



APRIL 20 TUESDAY

7:30-8:45	CONTINENTAL BREAKFAST
9:00-4:30	WORKSHOP: Privacy and Civil Liberties Issues in R&D
9:00-12:00	TUTORIALS: Who Are You? Identity and Privacy Basics Network Surveillance How-To Liability for Unsecured Computers RFID and Privacy
1:30-4:30	TUTORIALS: Constitutional Law in Cyberspace Telecommunications Law for the Rest of Us Privacy; Readability vs. Completeness
6:00-8:00	WELCOME RECEPTION

PRIVACY AND CIVIL LIBERTY ISSUES IN COMPUTING APPLICATIONS AND RESEARCH AND DEVELOPMENT

9:00-4:30 WORKSHOP 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 it 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

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

9:00-12:00 TUTORIAL 1 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; Susan Crawford, Khaja Ahmed, Microsoft; Paula Arcioni, New Jersey Office of Information Technology; Alana Maurushat, University of Hong Kong; Susan Landau, Sun Microsystems Research

NETWORK SURVEILLANCE HOW-TO: SNOOPING AROUND MODERN NETWORKS

9:00-12:00 TUTORIAL 2 This half-day tutorial workshop 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 network against passive and active surveillance. Panelists: Dan Moniz, EFF; Dan Silverstein, UC Berkeley; Jeffrey Schiller, MIT

LIABILITY FOR UNSECURED COMPUTERS

9:00-12:00 TUTORIAL 3 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. Concurrently, FTC and State Attorney General have investigated numerous companies' security practices in response to concerns with vulnerability, or following a breach of security. Collectively, these laws, regulations, and decisions create standards, which 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

9:00-12:00 TUTORIAL 4 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; Richard M. Smith; Ross Stapleton-Gray

CONSTITUTIONAL LAW IN CYBERSPACE

1:30-4:30 TUTORIAL 5 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. Godwin has done evolving versions of this tutorial at 11 different CFP conferences (sometimes for CLE credit and sometimes not), and the tutorial has continued to be well-subscribed and highly rated.

TELECOMMUNICATIONS LAW FOR THE REST OF US

1:30-4:30 TUTORIAL 6 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; and 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 radio & networks, including spread-spectrum and smart-radio technology, and voice over IP. Panelists: Lee Tien, EFF; Christopher Savage, Cole, Rayvid & Braverman; Robert Cannon, Federal Communications Commission

PRIVACY NOTICES: READABILITY VS. COMPLETENESS

1:30-4:30 TUTORIAL 7 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 as well. Panelists: Martin Abrams, Center for Information Policy Leadership; Ari Schwartz, Center for Democracy and Technology; Peggy Eisenhauer, Huntz & Williams; Susan Henrichsen, California Dept. of Justice (invited); Beth Givens, Privacy Rights Clearinghouse (invited); Joanne McNabb, California Office of Privacy Protection (invited)

WELCOME RECEPTION

6:00-8:00

APRIL 21 WEDNESDAY

7:30-8:45	CONTINENTAL BREAKFAST
8:45-9:45	OPENING KEYNOTE: DAVID DILL
10:15-11:30	PLENARIES: 'Overseeing' the Poor Tapping the Net Revisited
11:30-12:15	LUNCH
1:15-2:15	CONCURRENT SESSIONS: RFID and Privacy Technology Transfer, Technology Dumping Gatekeepers of the Web? Nations vs. the Net
2:30-3:45	PLENARIES: Datamining the Unknown Unknowns Organizing Online for Political Change Screening: Information Futures
3:45-5:00	7:00-9:30 BOF BROTHER AWARDS (AT CLAREMONT)
9:30-12:00	BOF SESSIONS

OPENING KEYNOTE (DAVID DILL)

8:45-9:45

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

10:15-11:30 PLENARY 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

TAPPING THE NET REVISITED: VOICE OVER IP AND LAW ENFORCEMENT

11:30-12:45 PLENARY The FBI is back, insisting that VoIP be subject to the same wiretap-friendly design mandates that apply to the PSTN under the controversial CALEA legislation. The FCC has announced its intent to undertake a 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? Leading participants in the debate from law enforcement, civil liberties and industry explore these and related issues. Moderator: John Morris, Center for Democracy and Technology; Panelists: Jeff Pulver, pulver.com; Lee Tien, EFF; Steve Bellwin, AT&T Lab-Research

