

THE 14TH CONFERENCE ON COMPUTERS, FREEDOM & PRIVACY / BERKELEY, CA / APRIL 20-23

WHO IS WATCHING THE WATCHERS?



CFP2004



COMMITTEE

DEIRDRE K. MULLIGAN, Conference Chair, Boalt Hall, School of Law

HAL ABELSON, Massachusetts Institute of Technology

KIM ALEXANDER, California Voter Foundation

STEFAN BECHTOLD, University Tübingen Law School, Germany; Center for Internet and Society, Stanford Law School

BOB BLAKELY, IBM

AARON BURSTEIN, Boalt Hall, School of Law

ELSA ORTIZ CASHMAN, Special Assistant Attorney General Office of the Attorney General, State of California

LORRIE FAITH CRANOR, Carnegie Mellon University

KENNETH NEIL CUKIER, National Center for Digital Government, JFK School of Government, Harvard University

LENNY FONER, MIT Media Lab

ALEX FOWLER, Pricewaterhouse Coopers

JOHN HAN, School of Information Management & Systems, UC Berkeley

PETER HARTER, Managing Principal, The Farrington Group

MARY HODDER, School Information Management Systems, UCB

TOM KALIL, UC Berkeley

NUALA O'CONNOR KELLY, Chief Privacy Officer, US Department of Homeland Security

BRUCE KOBALL, Technical Consultant

SUSAN LANDAU, Senior Staff Engineer, Sun Microsystems Labs

ANDREW MCLAUGHLIN, Google

STEPHANIE PERRIN, Digital Discretion

LAURA QUILTER, Boalt Hall, School of Law

ANITA RAMASASTRY, University of Washington School of Law

IRA RUBINSTEIN, Microsoft

PAM SAMUELSON, Boalt Hall, School of Law

JASON SCHULTZ, EFF

ARI SCHWARTZ, Center for Democracy and Technology

PAUL SCHWARTZ, Brooklyn School of Law

GIGI SOHN, Public Knowledge

DAVE STAMPLEY, Senior Corporate Counsel and Director of Privacy, Reynolds and Reynolds

JEFF UBOIS, Internet Archive

JENNIFER URBAN, Boalt Hall, School of Law

RICK WEINGARTNER, American Library Association

MAURICE WESSLING, European Digital Rights

CONTRIBUTORS Google, M-A-D, The Open Society Institute, Public Interest Registry, Sun, Yahoo!

PATRONS & SPONSORS



Microsoft

7:30-9:00	2nd floor	COFFEE
9:00-4:30	Napa 1&2	WORKSHOP Privacy & Civil Liberties Issues in Computing Applications Research & Development
9:00-12:00	Napa 3 Sonoma Monterey Mendocino	TUTORIALS Who Are You? The Basics of Identity, Authentication and Privacy Today Network Surveillance How-To: A Tutorial Workshop on Snooping Around Networks Liability for Unsecured Computers RFID and Privacy
1:30-4:30	Napa 3 Sonoma Mendocino	TUTORIALS Constitutional Law in Cyberspace Telecommunications Law for the Rest of Us Privacy Notices: Readability vs. Completeness
6:00-8:00	Horizon	WELCOME RECEPTION

PRIVACY AND CIVIL LIBERTIES ISSUES IN COMPUTING APPLICATIONS RESEARCH & DEVELOPMENT

WORKSHOP
9:00-4:30
Napa 1&2
2nd floor

Numerous computing applications have been proposed, and in some cases implemented, that have the potential of being invasive of privacy. Examples range from commercially produced tags using Radio Frequency Identification (RFID) technology to governmental programs such as Total Information Awareness. We will discuss examples of computer science research and of applications of computing technology that raise privacy and civil liberties issues. We shall attempt to answer the following questions: (1) Is technology “neutral”? Should decisions about the applications of technology be left solely to the marketplace, the government, policy makers, and/or the law? Do the people developing the technology have any ethical, moral, or legal responsibilities regarding its subsequent use? What about businesses that market the technology? (2) Is it possible or even desirable to raise awareness of privacy and civil liberties issues among CS researchers and funders of CS research? Do researchers and/or funders have any ethical responsibilities in trying to raise awareness? (3) Is it possible to devise technologies that address privacy and civil liberties concerns? If so, what strategies might be effective in providing or increasing funding for the development of such technologies? Is there a risk in trying to develop “ameliorating” technologies? Examples? (4) Have there been examples of CS R&D projects where such issues have been successfully addressed? (5) Are there any research or development projects on which people should refuse to work? What is the role of the individual? How do you decide? What kinds of penalties might society extract? Examples? *Organizer: Barbara Simons, ACM; Presenters: Ruzena Bajcsy, University of California, Berkeley; Susan Landau, Senior Staff Engineer, Sun Microsystems Inc.: “Science—and Thinking About Ethical Solutions”;* Terry Winograd, Stanford University; Teresa Lunt, Xerox Palo Alto Research Center; Marcia Hofmann, EPIC; David Culler, University of California, Berkeley; Andrew Grosso, Andrew Grosso & Associates

WHO ARE YOU? THE BASICS OF IDENTITY, AUTHENTICATION AND PRIVACY TODAY

TUTORIAL 1
9:00-12:00
Napa 3
2nd floor

Identity issues have become part of daily business and the daily news for individuals around the world. The basic details about new identity technologies are often complex and counter-intuitive. Privacy issues are often viewed as standing in the way of better authentication and identification. But do they need to be? This tutorial will cover the terminology, standards, current controversies and best practices in privacy and authentication. We will explore the basics of important issues such as E-Authentication, biometrics, smart cards, datamining, and pattern analysis. Then we will look into basic privacy principles and see how some of the current authentication issues of the day address privacy. Commercial Web services, E-Government, transportation security, and identity fraud issues will be addressed. *Panelists: Ari Schwartz, Center for Democracy and Technology; Paula Arcioni, New Jersey Office of Information Technology; Susan Crawford, Cardozo Law School; Susan Landau, Sun Microsystems Research; Khaja Ahmed, CTO of Passport Project, Microsoft; Marty Abrams, Executive Director, Center for Information Policy Leadership at Hunton & Williams LLP; Lara Flint, Center for Democracy and Technology; Marcia Hofmann, EPIC*

