but protection of intellectual privacy is different. Intellectual privacy is vital to a robust culture of free expression, as it safeguards the integrity of our intellectual activities by shielding them from the unwanted gaze or interference of others. If we want to have something interesting to say in public, we need to pay attention to the freedom to develop new ideas in private. Free speech thus depends upon a meaningful level of intellectual privacy, one that is threatened by the widespread distribution of electronic records of our intellectual activities.

My argument proceeds in three steps. First, I locate intellectual privacy within First Amendment theory and show their consistency despite the fact that traditional metaphors for why we protect speech direct our attention to other problems. Second, I offer a normative theory of intellectual privacy that begins with the freedom of thought and radiates outwards to justify protection for spatial privacy, the right to read, and the confidentiality of communications. Third, I examine four recent disputes about intellectual records and show how a greater appreciation for intellectual privacy illuminates the latent First Amendment issues in these disputes and suggests different solutions to them that better respect our traditions of cognitive and intellectual freedom.

WORKSHOP C
Location: GR

Privacy, Free Speech, and "Blurry Edged" Social Networks
Lauren Gelman
Stanford Law School

Much of the Internet related scholarship over the past ten years has focused on the enormous benefits that come from eliminating intermediaries and allowing user generated one-to-many communications. Many have noted the tension created between the positive benefits for free speech and the negative effects on user privacy. This tension has been exacerbated by Web 2.0 technologies that permit users to create social networks with "blurry edges"-where they post information generally intended for a small network of friends and family, but left available to the whole world to access with the thought that someone they cannot identify a priori might find the information interesting or useful. This paper identifies the origin of the binary choice between public and private information as rooted in the social role of news intermediaries, and asks whether there is a legal, technical, or normative framework to permit users to maintain networks with blurry edges while still appropriately balancing speech and privacy concerns.

Part I addresses the legal and normative role news organizations play as balancers of privacy and free speech interests. It then examines how the institutional capability of the publishing entity differs in the specific cases of citizen journalists, Bloggers, Google Maps, YouTube, Flickr, and Facebook. Part II examines the binary choice users have to make between posting to the world or password protecting their information and identifies the phenomenon of what I call, "blurry edged" social networks. Part III looks at the current legal framework for analyzing privacy in the binary world, including the Computer Fraud and Abuse Act, the privacy torts, and copyright and describes the analogy to the Third Party Disclosure rule in the Fourth Amendment context. Part IV asks whether a legal framework is possible to address the privacy concerns while maintaining protections for free speech and the "generativity" benefits of the Internet. I also describe some technologies under development that might constitute an appropriate solution.

10:30 AM – 11:00 AM

Break

11:00 AM – 12:00 PM

Paper Workshops Group 4

Concurrent Sessions

Please plan to attend one of the following three workshops.

Prior to the conference, please download and read one of the following papers – A, B, or C.

WORKSHOP A
Location: FCC

Cyber Civil Rights
Danielle Keats Citron & David Super
University of Maryland Law School

Social networking sites and blogs have increasingly become breeding grounds for anonymous online groups that attack members of traditionally disadvantaged groups, especially women and people of color. These destructive groups target individuals with lies, threats of violence, and denial of service attacks that silence victims and concomitantly destroy privacy and reputations. Victims go offline or assume pseudonyms to prevent future attacks, thereby losing economic opportunities associated with a vibrant online presence and impoverishing online dialogue. Search engines also reproduce the lies and threats for employers and clients to see, creating digital "scarlet letters" that ruin reputations.

Today's destructive cyber groups update a history of anonymous mobs such as the Ku Klux Klan coming together to victimize and subjugate vulnerable people. The social science literature identifies conditions that accelerate dangerous group behavior and those that tend to defuse it. Unfortunately, Web 2.0 technologies provide all of the accelerants of mob behavior but very few of its inhibitors. With little reason to expect self-correction of this intimidation of vulnerable individuals, the law must respond.

This article argues that the harm inflicted by such destructive crowds ought to be understood and addressed as civil rights violations. Federal criminal and civil rights laws must be read to provide effective means to challenge the intimidation and harassment perpetrated by today's anonymous crowds as they have been to combat other masked mobs that menaced vulnerable groups and outspoken champions in the past.