RFID AND PRIVACY

1:15-2:15 CONCURRENT 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; Richard M. Smith; Ross Stapleton-Gray

TECHNOLOGY TRANSFER, TECHNOLOGY DUMPING

1:15-2:15 CONCURRENT 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? Panelist: Xiao Qiang, China Internet Project; Jagdish Parikh, Human Rights Watch

GATEKEEPERS OF THE WEB? THE HIDDEN POWER OF SEARCH ENGINES

1:15-2:15 CONCURRENT 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. Alarmingly, and 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, and render smaller sites nearly invisible. Search engines are famously prone to manipulation. Finally, 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. Panelists: Marcel Machill, Univ. of Leipzig and the Bertelsmann Foundation; Matthew Hindman, Fellow, Harvard's Kennedy School of Government; Benjamin Edelman, search engine censorship expert; Moderator: Kenneth Neil Cukier, Fellow, Harvard's Kennedy School of Government

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

1:15-2:15 CONCURRENT 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 devil's) lie? In Dec. 2003 more than 100 delegates from governments, industry and activist groups convened in Geneva for the first round of the UN World Summit on the Information Society. 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 Disruption; 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?

2:30-3:45 PLENARY 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. Panelists: Jeff Jonas, SRD; Lara Flint, Center for Democracy and Technology; Peter Swire, former chief counsel for privacy in Clinton Administration; Stewart Baker, former counsel at National Security Administration

ORGANIZING ONLINE FOR POLITICAL CHANGE

3:45-5:00 PLENARY 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'll 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. Panelists: Jonah Seiger, GWU; Bill Pease, Get Active; Wes Boyd, MoveOn.org; Tom Mattize, AFL-CIO; Don Means, Meatup.com

INFORMATION FUTURES

5:30-7:00 SCREENING Presenters: Rick Prölinger, Ross Stapleton-Gray

BIG BROTHER 30TH ANNIVERSARY (CLAREMONT)

7:00-9:30

BOF SESSIONS

9:30-12:00 NOTE: BOF SESSIONS ARE SUBJECT TO CHANGE

BRAINSTORMING PRIVACY SURVEYS

Presenter: Andrew Brandt

NEW CFP ATTENDEE'S TOWNHALL

Organizer: Freder Springstiel, Writer and former CS Professor

CREATIVE COMMONS LICENSE USERS' MEETING

Organizer: Herko Hietan

JAPANS NEW PRIVACY PROTECTION RULES

Presenter: Lawrence Repeta

COMPUTERS, FREEDOM AND MOORE'S LAW

Presenter: Drew Clark, National Journal's Technology Daily

THE FUTURE OF THE PATRIOT ACT

Presenter: Andrew Grosso

MOBILOPHOBIA

Presenter: Drew Hennment

APRIL 22 THURSDAY

7:30-8:45	CONTINENTAL BREAKFAST
9:00-10:15	PLENARIES: Trusted Computing Open Source, Open Society
10:15-11:30	CONCURRENTS: Data Retention And Privacy Wardriving, Wireless Networks & The Law Suing Filesharers: Privacy and Liberty Fahrenheit 451.3 The Next Drug War
1:15-2:30	PLENARIES: The Net: Caught in the FCC's Web? Facing the Music The Council of Europe Cybercrime Treaty
2:30-4:00	
4:15-5:30	
7:00-10:00	EFF PIONEER AWARDS (AT CHABOT)
10:00-12:00	BOF SESSIONS

TRUSTED COMPUTING

9:00-10:15 PLENARY 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. Panelists: Seth Shelton, EFF; David Safford, IBM; Geoffrey Strongen, AMD; Danny Weitzen, W3C and Computer Science & Artificial Intelligence Laboratory, MIT; Brian LaMacchia, Microsoft

OPEN SOURCE, OPEN SOCIETY

10:15-11:30 PLENARY 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; Bruce Perens, Perens LLC; Jason Matusow, Microsoft