NETWORK SURVEILLANCE HOW-TO: A TUTORIAL ON SNOOPING AROUND MODERN NETWORKS

TUTORIAL 2
9:00-12:00
Sonoma
2nd floor

This half-day tutorial will give you hands-on experience in network surveillance. It will provide a high-level overview of network basics, including the OSI layer model, as a prologue to getting down and dirty with packet sniffing, wireless network scanners, intercepting encrypted protocol transmissions, port scanning, and more. We'll cover everything from basic terminology to live demonstrations of how networks can be spied on, including packet sniffing, intercepting traffic, "man-in-the-middle" attacks, SSL spoofing, and more, as well as information and demonstrations on how common defense mechanisms work to protect your networks against passive and active surveillance. *Panelists: Chris Palmer, Staff Technologist, EFF; Dan Silverstein, UC Berkeley; Jeffrey Schiller, MIT*

LIABILITY FOR UNSECURED COMPUTERS

TUTORIAL 3
9:00-12:00
Monterey
2nd floor

While many companies try to minimize the expense of complying with existing laws, crucial information is being stolen, modified, and used for illegitimate purposes. What is a company's exposure to liability in the event of a breach of security? Should there be additional laws and regulations to force companies to protect private or sensitive data? Recently, new information security laws and regulations have been enacted. The Federal Trade Commission & State Attorney Generals have investigated numerous companies' security practices in response to concerns with vulnerabilities, breaches of security. Collectively, these laws, regulations, and decisions create standards, likely become the measuring stick in litigation. We'll provide a survey of recent laws, enforcement actions, and class action litigation related to information security; presents possible actions for companies; and suggests possible incentives for creating and implementing security measures. *Panelists: Françoise Gilbert, IT Law Group; Jodie Westby, The Work-IT Group; Mike Jerbic, Trusted Systems Consulting*

RFID AND PRIVACY

TUTORIAL 4
9:00-12:00
Mendocino
2nd floor

Radio frequency ID (RFID) presents the possibility of an Internet-for-things, bringing digital information economics and control into the analog, informationally limited, real world. It presents a new set of privacy risks, including the possibility of much more robust and pervasive profiling. To what degree should RFID be subject to regulatory restraints? Can we avoid privacy problems through intelligent technical design now? This tutorial is for anyone who wants to learn about the privacy/civil liberties risks posed by RFID. It will examine the technology, its current and contemplated applications, and the possibilities for political action to mitigate the privacy risks of RFID and other location/tracking technologies and practices. *Panelists: Lee Tien, EFF; Richard M. Smith; Linda Ackerman, Staff Counsel, PrivacyActivism; Beth Givens, Director, Privacy Rights Clearinghouse; Ross Stapleton-Gray*

CONSTITUTIONAL LAW IN CYBERSPACE

TUTORIAL 5
1:30-4:30
Napa 3
2nd floor

Mike Godwin, Senior Technology Counsel, Public Knowledge, will teach the basics of constitutional law in cyberspace, with an emphasis on free-speech and privacy issues. This tutorial is designed to inform non-lawyers and lawyers alike about the constitutional issues that underlie computer-crime and computer civil-liberties cases, as well as about the policy issues relating to intellectual property and jurisdiction on the Net. Its goal is to prepare attendees to understand the full range of constitutional and civil-liberties issues discussed at the main panels and presentations at CFP2004, with particular emphasis this year on the intersection of copyright law, constitutional law, and technology policy. *Presenter: Mike Godwin, Public Knowledge. Godwin has done evolving versions of this tutorial at 11 different CFP conferences, and the tutorial has continued to be well-subscribed and highly rated.*

TELECOMMUNICATIONS LAW FOR THE REST OF US

TUTORIAL 6
1:30-4:30
Sonoma
2nd floor

Primer on telecommunications law and concepts critical to understanding the scope of the FCC's regulatory authority over the Internet. Covers the original regulation of telephone companies under a "common carrier" model, and the gradual removal of services such as data storage and long-distance service from the framework of monopoly regulation, a process that culminated in the 1996 Telecommunications Act. It will also provide an overview of today's hot regulatory topics. It will introduce the major players: FCC commissioners; relevant congressional commissions; state public utility commissions; & affected industries. It will review the classification of Internet access as unregulated "information services," and explain the practical implications of classification as a regulated "telecommunications service." Finally, it will provide background on debates about broadband Internet access, wireless telephony & networks, including spread-spectrum and smart-radio technology, and voice over IP. *Panelists: Lee Tien, EFF, Christopher Savage, Cole, Raywid & Braverman; Robert Cannon, Federal Communications Commission*

PRIVACY NOTICES: READABILITY VS. COMPLETENESS

TUTORIAL 7
1:30-4:30
Mendocino
2nd floor

Research has established that notices need to be relatively short, in a common format and in plain English to work for consumers. However, such notices are, by definition, not complete. This creates liability issues for companies. Sometimes, laws are conflicted over what lawmakers want from organizations giving notice. This tutorial will explore the research, government action on short notices, and the liability issues. *Panelists: Marty Abrams, Center for Information Policy Leadership; Ari Schwartz, Associate Director, Center for Democracy and Technology; Rebecca Richards, Director of Policy, TRUSTe; Beth Givens, Executive Director, Privacy Rights Clearinghouse; Ken McEldowney, Executive Director, Consumer Action; Jennifer Barrett, Privacy Team Leader, Axiom*

7:30-8:30	Claremont Ballroom	CONTINENTAL BREAKFAST (sponsored by Google)
8:30-8:45	Empire Ballroom	OPENING REMARKS: CHAIR, DEIRDRE MULLIGAN
8:45-9:45	Empire Ballroom	OPENING KEYNOTE: DAVID DILL
		PLENARIES
9:45-11:00	Empire Ballroom	'Overseeing' the Poor
11:15-12:30	Empire Ballroom	Tapping the Net Revisited: Voice Over IP and Law Enforcement
12:30-2:15		CONCURRENT SESSIONS AND WORKING LUNCH
1:00-2:00		CONCURRENT SESSIONS
	Napa 1&2	RFID and Privacy
	Sonoma	Technology Transfer, Technology Dumping
	Monterey	Gatekeepers of the Web: The Hidden Power of Search Engine Technology
	Napa 3	Nations vs. the Net: The UN World Summit on the Information Society (WSIS)
		PLENARIES
2:15-3:30	Empire Ballroom	Datamining the Unknown Unknowns
3:30-4:00	Claremont Ballroom	COFFEE BREAK (sponsored by Hewlett-Packard)
4:00-5:15	Empire Ballroom	Organizing Online for Political Change
		SPECIAL EVENT
5:15-7:00	Empire Ballroom	Screening: "Misleading Information: The Future As It Never Was"
7:00-9:30	Horizon	BIG BROTHER AWARDS (AT CLAREMONT)
9:30-midnight		BOF SESSIONS