WORKSHOP B
Location: SCC

Creating a Flexible Duty of Care to Secure Personal Information
Deirdre K. Mulligan (presenting) & Joseph Simitian
Berkeley Law School

The use of compulsory information disclosures as a regulatory tool is recognized as an important, modern development in American law. The Toxics Release Inventory (TRI), a publicly available EPA database that contains information on toxic chemical releases and other waste management activities, established under the Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA) is a widely studied example of the potential power of these comparatively light-weight regulatory interventions. The EPCRA has been credited with providing incentives for reductions and better management of toxic chemicals by firms eager to avoid

reporting releases. It has also been credited with providing information essential citizen and government engagement and action.

Drawing from a wide body of literature documenting how and why the EPCRA led to dramatic reductions in toxic releases, the paper considers the extent to which security breach notification laws are likely to produce similar results. Anecdotal evidence and some qualitative research indicate that the security breach notification laws have created incentives for businesses to better secure personal information. The law has encouraged investments in computer security as well as the development of new corporate policies. The desire to avoid incidents that trigger the reporting requirement have led businesses to reconsider decisions about where data is stored, who has access to it, under what circumstances and with what protections it can reside on portable devices or media, and to generate more detailed mechanisms of both controlling and auditing information access events. The authors, who, respectively, advised upon and authored California's security breach notification law (AB 700/SB 1386), conclude that, in contrast to previous prescriptive regulation, the reporting requirement created an evolving standard of care, in effect a race or at least rise to the top, but due to characteristics of information breaches and aspects of the current laws it has not engendered citizen engagement and organization similar to that of the EPCRA.

WORKSHOP C
Location: GR

On-Line Access to Court Records
Peter Winn
U.S. Department of Justice

In 2002, with almost no debate, US courts began using electronic filing systems. Under the earlier paper system, court records were required to be kept public to maintain the accountability of the legal system, but given the difficulty of accessing paper records, most legal files remained "practically obscure," thus still protecting the privacy of litigants. This accountability/privacy balance was dramatically changed by the shift to electronic court records, subjecting a treasure trove of sensitive information to unintended uses - from wholesale extraction by commercial data-miners to individual mischief by criminals. What is the proper balance between accountability and privacy in an age of electronic judicial information?

12:00 PM – 1:00 PM

Lunch

1:00 PM – 2:00 PM

Concurrent Roundtable Discussions

Attend discussion A, B, or C.

DISCUSSION A
Location: FCC

Death to Privacy Policies?

Nobody seems to read privacy policies, yet they form the backbone of the predominant notice and choice regime toward protecting privacy. If privacy policies don't work, what are the alternatives? Is there any alternative that isn't too paternalistic?

DISCUSSION B

Location: SCC

Issues to Watch in Criminal Procedure, Electronic Surveillance, and National Security

What are the most important emerging issues in criminal procedure, electronic surveillance, and national security?

DISCUSSION C
Location: GR

Assessing Privacy Harm

How can victims of privacy violations prove that they have been harmed?

2:00 PM – 2:30 PM

Break

2:30 PM - 3:30 PM

Concurrent Roundtable Discussions

Attend discussion A, B, or C.

DISCUSSION A
Location: FCC

How to Win Friends and Influence Policy

What do policymakers think of academic work? How can academics help policymakers? What kinds of works do policymakers find influential?

DISCUSSION B
Location: SCC

International Privacy and Transborder Data Flows

APEC, OECD, or a "third way?" What are the challenges for protecting privacy and doing business across borders?

DISCUSSION C
Location: GR

Behavioral Marketing

Federal regulators and consumers are raising concerns about the ability of marketers to target consumers based on their online behavior. How should such marketing be regulated?

3:30 PM

Conference Ends

PARTICIPANTS

back to top...

Click here to download a file of bios for each participant

Alessandro Acquisti
Assistant Professor, Carnegie Mellon University

Annie Anton
Professor, North Carolina State University

Jack Balkin
Professor, Yale Law School

William Banks
Professor, Syracuse University College of Law

Kevin Bankston
Senior Staff Attorney, Electronic Frontier Foundation

Ann Bartow
Prof., Univerisity of South Carolina

Howard Beales
Associate Professor, Strategic Management and Public Policy, George Washington University