DATA RETENTION AND PRIVACY: A REAL WORLD APPROACH TO EU/JUS REGULATIONS

12:00-1:00 CONCURRENT 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 analyze 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; Stephen A. Firth

WARDRIVING, WIRELESS NETWORKS & THE LAW

12:00-1:00 CONCURRENT Wireless networks are exploding in popularity, but are difficult to secure. Locating insecure networks & advertising their location 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

SUING FILE SHARERS: PRIVACY & LIBERTY IMPLICATIONS

12:00-1:00 CONCURRENT 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 for 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? This panel will involve a vigorous and wide-ranging debate among advocates of each of these positions, with a focus on the privacy and liberty implications of the recent spate of lawsuits. Moderator: Mark Lemley, UC Berkeley and Keker & Van Nest. Panelists: Stacey Dogan, Northwestern University; Jon Healy, LA Times; Wendy Seltzer, EFF; Ian Clarke, Freenet

FAHRENHEIT 451.3: USING ISPS TO CONTROL CONTENT ON THE INTERNET

12:00-1:00 CONCURRENT 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 Schulz, University of Hamburg; Bruce Taylor, National Law Center for Children and Families

THE NEXT DRUG WAR: POSSESSION STATUTES TARGET TECHNOLOGY

12:00-1:00 CONCURRENT 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? "mere possession"? Panelists: Fred Von Lohmann, EFF; Jason Schultz, EFF; Jennifer Granick, Stanford Center for Internet and Society; Van Stevenson, Motion Picture Association of America

THE NET: CAUGHT IN THE FCC'S WEB?

1:15-2:30 PLENARY 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, Rayvid & Braverman; Robert Cannon, Senior Counsel for Internet Issues (Federal Communication Commission's Office of Plans and Policy)

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

2:30-4:00 PLENARY 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, EMU; Sarah Deutsch, Verizon; Eric Garland, BigChampaign; Daniel Gervais, Univ. of Ottawa Faculty of Law; Neil Netanel, UT School of Law; Fred von Lohmann, EFF

THE COUNCIL OF EUROPE CYBERCRIME TREATY: IT MAY CHANGE THE NET FOREVER

4:15-5:30 PLENARY The Council of Europe Cybercrime Treaty is an international agreement 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 surveil 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 Hosen, LSE/Privacy International. Panelists: Barry Steinhardt, American Civil Liberties Union; Betty Shane, Computer Crimes and Intellectual Property Section of the US Justice Department; Tracy Cohen, London School of Economics & Consultant to the South African Broadcasting Authority.

BOF SESSIONS

9:30-12:00 NOTE: BOF SESSIONS ARE SUBJECT TO CHANGE

SCREENING: HACKAVISTA DOCUMENTARY

Presenter: Robert Guerra

PROGRAM FOR ONLINE DELIBERATION

Presenter: Todd Davies

DIGITAL COPYRIGHT IN EUROPE/ASIA VS. US

Panelists: Yuko Noguchi, Stanford Law School; Andrea Ottilia, Game Room; Presenter: Qiong Wu, UC Berkeley.

THE PATRIOT ACT (THE GAME)

Game Room; Presenters: TBA

KIDS AND TEENS: E-PRIVACY AT STAKE

Presenter: Michel Walrave, University of Antwerp (Belgium)

HOW TO FIGHT THE PATRIOT ACT IN THE COURTS

Presenter: Kevin Bankston, EFF

DESIGNING PRIVACY

Presenter: Barbara Lawler, Hewlett Packard

APRIL 23 FRIDAY

7:30-8:45	CONTINENTAL BREAKFAST
9:00-10:30	PLENARIES Policy Laundering Government Profiling & Private Data
10:30-11:45	KEYNOTE (TBA) & LUNCH
12:00-1:30	CONCURRENT SESSIONS: Identity Theft Cease and Desist Next Generation Democracy Security and Privacy for the EU Citizen The Law and Ethics of Online Research
PLENARY: Electronic Voting	
3:15-4:45	
4:45-5:30	CLOSING KEYNOTE: BREWSTER KAHLE

POLICY LAUNDERING

9:00-10:30 PLENARY 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 of the most 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. Panelists: Gus Hosen, Privacy.org; Ken Anderson, Assistant Commissioner for Privacy, Ontario, Canada; Tom Kallit, UC Berkeley