8:30-8:45 **OPENING REMARKS**
Empire Ballroom Chair, Deidre Mulligan

DAVID DILL, PROFESSOR OF COMPUTER SCIENCE, STANFORD UNIVERSITY

KEYNOTE
8:45-9:45
Empire Ballroom
1st floor

"The Battle for Accountable Voting Systems"
Touch-screen voting machines store records of cast votes in internal memory, where the voter cannot check them. Because of our system of secret ballots, once voters leave the polls there is no way anyone can determine whether the vote captured was what the voter intended. Why should we trust these machines? Last December, I drafted a "Resolution on Electronic Voting" stating that every voting system should have a "voter verifiable audit trail"—a permanent record of the vote that can be checked for accuracy by the voter, and which is saved for a recount if it is required. After many rewrites, I posted the page in January with endorsements from many prominent computer scientists. At that point, I became embroiled in a surprisingly fierce (and time consuming) battle that continues today. We still don't have an answer for why we should trust electronic voting machines, but a lot of evidence has emerged for why we should not. In this talk, I will discuss the basic principles and issues in electronic voting.

'OVERSEEING' THE POOR: TECHNOLOGY PRIVACY INVASIONS OF VULNERABLE GROUPS

PLENARY 1
9:45-11:00
Empire Ballroom
1st floor

2004 marks the 40th Anniversary of the '64 Civil Rights Act. This landmark Act outlawed discrimination in public places, required employers to provide equal employment opportunities, and stated that uniform standards for the right to vote must prevail. We will explore the relationship between privacy and civil rights, in light of the anniversary, focusing on the segment of our population who are without computers but constantly subject to computer monitoring. Computer systems have not eliminated discrimination—on the contrary: Discrimination has been grafted into profiling algorithms, taking on airs of impartiality. We will focus on three prominent issues that intersect computing and disadvantaged populations: Homeless Management Information Systems, Credit Scoring, and Biometric Collection of information on recipients of public benefits. Moderator: Chris Hoofnagle, EPIC; Panelists: Cindy Southworth, National Network to End Domestic Violence; Chance Martin, SF Coalition on the Homeless; Birny Birnbaum, "Insurance Credit Scoring: 21st Century Redlining"

TAPPING THE NET REVISITED: VOICE OVER IP AND LAW ENFORCEMENT

PLENARY 2
11:15-12:30
Empire Ballroom
1st floor

The FBI is back, insisting that VoIP be subject to the same wiretap-friendly design mandates that apply to the plain old telephone system under the controversial CALEA legislation. The FBI recently filed a petition asking for an FCC rulemaking on the issue. Will the desire to guarantee law enforcement access reach into the core of the Internet? What are the risks of tapping the Net? Can surveillance questions be rationally addressed

in the age of terrorism? *Moderator: John Morris, Center for Democracy and Technology; Panelists: Jeff Pulver, pulver.com; Lee Tien, EFF; Steve Bellovin, AT&T Lab-Research, Mike Warren, fiducianet.biz*

RFID AND PRIVACY

CONCURRENT 1
1:00-2:00
Napa 1&2
2nd floor

Radio frequency ID (RFID) presents the possibility of an “Internet-for-things,” bringing digital information economics and control into the analog, informationally limited, real world. It presents a new set of privacy risks, including the possibility of much more robust and pervasive profiling. To what degree should RFID be subject to regulatory restraints? Can we avoid privacy problems through intelligent technical design? *Panelists: Beth Givens, Director, Privacy Rights Clearinghouse; Elliot Maxwell, Fellow, Center for the Study of American Government, Johns Hopkins; Jackie Griffin, Director, Berkeley Public Library; Jonathan Weinberg, Wayne State University Law School; Ann Brick, Staff Attorney, ACLU of Northern California*

TECHNOLOGY TRANSFER, TECHNOLOGY DUMPING

CONCURRENT 2
1:00-2:00
Sonoma
2nd floor

US and European technologies have made their way across the world through global commerce. However, technologies have different applications and implications under different cultures and legal regimes. In China firewall technology is used as a tool of censorship, a wall to keep citizens in rather than to keep hackers out. What is being done to ameliorate negative and positive and advance impacts of technology? *Panelists: Xiao Qiang, China Internet Project; Jagdish Parikh, Online Communications Content Coordinator, Human Rights Watch; Dave Del Torto, CryptoRights Foundation*

GATEKEEPERS OF THE WEB: THE HIDDEN POWER OF SEARCH ENGINE TECHNOLOGY

CONCURRENT 3
1:00-2:00
Monterey
2nd floor

People use search engines for the vast majority of online content they access—giving a handful of companies the ability to shape what the world sees and thinks about. Unbeknownst to users, search engine companies effectively censor content in subtle ways, both for commercial reasons and when asked by governments. Ranking technologies provide users with a homogenized handful of sites that render smaller sites nearly invisible. Search engine results are famously prone to manipulation. Using search engines is more complex than it seems and general users have difficulty finding the right content. The panel exposes hidden vulnerabilities of these critical gatekeepers to the online world, and considers remedies. *Moderator: Kenneth Neil Cukier, Fellow, Harvard’s Kennedy School of Government; Panelists: Prof. Dr. Marcel Machill, Professor for Journalism & International Media Systems, Univ. of Leipzig, Germany, and the Bertelsmann Foundation: “Transparency on the Net: Search Engines and Media Policy”; Andrew McLaughlin, Google; Matthew Hindman, Fellow, Harvard’s Kennedy School of Government; Benjamin Edelman, Student, Harvard University.*

NATIONS VS. THE NET: THE UN WORLD SUMMIT ON THE INFORMATION SOCIETY

CONCURRENT 4
1:00-2:00
Napa 3
2nd floor

Are governments trying to take over the Internet? Are their actions indispensable to bringing the benefits of the information society to all? Or is it something in the murky middle, where the details (and devils!) lie? In Dec. 2003 over 10,000 delegates from governments, industry and activist groups convened in Geneva for the first round of the UN World Summit on the Information Society (WSIS). There was little harmony on issues—from human rights and the digital divide, to open source software and ICANN. Join us for a meeting to discuss the issues, the stakes and the dangers that will emerge as the world prepares for the final round of the Summit, in Tunisia in 2005. *Panelists: Stephanie Perrin, President, Digital Discretion; Peter Harter, Managing Principal, The Farrington Group; Kenneth Neil Cukier, Fellow, Harvard’s Kennedy School of Government*

DATAMINING THE UNKNOWN UNKNOWN: IS IT USEFUL FOR KNOWING WHAT WE DON'T KNOW WE DON'T KNOW?