Jerry Berman
Chairman, Center for Democracy and Technology

Gaia Bernstein
Associate Professor of Law, Seton Hall Law School

Ellen Blackler
Executive Director - Regulatory Policy, AT&T

Marc Blitz
Professor, Oklahoma City University School of Law

Bruce Boyden
Assistant Professor, Marquette University Law School

Susan Brenner
NCR Distinguished Professor of Law & Technology, University of Dayton School of Law

Julie Brill
Assistant Attorney General, Vermont Attorney General's Office

Aaron Burstein
Research Fellow, U.C. Berkeley School of Law

Ryan Calo
Resident Fellow, Stanford Law School Center for Internet and Society

Lisa Madelon Campbell
Senior Legal Counsel, Office of the Privacy Commissioner of Canada

Robert Cannon
Senior Counsel, FCC OPA

Fred Cate
Distinguished Professor, Indiana University

Danielle Citron
Assistant Professor of Law, University of Maryland School of Law

Julie Cohen
Professor of Law, Georgetown University Law Center

Raphael Cohen-Almagor
Professor, Woodrow Wilson International Center for Scholars

Lorrie Cranor
Associate Professor of Computer Science and Engineering & Public Policy, Carnegie Mellon University

Doug Curling
President & COO, ChoicePoint

Clifford Davidson
Associate, Proskauer Rose LLP

James Dempsey
Policy Director, Center for Democracy & Technology

Deven Desai
Professor, Thomas Jefferson School of Law

Will DeVries
Attorney, WilmerHale

"Dissent"
Psychologist

Carol DiBattiste
General Counsel & Chief Privacy Officer, ChoicePoint

Pam Dixon
Executive director, World Privacy Forum

Laura Donohue
Fellow, Stanford Law School's Constitutional Law Center

Henry Farrell
Assistant Professor, GWU

Edward Felten
Professor of Computer Science and Public Affairs, Princeton University

Tanya Forsheit
Partner, Proskauer Rose LLP

Alex Fowler
Co-Leader, Privacy, PriceWaterhouseCoopers, LLC

Susan Freiwald
Professor of Law, University of San Francisco School of Law

Allan Friedman
Research Fellow, Harvard University

Michael Froomkin
Professor, U. Miami School of Law

Amy Gajda
Assistant Professor of Journalism & Law, University of Illinois

Robert Gellman
Privacy and Information Policy Consultant

Lauren Gelman
Executive Director, Center for Internet and Society, Stanford Law School

Dorothy Glancy
Professor of Law, Santa Clara University School of Law

Tomas Gomez-Arostegui
Assistant Professor, Lewis & Clark Law Schol

Nathaniel Good
PhD, U.C. Berkeley's iSchool

James Grimmelmann
Associate Professor, New York Law School

Jens Grossklags
PhD Candidate, U.C. Berkeley School of Information

Joseph Lorenzo Hall
PhD Candidate, U.C. Berkeley School of Information

Allyson Haynes
Associate Professor, Charleston School of Law

Stephen Henderson
Associate Professor, Widener University School of Law

Evan Hendricks
Editor/Publisher, Privacy Times

Michael Hintze
Associate General Counsel, Microsoft Corporation

Dennis Hirsch
Professor, Capital University Law School

Lance Hoffman
Distinguished Research Professor, The George Washington University

Marcia Hofmann
Staff Attorney, Electronic Frontier Foundation

Chris Hoofnagle
Senior Fellow, Berkeley Center for Law & Technology

Stuart Ingis
Partner, Venable LLP

Christine Jolls
Professor of Law, Yale Law School

Ian Kerr
Canada Research Chair in Ethics, Law and Technology, University of Ottawa, Faculty of Law

Orin Kerr
Professor, George Washington University

Jennifer King
Research Specialist, U.C. Berkeley School of Law

David Kramer
Partner, Wilson Sonsini Goodrich & Rosati

Raymond Ku
Professor of Law, Case Western Reserve University School of Law

Rick Kunkel
Associate Professor, University of St. Thomas

James Lee
Principal, C2M2 Associates, LLC

Toby Levin
Senior Advisor, DHS Privacy Office

Jacqueline Lipton
Professor of Law, Case Western Reserve University School of Law

Tim Lordan
Executive Director, Internet Caucus Advisory Committee

Sarah Ludington
Senior Lecturing Fellow, Duke Law School

Jennifer Lynch
Samuelson Law, Technology & Public Policy Clinic Fellow, U.C. Berkeley Law School