GOVERNMENT PROFILING AND PRIVATE DATA

10:30-11:45 PLENARY 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. At the same time, 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 use of private sector databases, the privacy and security concerns posed by government use of such databases for terrorism purposes, and the possible benefits of government use of such databases. Moderator: Nick Gillespie, Reason Magazine; Panelists: Danny De Temmerman; Jennifer Barrett, Chief Privacy Officer, Accion; Nualla Kelly, Representative from Privacy Office, Homeland Security Dept.; Bill Skidell, BoycottDelta.org; Jim Harper, Privacilla

KEYNOTE (TBA) & LUNCH

12:00-1:30

ID THEFT: ADDRESSING THE PROBLEM GLOBALLY

1:45-2:45 CONCURRENT Identity theft often reaches beyond the borders of a single state or country. Recently, for instance, credit card information of US citizens was used to manufacture false cards in Romania, and then the cards were used in the EU. To efficiently combat cyber-crime and ID theft, countries must cooperate to create a system of protection & enforcement that goes beyond each country's borders. This session will provide actual examples of national and global identity theft schemes; analyze existing and pending cyber security laws, protections, and initiatives in different countries that address directly or indirectly identity theft; review existing global cybercrime treaties and initiatives, and suggest potential coordinated actions nationally and globally. Moderator: Françoise Gilbert; Panelists: Jody Westby, The Work-IT Group; Jacques Gilbert, First Data Corp.; Joanne McNabb, Chief Privacy Officer, State of California

CEASE & DESIST: 2 YEARS OF FIGHTING ONLINE CHILL

1:45-2:45 CONCURRENT 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 cataloging these letters for the past two years and, where appropriate, fighting online chill. Panelists from the project will give a weather map from data we've gathered, assessing the climate for online activity. What activities risk being frozen out? What can we do to warm the air? Moderator: Wendy Seltzer, EFF; Panelists: Jennifer Urban, Boalt Hall, School of Law; Diane Cabell, Berkman Center for Internet and Society, Harvard Law School; Rita Heimes, University of Maine School of Law

NEXT GENERATION DEMOCRACY: INTERNET, YOUNG VOTERS AND THE 2004 ELECTION

1:45-2:45 CONCURRENT The 18-24 year-old age group exhibits a vigorous attachment to online community, with 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 Anderson, Youth '04; Panelists: Vince Keenan, Publius.org; Tom Bryer, Party Y; David Smith, Mobilizing America's Youth

SECURITY AND PRIVACY FOR EU CITIZENS IN A POST 9/11 AGE: A EUROPEAN PERSPECTIVE

1:45-2:45 CONCURRENT 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: Laurent Beslay. Panelists: M. Calvoman; Paul de Hert; Marie-Helene Boulanger, "Integration of Data Protection Concerns in Justice and Home Affairs Large Scale IT Systems".

THE LAW AND ETHICS OF ONLINE RESEARCH

1:45-2:45 CONCURRENT 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

E-VOTING: THE GREAT PAPER TRAIL DEBATE

3:15-4:45 PLENARY If your next vote is cast on a touch screen voting machine, how will you know 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 our 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 improving the integrity of elections. Moderator: Lorrie Cranor. Panelists: David Wagner, UC Berkeley; Warren Slocum, San Mateo Registrar; Kim Alexander, California Voter Foundation; Mike Shamos, CMU; Brad Clark, Alameda Registrar; Barry Steinhardt, ACLU.

CLOSING KEYNOTE: BREWSTER KAHLE

4:45-5:30

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
John F. Kennedy 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, The Open Society Institute,
Public Interest Registry, Sun, Yahoo!,

PATRONS & SPONSORS:



DEADLINES

Early fees deadline: March 31, 2004
Last day to register online: April 7, 2004

CANCELLATIONS

Cancellation requests received in writing and postmarked by
April 7, 2004 will be honored. A cancellation fee of \$35 US will
apply. Please allow 2-4 weeks for processing after the conference.