PLENARY 3
2:15-3:30
Empire Ballroom
1st floor

Search and analysis of structured and unstructured data races in parallel to the ever increasing volume of information generated globally by people and technology. Technology continually converts analog to digital, adding to the complexity of information. These developments erode security through obscurity individuals have historically enjoyed. This panel will discuss the positive and negative aspects of the business and government activities which capitalize and exploit person-based data. *Moderator: Peter Swire, former chief counsel for privacy in Clinton Administration; Panelists: Jeff Jonas, SRD; Lara Flint, Center for Democracy and Technology; Stewart Baker, former counsel at National Security Administration; Doug Tygar, Professor, UC Berkeley*

ORGANIZING ONLINE FOR POLITICAL CHANGE

PLENARY 4
4:00-5:15
Empire Ballroom
1st floor

Can online organizing change the outcome of the 2004 elections? From the “open-source” campaign model that briefly propelled Howard Dean to the front of the Democratic pack, to the stunning impact of Moveon.org, American politics is being turned upside down by new and innovative network-centered campaign strategies. Or is it? We will examine recent trends and explore their implications on the 2004 election and American Democracy, discussing what tools and strategies have worked—and failed—in recruiting and mobilizing supporters. *Moderator: Jonah Seiger, GWU; Panelists: Bill Pease, Get Active; Wes Boyd, MoveOn.org; Tom Mattzie, AFL-CIO; Myles Weissleder, Vice-President of Communications, Meetup.com*

“MISLEADING INFORMATION: THE FUTURE AS IT NEVER WAS”

SCREENING
5:15-7:00
Empire Ballroom
1st floor

This video screening brings back the futuristic promises of the past—alluring, utopian ideas like domestic robots, ubiquitous networking, telepresence, and intelligent appliances—and shows how major American corporations appropriated them as their own. Their promise: a bright, affluent future enabled by cybernetics and technology, and they’re still singing the same song. We’ll counterpose films like *Century 21 Calling, A Nation At Your Fingertips*, and *Magic In The Air* with recent futuristic TV commercials from AT&T and IBM. What (if anything) has changed? Why has utopian fantasy become campy anachronism rather than call to action? And would we really want to live in this utopian world, anyway? *Presenter: Rick Prelinger, Prelinger Archives*

BIG BROTHER AWARDS

AWARDS
7:00-9:30
Horizon
1st floor

Privacy International holds the 6th annual US Big Brother awards to celebrate the invaders and champions of privacy. “Orwell” statutes will be presented to the government agencies, companies and initiatives which have done most to invade personal privacy. Brandeis Awards will be given to champions of privacy. The Brandeis Award is named after US Supreme Court Justice Louis Brandeis, who described privacy as “the right to be let alone.” The awards are given to those have done exemplary work to protect and champion privacy.

THE GREAT AMERICAN PRIVACY MAKEOVER, UNDRESSED: SURVEY RESULTS & METHODOLOGY

BOF 1
9:30-midnight
Napa 1
2nd floor

In July, 2003, PC World conducted what is thought to be the largest journalistic survey of its kind: The magazine asked 1500 people to provide details about their online privacy practices and motivations. In this session, the author of the survey and the head of PC World’s research division will discuss the methodology for conducting the survey, and present more results than there was space to report in print in the November, 2003 issue. *Presenters: Andrew Brandt, Senior Associate Editor, PC World; Lisa Huck, Director, PC World’s Research Department*

JAPAN’S NEW PRIVACY PROTECTION RULES, CITIZEN NUMBERING, AND THREATS TO CIVIL LIBERTIES

BOF 2
9:30-midnight
Mendocino
2nd floor

Between 1998 and 2003 Japan’s national Diet passed a series of laws that will fundamentally reshape the relationships among free speech, government surveillance and individual privacy. Among other things, the new laws create the country’s first comprehensive citizen numbering system, provide rules requiring confidentiality of personal information, and provide the first formal legal authority for wiretaps. Another new law established Japan’s first national freedom of information system. The speaker will provide an overview of all these developments and will solicit comments from participants, especially seeking to draw comparisons with developments in the United States and elsewhere. *Presenter: Lawrence Repeta*

THE FUTURE OF THE PATRIOT ACT

BOF 3
9:30-midnight
Monterey
2nd floor

Is the Patriot Act a foreshadow of things to come, or an aberration soon to be corrected? What are specifics of the Act, of “Patriot II”, and their pluses and minuses? What are the courts doing about the Act, and how should computer professionals respond as responsible citizens? First, a description of the Patriot Act, the proposals in “Patriot II,” the history of the various provisions, and a description of court cases that are coming down the pipe. Then a round table discussion as to the pluses and minuses of the Act’s

purposes and means; where these might lead in the future; and role of technology in such evolution. *Presenter: Andrew Grosso, Andrew Grosso @ Associates*

COMPUTERS, PRIVACY AND MOORE'S LAW

BOF 4
9:30-midnight
Napa 2
2nd floor

Moore's Law promises the semiannual continual doubling of transistors on a Silicon chip. It has stressed copyright law, and its continued vitality promises to unleash previous limits on digital transmissions. Further, the presence of more and smaller Internet-connected devices has begun to raise questions about the fate of privacy in the networked world. This BOF will consider the implications of Moore's Law on public policy questions pertaining to computer freedom, including copyright, telecommunications, and privacy. *Presenter: Drew Clark, Senior Writer, National Journal's Technology Daily*

NEW CFP ATTENDEES TOWN HALL (TENTATIVE)

BOF 5
9:30-midnight
Lanai 2
1st floor

BOF session for those with no obvious "flock": this 90-minute town meeting will try to orient first or second attendees at a CPSR conference on how to make the most of their expensive trip. Meet newbies like yourself! Later, we'll compare notes.