Aaron Massey
North Carolina State University

Kristen Mathews
Partner, Proskauer Rose LLC

Andrea Matwyshyn
Assistant Professor, University of Pennsylvania

William McGeveran
Associate Professor, University of Minnesota Law School

David Medine
Partner, WilmerHale

Marci Meingast
Graduate Student Researcher, University of California Berkeley

Deirdre Mulligan
Director, Samuelson Law, Technology & Public Policy Clinic; Director, Center for Clinical Education; Clinical Professor, U.C. Berkeley School of Law

Kirk Nahra
Partner, Wiley Rein LLP

Helen Nissenbaum
Professor, New York University

Nuala O'Connor Kelly
Chief Privacy Leader, General Electric

Paul Ohm
Associate Professor, University of Colorado Law School

Paul Otto
Intern, Center for Democracy & Technology

Pablo Andres Palazzi
www.habeasdata.org

Frank Pasquale
Professor of Law, Seton Hall University

Harriet Pearson
Vice President, Regulatory Policy and Chief Privacy Officer, International Business Machines Corporation

Marcy Peek
Assistant Professor of Law, Whittier Law School

Vincent Polley
President, KnowConnect PLLC

Jules Polonetsky
Chief Privacy Officer, AOL

Tori Praul
Privacy Researcher, ACLU of Southern California

Peter Raven-Hansen
Professor of Law, George Washington University Law School

Priscilla Regan
Professor, George Mason University

Jessica Rich
Assistant Director, Federal Trade Commission

Neil Richards

Professor, Washington University School of Law

Jeffrey Rosen
Professor, George Washington Univeristy Law School

Alan Rosenberg
Vice President, Privacy, Ethics & Compliance Programs and Assistant General Counsel,

Ira Rubinstein
Senior Fellow, NYU School of Law, Information Law Institute

James Rule
Distinguished Affiliated Scholar, Center for the Study of Law and Society, UC Berkeley

Pamela Samuelson
Professor, U.C. Berkeley School of Law

Patricia Sanchez Abril
Assistant Professor, University of Miami School of Business Administration

Peter Sand
Director of Privacy Technology, U.S. Department of Homeland Security

Albert E. Scherr
Professor of Law, Franklin Pierce Law Center

Jason Schultz
Associate Director, Samuelson Clinic, U.C. Berkeley School of Law

Ari Schwartz
Vice President, Center for Democracy and Technology

Wendy Seltzer
Fellow, Berkman Center for Internet & Society

Christopher Slobogin
Stephen C. O'Connell Professor of Law, University of Florida

Thomas Smedinghoff
Partner, Wildman Harrold

Andrew Smith
Partner, Morrison & Foerster, LLP

David Sobel
Senior Counsel, Electronic Frontier Foundation

Daniel Solove
Professor of Law, George Washington University Law School

Jeff Sovern
Professor of Law, St. John's University School of Law

Michael Standard
General Attorney, AT&T

Jay Stanley

Public Education Director, Technology & Liberty Program, ACLU

Gerry Stegmaier
Partner, Wilson Sonsini; Adjunct Professor, George Mason University

Barry Steinhardt
Director, Technology and Liberty Program, American Civil Liberties Union

Tina Stow
Assistant Chief Privacy Officer, ChoicePoint

Katherine Strandburg
Associate Professor, DePaul University / New York University (visiting)

David Super
Professor, University of Maryland Law School

Peter Swire
Professor, Ohio State University

Andrew Taslitz
Professor of Law, Howard University

Brendon Tavelli
Associate, Proskauer Rose, LLC

Hugo Teufel
Chief Privacy Officer, U.S. Department of Homeland Security

David Thaw
J.D./Ph.D. Student, U.C. Berkeley

Timothy Tobin
Senior Litigation Associate, Proskauer Rose LLP

Frank Torres
Director, Consumer Affairs, Microsoft

Christine Varney
Partner, Hogan & Hartson LLP

Steve Vladeck
Associate Professor, American University Washington College of Law

Stephen Wicker
Professor, Cornell University

Peter Winn
Assistant US Attorney, U.S. Department of Justice; Adjunct Professor, University of Washington School of Law

Christopher Wolf
Partner, Proskauer Rose LLP

Tal Zarsky
University of Haifa - Faculty of Law

Michael Zimmer

Fellow, Yale Information Society Project

Diane Zimmerman
Samuel Tilden Professor of Law, New York University School of Law