REGISTRATION INQUIRIES

Please e-mail: MANDY@REGMASTER.COM

GENERAL INFORMATION

Please visit: HTTP://WWW.CFP2004.ORG

VENUE AND LODGING

CFP 2004 will be held at the CLAREMONT RESORT & SPA IN BERKE-
LEY, CA. A special rate of \$139 US is available for CFP attendees.

Please call 1.800.551.7266 to make your reservation or visit
HTTP://WWW.CFP2004.ORG for online reservation information.

For more information about the Claremont visit:
HTTP://WWW.CLAREMONTRESORT.COM

STUDENTS ONLY: To be eligible for the student rate,
you must be a full-time student in an undergraduate,
graduate, or professional degree program. A valid student
ID or other proof of student status will be required at time of
registration and check-in. Students who wish to guarantee
a space in tutorials must pre-register and pay the regular
tutorial fee.

PAYMENT

Payment must accompany registration form in order to be
processed. Purchase orders, telephone orders, and wire
transfers are not accepted.

YOU MAY REGISTER BY MAIL (INCLUDE PAYMENT)
CFP 2004, c/o Registration Systems Lab, 779 East Chapman
Road, Oviedo, FL 32765, USA

FAX 1.407.366.4138

ONLINE <http://www.regmaster.com/cfp2004.html>

MEMBERS OF THE PRESS are invited to cover CFP2004 at
no charge, except for meals. Full Conference fee includes
3 lunches, breakfasts, and breaks. 1 day Conference fee
includes lunch, breakfast and breaks for that day.

PAYMENT must accompany registration form in order
to be processed. Purchase orders, telephone orders, and
wire transfers are not accepted. Please make checks pay-
able in **US\$** to **ACM/CFP2004**. Your credit card transaction will
be charged on your statement as from **ACM/CONFERENCE BY RSL**.
Your signature indicates your agreement to pay the fees
with the credit card number provided.

DESIGN: M-A-D / madxs.com

REGISTER

FIRST NAME LAST NAME
TITLE AFFILIATION
ADDRESS
CITY STATE/PROVINCE
ZIP/POSTAL CODE COUNTRY
PHONE FAX
EMAIL

OTHER INFORMATION (check which apply)

ACM MEMBER NO. (required for member rates)
I AM A MEMBER OF THE PRESS AND AM ENCLOSING MEDIA CREDENTIALS
I AM REQUESTING VEGETARIAN MEALS
SPECIAL NEEDS (please specify)

TUTORIAL SELECTIONS (circle which apply)

MORNING T1 T2 T3 T4
AFTERNOON T5 T6 T7
OR WORKSHOP

ON/BEFORE MAR 31: FEES IN US DOLLARS (circle which apply)

CONFERENCE STUDENT 75 ACM MEMBER 535 NON-MEMBER 585 PRESS* 0
EA. TUTORIAL STUDENT 25 ACM MEMBER 75 NON-MEMBER 100 PRESS* 75
WORKSHOP STUDENT 25 ACM MEMBER 125 NON-MEMBER 150 PRESS* 125
SUBTOTAL

AFTER MAR 31: FEES IN US DOLLARS (circle which apply, enter quantities where applicable)

CONFERENCE STUDENT 100 ACM MEMBER 650 NON-MEMBER 690 PRESS* 0
WORKSHOP STUDENT 50 x ACM MEMBER 175 x NON-MEMBER 200 x PRESS* 175 x
EA. TUTORIAL STUDENT 50 ACM MEMBER 105 NON-MEMBER 130 PRESS* 105
SUBTOTAL

SPECIAL 1 DAY RATE (circle which apply)

1 DAY RATE STUDENT 40 ACM MEMBER 125 NON-MEMBER 125 PRESS* 0
CHOOSE ONE DAY WEDNESDAY THURSDAY FRIDAY
SUBTOTAL

***DAILY MEAL TICKETS FOR PRESS**

CHOOSE DAYS WEDNESDAY 35 THURSDAY 35 FRIDAY 35
SUBTOTAL

TOTAL FEES

PAYMENT INFORMATION

CARD NO. EXPIRATION DATE
CARD ID CODE (AmericanExpress: 4-digits above card No. on front. Visa/MasterCard: last 3-digits on back.)
NAME SIGNATURE
ADDRESS (if different from above)