CREATIVE COMMONS USERS' MEETING

BOF 6
9:30-midnight
Lanai 3
1st floor

Open content is revolutionizing content creation and distribution just like open source has changed software business. Everyone who are using Open Content Licensed material or are interested of open content licensing are invited to a the BOF to hear a presentation of Creative Commons and legal issues of open content licensing. The BOF gives an opportunity to exchange experiences of sharing open content. *Organizer: Herkko Hietanen*

MOBILOPHOBIA

BOF 7
9:30-midnight
Sonoma
2nd floor

MobiloPhobia asks whether we should fear the friend in our pocket, investigating how the mobile phone functions as a tracking device, through which our movements can be monitored 24 hours a day. Mobile phones routinely generate location data, which is stored by the operators, and regularly used in court cases and by the intelligence services. This is cell based and simply records the closest mast to the handset against time, while triangulation techniques allow for far greater accuracy, and the radar-like Celldar™ system offers the capability to pull up a real-time visual display of objects by analyzing deviations in the microwave radiation emitted by mobile phone masts. MobiloPhobia will assess the technical capacity of different mobile phone surveillance techniques, and examine how artists and DIY technologies offer alternative ways of engaging in surveillance to traditional campaigning strategies. On the one hand creative projects that test the limits of new locative technologies offer the chance to inhabit or explore the blind spots and incoherencies of surveillance systems. And, on the other, the emerging field of locative media explores the use of location aware portable networked devices for social networking and cultural projects, highlighting socially beneficial applications and creating an argument for safeguards and openness to be integral to the platforms of tomorrow. (www.mobileconnections.org, www.futuresonic.com) *Presenter: Dr. Drew Hemment, AHRB Research Fellow in Creative Technologies at University of Salford, UK*

SAN FRANCISCO SURVEILLANCE CAMERA PLAYERS

BOF 8
9:30-midnight
Napa 3
2nd floor

The San Francisco Surveillance Camera Players oppose the surveillance of everyday life, in particular the video surveillance of public space, including public transit, streets, and parks. We perform short, silent plays in front of surveillance cameras in public places, to bring attention to and challenge their presence. We also are beginning to map the locations of surveillance cameras in the Bay Area and give occasional walking tours. We will discuss how to identify surveillance cameras, how common they are in the Bay Area, and what some of the issues are (legal, Constitutional, and moral). A walking tour is also scheduled for the following Saturday, April 24th. It meets at 2pm by the statue in the middle of Union Square in San Francisco (take the BART to Powell Street, then walk three blocks north on Powell). *Players: Martin and Bettina. More information can be found at www.surville.org*

7:30-8:45	Claremont Ballroom	CONTINENTAL BREAKFAST (sponsored by Yahoo!)
		PLENARIES
8:45-10:00	Empire Ballroom	Trusted Computing
10:00-11:15	Empire Ballroom	Open Source, Open Society
11:15-1:30		CONCURRENT SESSIONS AND WORKING LUNCH (pick up lunch 11:15-11:45 on 2nd floor)
11:45-12:45		CONCURRENT SESSIONS
	Sonoma	Wardriving, Wireless Networks & the Law
	Napa 1&2	Privacy and Liberty Implications of Suing File Sharers
	Mendocino	Fahrenheit 451.3: Using ISPS to Control Content on the Internet
	Monterey	Data Retention and Privacy: A 'Real World' Approach to EU and US Regulations
	Napa 3	The Next Drug War: Possession Statutes Target Technology
		PLENARIES
1:00-2:15	Empire Ballroom	The Net: Caught in the FCC'S Web?
2:15-3:45	Empire Ballroom	Facing the Music: Can Creators Be Paid for P2P File Sharing?
3:45-4:15	Claremont Ballroom	COFFEE BREAK
4:15-5:30	Empire Ballroom	The Council of Europe Cybercrime Treaty
7:00-10:00	Offsite	EFF PIONEER AWARDS (at Chabot Space and Science Center)
10:00-midnight		BOF SESSIONS

TRUSTED COMPUTING

PLENARY 5
8:45-10:00
Empire Ballroom
1st floor

Recent technology initiatives described as “Trusted Computing” have been very controversial. We’ll examine how they work and what their advantages and disadvantages may be from a variety of points of view. *Moderator: Danny Weitzner, W3C and Computer Science & Artificial Intelligence Laboratory, MIT; Panelists: Seth Schoen, Staff Technologist, EFF; David Safford, IBM; Geoffrey Strongin, Platform Security Architect, AMD*

OPEN SOURCE, OPEN SOCIETY

PLENARY 6
10:00-11:15
Empire Ballroom
1st floor

As governments increase the use of technology and bring functions online for everything from birth certificates, paying taxes, and voting, the software that is used determines the degree of transparency and freedom. Open source proponents claim that open source lets citizen users inspect, improve and redistribute the software freely, and point out that commercial software risks locking up official documents in proprietary formats. But commercial software advocates point out the benefits to a single entity claiming responsibility for their work. What are the risks and benefits to each model? *Panelists: Tony Stanco, E-Government; Bernardo Benhamou, French Government; Jason Matusow, Microsoft*

WARDRIVING, WIRELESS NETWORKS, AND THE LAW

CONCURRENT 5
11:45-12:45
Sonoma
2nd floor

Wireless networks are exploding in popularity, but are difficult to secure. Locating insecure networks & advertising their locations has become a sport known as “wardriving.” We examine the Pen Register Act, the Wiretap Act, the Electronic Communications Privacy Act, the Computer Fraud & Abuse Act to evaluate criminal & civil liability which may apply to wardriving. *Panelists: Steve Schroeder, CCIPS consultant; Simon Byers, AT&T; Kevin Bankston, EFF*

PRIVACY AND LIBERTY IMPLICATIONS OF SUING FILE SHARERS

CONCURRENT 6
11:45-12:45
Napa 1&2
2nd floor

Copyright owners have sued P2P network services, providers of software, ISPs, phone companies, and even venture capitalists who fund P2P companies. While those initial suits were successful, content industries have recently suffered reversals, most notably in their litigation against Streamcast & Grokster. Unable to shut down P2P networks altogether, the music industry has begun to sue individuals who upload music files. These lawsuits present numerous legal, moral and policy issues. What First Amendment and privacy rights are affected by the RIAA’s subpoenas to ISPs’ file sharers’ identities? How to balance the fact that P2P software has legal uses as well as illegal ones, with the RIAA’s claims that it is more efficient, and better business, to sue the P2P software companies rather than users? Or should the RIAA simply find a new business model? *Moderator: Mark Lemley, Professor, Boalt Hall School of Law, UC Berkeley, and Of Counsel, Kecker & Van Nest; Panelists: Stacey Dogan, Associate Professor of Law, Northeastern University School of Law; Jon Healey, Los Angeles Times; Wendy Seltzer, Staff Attorney, Electronic Frontier Foundation*

FAHRENHEIT 451.3: USING ISPS TO CONTROL CONTENT ON THE INTERNET

CONCURRENT 7
11:45-12:45
Mendocino
2nd floor

Recently, governments have tried a controversial new approach to regulating Internet content: requiring ISPs to block access to content, such as pornography and gambling, before it is delivered to Internet users. Targeting neither the source nor host of the content, this content control instead places the burden of blocking content on the delivering ISP. Yet this approach often leads to the blocking of wholly unrelated content. We'll look at the court decision on the Pennsylvania web blocking law, and other state efforts to control content at the ISP bottleneck. *Moderators: John Morris, Center for Democracy & Technology; Stewart Baker, former counsel at National Security Administration; Panelists: Wolfgang Schultz, University of Hamburg*

DATA RETENTION AND PRIVACY: A 'REAL WORLD' APPROACH TO EU AND US REGULATIONS

CONCURRENT 8
11:45-12:45
Monterey
2nd floor

Data retention of ISP-generated traffic data is a major issue, not only for privacy protection but even for the enforcement of the right of defense in court. We'll analyse first the difference and similarity between EU and US and, from a technical point of view, at which conditions the ISP retained data might be held reliable in Court. *Presenters: Andrea Monti, Electronic Frontier, Italy; Susan Brenner, University of Dayton School of Law; Cindy Cohn, Electronic Frontier Foundation*

THE NEXT DRUG WAR: POSSESSION STATUTES TARGET TECHNOLOGY

CONCURRENT 9
11:45-12:45
Napa 3
2nd floor

Suing customers appears to be in vogue. But long before the RIAA got in on the action, DirecTV blazed the trail. Today, state "super DMCA" initiatives across the US aim to make "mere possession" of general purpose technologies unlawful, encouraging others to go where only DirecTV has dared to go before. What are the implications for civil liberties and general purpose technologies when lawyers can come for you for "mere possession"? *Moderator: Fred von Lohmann, EFF; Panelists: Jason Schultz, EFF; Van Stevenson, Motion Picture Association of America; Albert Zakarian, Esquire, DTVDefense.com; Christian Genetski, Partner, Sonnenschein, Nath & Rosenthal, Anti-Piracy Counsel for DirecTV; Robert S. Apgood, Attorney at Law, AvantLaw PLLC*

THE NET: CAUGHT IN THE FCC'S WEB?

PLENARY 7
1:00-2:15
Empire Ballroom
1st floor

The FCC has long had a role in regulating (or not regulating) the Internet. In the past years it has been reviewing that role. This panel will provide an overview of the FCC's current plans and examine the implications for the future of the Internet, focusing not only on concrete regulatory issues but also policy issues about competition and/or openness, network neutrality, the "end-to-end" principle and the very concept of common carriage. Can FCC regulation or regulatory forbearance foster openness, competition, and neutrality? *Panelists: Lee Tien, EFF; Chris Savage, Cole, Raywid & Braverman; Robert Cannon, Senior Counsel for Internet Issues (Federal Communication Commission's Office of Plans and Policy); Jeff Pulver, President and CEO, Pulver.com, Inc.; Dan Brenner, Senior Vice President for Law & Regulatory Policy, National Cable & Telecommunications Association; Paul Misener, Vice President, Global Public Policy, Amazon.com*

FACING THE MUSIC: CAN CREATORS GET PAID FOR P2P FILE SHARING?

PLENARY 8
2:15-3:45 pm
Empire Ballroom
1st floor

While the entertainment industry litigated and lobbied, many observers concluded that P2P is an exciting technology with one significant downside: paying authors & artists for their work. The file sharing wars inspired widely divergent proposals for fostering online distribution and paying authors and artists. We'll consider leading alternatives, including digital rights management, compulsory licenses and levies, voluntary collective licensing, and voluntary user payments. We'll focus on nuts & bolts, rather than debating the file-sharing wars. We'll ask which proposals could work. What are their practical advantages & drawbacks? How do they measure consumer demand? How do they affect privacy? *Moderator: Jessica Litman, Wayne State Univ. Law School. Panelists: Ted Cohen, EMI; Sarah Deutsch, Verizon; Eric Garland, CEO, BigChampagne, LLC; Daniel Gervais, Univ. of Ottawa Faculty of Law; Neil Netanel, UT School of Law; Fred von Lohmann, EFF*

THE COUNCIL OF EUROPE CYBERCRIME TREATY—THE TREATY MOST OF THE NET HASN'T HEARD OF, BUT THAT MAY CHANGE IT FOREVER

PLENARY 9
4:15-5:30 pm
Empire Ballroom
1st floor

The Council of Europe Cybercrime Treaty is an international agreement created for the stated purpose of helping police cooperate on crimes that take place on the Internet. Its supporters, including the US DOJ, argue that it is a surgical instrument necessary to allow for international law enforcement cooperation in prosecuting crime on the Net. Opponents say it is like a meat axe, requiring signatory nations to cooperate with foreign dictatorships and give invasive new surveillance powers to law enforcement. While the treaty has broad implications for the wired world, it has received very little attention since 9-11. President Bush recently sent the Treaty to the Senate for ratification, which will rekindle the controversy in the US. *Moderator: Gus Hosein, Fellow, Privacy International; Panelists: Barry Steinhardt, American Civil Liberties Union; Betty Shave, Computer Crimes and Intellectual Property Section of the US Justice Department; Tracy Cohen, London School of Economics & Consultant to the South African Broadcasting Authority*

PIONEER AWARDS

AWARDS
7:00-10:00 pm
Offsite at Chabot

EFF established the Pioneer Awards to recognize leaders on the electronic frontier who are extending freedom and innovation in the realm of information technology. The International Pioneer Awards nominations are open both to individuals and organizations from any country. All nominations are reviewed by a panel of judges chosen for their knowledge of the technical, legal, and social issues associated with information technology.

BOF 9 “MISLEADING INFORMATION: THE FUTURE AS IT NEVER WAS”

10:00-midnight
Location TBA

Repeat of screening. *Presenter: Rick Prelinger, Prelinger Archives*

TRAVEL DATA AND PRIVACY

BOF 10
10:00-midnight
Mendocino
2nd Floor

This BOF will provide an update and overview of (1) current proposals for government and commercial uses of travel data and the conversion of the travel reservation infrastructure into a system for surveillance of travelers, including CAPPS-II, US- VISIT, APIS, biometric and RFID passports and travel documents, the jetBlue Airways and Northwest Airlines “sharing” of reservation archives, and current and potential policies and practices for commercial uses of travel reservation archives; (2) the status of related regulatory and legislative activity and litigation in the USA, EU, Canada, and international standard-setting bodies such as IATA and ICAO; (3) *Gilmore v. Ashcroft*, *Hiibel v. Nevada*, and anonymous travel; and (4) strategizing for responses and initiatives to protect and defend the privacy of travelers and the right to travel. *Presenter: Edward Hasbrouck, Author, “The Practical Nomad”, Hasbrouck.org*

DIGITAL COPYRIGHT IN EUROPE AND ASIA: HOW DOES IT DIFFER FROM THE U.S.?

BOF 11
10:00-midnight
Napa 3
2nd Floor

This BOF will present the discussions on digital copyright in Europe, Japan and China. It will explore how these discussions differ from those taking place in the United States, and how they are influenced by the United States. It is widely recognized that the United States has been leading the digital copyright policy discussions on the international level (such as TRIPS and WIPO) and influencing other countries’ policies. However, the United States is not the only country in which policy makers, lawyers and technologists debate about digital copyright issues. The BOF will cover: how Europe is trying to solve the problem of balancing anti-circumvention regulations and user freedoms; how its strategies differ from the fair use approach taken in the U.S., and what pros and cons these two strategies have in the digital environment; how the Japanese copyright law currently respects and preserves user freedom; how the Koizumi Administration is trying to expand the scope of copyright regulations inspired by the U.S. pro-IP policy in the 1980’s; how China has changed its copyright law in the past two decades under U.S. diplomatic and political influence; and, finally, the vigorous opposing voices against a stronger copyright policy as well as unexpected copyright and other legal issues arising from the digital freedom movement in China. *Presenters: Yugo Noguchi, Stanford University Law School; Qiong Wu, UC Berkeley, School of Law (Boalt Hall)*

LITIGATING SURVEILLANCE: HOW TO FIGHT THE USA PATRIOT IN COURTS

BOF 12
10:00-midnight
Napa 1
2nd Floor

Lawyers and legal activists are invited to brainstorm solutions to the legal hurdles facing any challenge to the USA PATRIOT Act's surveillance provisions. In particular, we'll talk about how to find plaintiffs with standing to challenge surveillance laws that operate in secret, and what legal theories may succeed in the face of a decades-long weakening of Fourth Amendment protections. After 10-15 minutes of introductory comments from Kevin Bankston outlining the various legal hurdles facing lawyers hoping to challenge the PATRIOT Act's surveillance provisions, attendees will participate in an interactive discussion of innovative approaches and potential solutions to these problems. *Presenter: Kevin Bankston, EFF*

DESIGNING IN PRIVACY: ARCHITECTURE AND STRATEGY DISCUSSION

BOF 13
10:00-midnight
Monterey
2nd Floor

Technologists, developers, policy makers and advocates are invited to a discussion with the HP Chief Privacy Officer and a HP Trusted Systems Lab scientist to explore the needs of developers to design and build privacy-compliant and privacy enabling products and systems. We will focus on ideas that contribute to the practical application of design: tools, training, impact assessments and review guides. *Presenters: Barb Lawler, HP; Tomas Sander, Research Scientist, Hewlett-Packard Laboratories*

SCREENING: "HACKTIVISTA" DOCUMENTARY

BOF 14
10:00-midnight
Sonoma
2nd Floor

"Hacktivist" is the story of three University of Toronto students who travel with their professor to Guatemala and Chiapas to work with human rights organizations and activists on Internet security and connectivity. The students call themselves "hacktivists"—a new breed of social activists who use technology to fight for privacy and freedom of speech. See www.citizenlab.org/hacktivist for more info. *Presenter: Robert Guerra, consultant to and translator for the documentary, will introduce the documentary and answer questions after the screening.*

SOFTWARE DEMONSTRATION: PROGRAM FOR ONLINE DELIBERATION

BOF 15
10:00-midnight
Napa 2
2nd Floor

Demonstration of POD, a new open platform for online deliberation: an asynchronous, web-based tool for group discussion, collaboration, and decision making. POD is a project of PIECE (Partnership for Internet Equity and Community Engagement, <http://piece.stanford.edu>). *Presenter: Todd Davies, Coordinator, Symbolic Systems Program, Stanford University, and Partnership for Internet Equity and Community Engagement*

EXHIBIT: OBSERVING SURVEILLANCE

BOF 16
10:00-midnight

Discussion of the exhibit.

GAMING: THE PATRIOT ACT

BOF 17
10:00-midnight

7:30-8:45	Claremont Ballroom	CONTINENTAL BREAKFAST
		PLENARIES
8:45-10:15	Empire Ballroom	Policy Laundering
10:15-11:30	Empire Ballroom	Government Profiling / Private Data
11:45-1:15	Claremont Ballroom	KEYNOTE & LUNCH: RACHEL BRAND
1:30-2:30		CONCURRENT SESSIONS
	Mendocino	Identity Theft: Addressing the Problem at a Global Level
	Sonoma	Cease and Desist: Two Years of Fighting Online Chill
	Napa 1&2	Next Generation Democracy: Internet, Young Voters & Election 2004
	Monterey	The Law and Ethics of Online Research
	Napa 3	Security and Privacy for the Citizen in the Post 9-11 Digital Age: European Perspective
2:45-3:15	Empire Ballroom	SPECIAL EVENT: VERIFIED VOTING MOCK ELECTION
		PLENARY
3:15-4:30	Empire Ballroom	Electronic Voting: The Great Paper Trail Debate
4:30-5:30	Empire Ballroom	CLOSING KEYNOTE: BREWSTER KAHLE

POLICY LAUNDERING

PLENARY 10
8:45-10:15
Empire Ballroom
1st floor

Governments are becoming increasingly adept at using international forums' influence over the laws of other jurisdictions, and the push for "harmonization," supposedly demanded by globalization, to further domestic policy agendas. Using these various tools they exert pressure, and at times circumvent, the traditional deliberative process. Many controversial policies influencing freedom, privacy and copyright policy, such as the Digital Millennium Copyright Act and the Cybercrime Treaty, on digital networks are the result of such efforts. *Moderator: Tom Kalil, UC Berkeley; Panelists: Gus Hosein, Fellow, Privacy International; Becky Burr, Wilmer Cutler Pickering LLP*

GOVERNMENT PROFILING / PRIVATE DATA

PLENARY 11
10:15-11:30
Empire Ballroom
1st floor

The US government's use of corporate databases containing personal information on individuals in its effort to identify terrorists has garnered criticism from elected officials, private citizens, and other nations. Simultaneously, elected officials, think tanks, and those involved in intelligence and law enforcement argue that identifying terrorists requires enhanced access and use of information. We'll consider the current legal framework controlling government access and its use of private sector databases, privacy and security concerns, and possible benefits of their use. *Moderator: Nick Gillespie, Reason Magazine; Panelists: Danny De Temmerman; Jennifer Barrett, Acxiom; Lisa Dean, Transportation Security Administration; Bill Skannell, DontSpyOnUS.com; Jim Harper, Privacilla*

11:45-1:15
Claremont Ballroom

KEYNOTE & LUNCH: RACHEL BRAND, PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL, OFFICE OF LEGAL POLICY, US DEPARTMENT OF JUSTICE
Introduced by Microsoft

CONCURRENT 10
1:30-2:30
Mendocino
2nd floor

IDENTITY THEFT: ADDRESSING THE PROBLEM AT A GLOBAL LEVEL

Identity theft reaches beyond borders. Recently credit card information of US citizens was used to manufacture false cards in Romania, which then were used in the EU. To efficiently combat cybercrime and ID theft, countries must cooperate to create a system of protection & enforcement that goes beyond each country's borders. We'll provide actual examples of Identity theft schemes; analyze existing and pending cyber security laws, protections, and initiatives in different countries that address directly or indirectly Identity theft and suggest potential coordinated actions. *Moderator: Françoise Gilbert, IT Law Group; Panelists: Jody R. Westby, The Work-IT Group; Jacques F. Gilbert, First Data Corp.; Joanne McNabb, Chief Office of Privacy Protection, State of California*

CONCURRENT 11
1:30-2:30
Sonoma
2nd floor

CEASE AND DESIST: TWO YEARS OF FIGHTING ONLINE CHILL

During the course of the conference (or before, if you're less fortunate) you may have been served with a cease-and-desist demand letter making outrageous allegations that your online activities violate the law. The Chilling Effects Clearinghouse (chillingeffects.org) has been collecting and cataloguing these letters for the past two years and fighting online chill. We'll give a weather map from data we've gathered, assessing the climate for online activity. *Panelists: Wendy Seltzer, Electronic Frontier Foundation; Jennifer M. Urban, UC Berkeley School of Law (Boalt Hall)*

CONCURRENT 12
1:30-2:30
Napa 1&2
2nd floor

NEXT GENERATION DEMOCRACY: INTERNET, YOUNG VOTERS & ELECTION 2004

The 18-24 year-old age group exhibits a vigorous attachment to online community, from P2P networks to IM and text messaging. Will these attachments spill over into the physical, and the political world? Will these attachments stick with youth as their own demographics change? This panel will explore the ways that the Internet has been used to engage youth in politics and in Election 2004. *Moderator: David M. Anderson, Executive Director, Youth '04; Panelists: Vincent M. Keenan, President, Publius.org, and Michigan Secretary of State; Thomas A. Bryer, Director, Party Y; David B. Smith, Mobilizing America's Youth*

CONCURRENT 13
1:30-2:30
Monterey
2nd floor

THE LAW AND ETHICS OF ONLINE RESEARCH

A lawyer and an ethicist will lead a discussion regarding the unique ethical and legal issues of privacy, anonymity, consent, and data ownership that attend on-line research, and regarding the formulation of guidelines for conducting such research. *Panelists: Dan Burk, Oppenheimer Wolff & Donnelly Professor of Law, University of Minnesota; Charles Ess, Professor of Philosophy and Religion and Distinguished Research Professor of Interdisciplinary Studies, Drury University*

CONCURRENT 14
1:30-2:30
Napa 3
2nd floor

SECURITY AND PRIVACY FOR THE CITIZEN IN THE POST 9-11 DIGITAL AGE: A EUROPEAN PERSPECTIVE

Identity is a unifying concept bringing together security and privacy aspects under one roof. The European Union has developed a strong legal and regulatory framework in order to properly manage the balance between these two aspects while respecting the fundamental rights of the citizen. This balance, strongly influenced by cultural environments in each country, has been challenged recently by emerging information and communications technologies and post 9-11 policy initiatives. In this panel, technical experts will provide an overview of the future of identity in Europe and its impact on security & privacy. Presentations will be followed by a discussion between European privacy proponents & representatives from law enforcement agencies about the future challenges related to identity. *Moderator: Emilio De Capitani, Civil Servant, European Parliament, Secretary of Committee on Citizen's Rights, Justice and Home Affairs; Panelists: Laurent Beslay, Scientific Officer, Institute for Prospective Technological Studies (IPTS), European Commission; Paul De Hert, Associated Professor, University of Leiden, Netherlands, and Professor of Law, University of Brussels, Belgium; Marie-Helene Boulanger, Justice and Internal Affairs, European Commission*

SPECIAL EVENT
2:45-3:15
Empire Ballroom
1st floor

VERIFIED VOTING MOCK ELECTION

Two candidates will stump us all in an election for "CFPer of the Year" at a mock election designed to raise some of the issues brought up by electronic voting systems with and without an auditing capability. Run by Verified Voting Founder David Dill, this election will employ real election officials impersonating mock election officials representing California and Florida and will serve as an excellent introduction to the Electronic Voting panel that follows. Join us for a fun way to explore this important topic and support the candidate you like best. Who knows what might happen to your vote! *Presented by the Verified Voting Foundation*

PLENARY 12
3:15-4:30
Empire Ballroom
1st floor

ELECTRONIC VOTING: THE GREAT PAPER TRAIL DEBATE

If your next vote is cast on a touch screen voting machine, how will you know that it was counted correctly? Many computer scientists and public interest groups argue that voter verified paper ballots are a necessary check for the integrity of elections. Opponents of voter verified paper ballots counter that they unnecessarily complicate the voting process, add expenses, and make providing access for the disabled more difficult, without really improving the integrity of elections. *Moderator: Lorrie Faith Cranor, Associate Research Professor, Carnegie Mellon University; Panelists: David Wagner, Assistant Professor, UC Berkeley; Douglas A. Kellner, Commissioner, NYC Board of Elections; Kim Alexander, California Voter Foundation; Michael I. Shamos, Distinguished Career Professor, Carnegie Mellon University; Scott Konopasek, Registrar of Voters, San Bernardino County, CA; Dan Tokaji, Assistant Professor of Law, Ohio State University, Moritz College of Law*

4:30-5:30
Empire Ballroom

CLOSING KEYNOTE: BREWSTER KAHLE, DIGITAL LIBRARIAN, INTERNET ARCHIVE
"Universal Access to All Human Knowledge"