CFP

Thursday

April 18, 2002

Today at a Glance

- How to Hack an Election @8:45
- Privacy in Identity and Location Services @10:00
- Sessions @11:30
  - Open Source
  - Global Internet
  - ICANN
  - Medical Info
  - Digital Divide
- Lunch with Larry Irving
- Global Grassroots @2:15
- DMCA and You @3:45
- Future of I/P @5:30
- BOFs @9:30

Seeking International Perspectives at CFP

By Mary Rundle

A limitation of CFP has often been its focus on debates and developments in the US (and to a lesser degree, Canada and Europe). But activists around the world are confronting different issues in their efforts to promote development of an open, affordable, and user-controlled Internet. In planning for CFP 2002, the Program Committee sought to include a full range of perspectives on Internet policy activism – including international perspectives on privacy, democracy, security and barriers to access.

Traditionally, one problem with having international perspectives at CFP has been financial: simply put, many non-governmental organizations (NGOs) abroad can't afford to send participants.

The Open Society Institute's generous support has added to the diversity of CFP2002.

The Open Society Institute (OSI), which had brought in some NGOs to CFP 1999 to much success, took up the challenge again this year. OSI's Jonathan Peizer led the charge, securing OSI funds to sponsor four experts from developing countries: Judit Bayer of Hungary, Rishi Chawla of India, Veni Markovsk of Bulgaria, and Mas Wigrantoro Roes Setiyadi of Indonesia. (Two other invited activists could not get visas, due to delays related to September 11-inspired changes in US Embassy procedures.)

OSI's generous support has added to the diversity of CFP 2002, with this year's Conference enjoying 90 international participants from 30 countries – including, among others, nine people from Great Britain, seven from Ghana, seven from Nigeria, and two from Nepal.

If you are an American, look out for these people and make them feel welcome, and be sure to benefit from their international perspectives. If you are one of these international participants, the rest of us want to thank you for being here – let us know if we can help you in any way. We look forward to an excellent exchange of views.

For an inside look at policy challenges for activists from around the globe, check out Concurrent Session #2: "Getting It Right – Global Internet Policy Issues" Thursday, April 18, 2002, 11:30am-12:45pm, with James Dempsey of CDT as Moderator and Rishi Chawla, Mas Wigrantoro, and Veni Markovski as panelists.

New Report Shines Light on States' Surveillance Procedures

By Laurel Jamtgaard

The Liberty and Security Initiative of the Constitution Project based at Georgetown University released a survey of state wiretap laws Wednesday at the CFP conference.

Peter Swire, a law professor at Moritz College of Law at Ohio State University and former Privacy Czar in the Clinton Administration, presented the survey to the CFP general session. More than half of the wiretap requests made in the U.S. are made by state law enforcement agencies under state laws, but, according to the report, the state-level laws are under less scrutiny than the laws at the federal level. Swire pointed out that this is the first comprehensive review of state wiretap approval procedures and their impact on individual liberties.

Discussing the importance of this review, Professor Swire noted "States don't have the same level of public scrutiny, press attention or institutional safeguards as the Federal government."

Since September 11, several states have initiated new legislation to give state law enforcement increased ability to tap criminal suspects' telephone or electronic communications, subpoena telephone or computer records, and conduct "roving" statewide wiretaps. In a press release issued by the Constitution Project, Joseph Onek, Director of the Liberty and Security Initiative, explains "For example, one state is proposing to eliminate the requirement that a wiretap application list the specified crime for which surveillance is sought. This reduces the oversight capability of the courts."

For more information about the study and to request a copy of the complete survey see, www.constitutionproject.org.

What's Inside

"Fair Use by Design?" Workshop Tries to Focus a Broad Debate

by Aaron Burnstein

This day-long workshop brought together lawyers, computer scientists, and technologists to examine whether digital rights management (DRM) software can manage access to digital works in a manner that preserves the expectations of fair use that have developed around physical works. Articulating some of these expectations was the first challenge of the day. Participants' notions of fair use went far beyond the concept codified in copyright law (17 U.S.C. section 107) to include such values as freedom of expression and promoting creation, innovation and competition.

Participants also identified privacy and user control of a copyrighted work, both in terms of its use and subsequent sale, as constituting part of "real space" fair use norms. Borrowing, lending, annotating, randomly accessing, and referring to works are other fair use expectations that participants wanted to see preserved by (or in spite of) DRM systems.

Fair use is not only complex but also ambiguous, as its definition has changed in the face of new technologies. However, according to Fred von Lohmann of EFF, this ambiguity can be viewed as "a feature, not a bug." Determining who will resolve some of this ambiguity was hotly debated, and participants reported on the efforts of courts, legislatures, copyright owners and legal scholars in this area.

Legislative approaches might be especially complicated. Since the Web trivializes the international distribution of digital works, legislatures of different countries need to "harmonize" their copyright laws or bring them into line with treaty requirements, as Séverine Dusollier of the University of Namur reported.

Copyright owners and technology companies are taking a different approach. The replacement of copyright law with DRM systems and end-user license agreements is

Fair use is not only complex but also ambiguous…

one extreme on the spectrum of choices available to copyright owners. Although this approach might create a market for license terms that does not exist today, several participants expressed concern about reducing the role of the public to one of "voting with its feet," rather than direct participation in shaping law.

Accommodating fair use with revisions in law has its own perils, though, as the enumeration of some fair use desiderata in a law might lead to the exclusion of all others. Standards bodies such as the World Wide Web Consortium (W3C) might have a role to play in the creation and standardization of DRM languages. Thus far, however, the W3C has chosen to focus its efforts on more general metadata technologies, leaving their application to DRM to private and academic development efforts.

Many of these efforts involve some tracking of the use of digital works, raising concerns for the privacy of users. Participants emphasized that it is the attempt to mimic the nuances of fair use that creates the need to track use, but not all copyright holders want the full protection of copyright law. As Molly

(continued on page 8)

Dining with Bill Lockyer

By Sky Canaves

At Wednesday's keynote dinner address, California Attorney General Bill Lockyer confided, "I always thought I would be an astrophysicist, but I strayed." That hasn't stopped him from coming up with his own list or the top ten new elements for the periodic table, including such gems as "Enronite: reputed to have active electrons, now only attracts subpoenatrons," and "Dickchenium: element stored in an undisclosed location, mainly to attract fundraisium from petroleum."

Managing 1069 attorneys in his department, Lockyer is very involved with privacy issues. His office also manages the CLET (California Law Enforcement Technology) system for law enforcement. Forensic labs have been collecting DNA samples from convicted felons for more than a decade; Lockyer's office has now processed these so that they have 210,000 DNA samples in the computer system. The department has had software written which allows photos to be downloaded to squad cars, and virtual lineups can be conducted on street corners rather than by taking people up to the police station.

Lockyer has also promoted efforts to halt the spread of identity theft. His office pushed through a law that requires businesses to make reasonable efforts to destroy documents that contain personal information, and formerly reluctant police departments are now required to take reports in cases of identity theft. In terms of protecting individual privacy, Lockyer supports easily comprehensible notice requirements governing the disclosure of personal information, and he advocates simple methods for consumers to protect their individual privacy, such as postcards that allow consumers to opt out of personal information disclosure. However, in California the debate over the protection of consumer data has "been debated to a standstill."

In his conclusion Lockyer urges us to follow up on two things: First, polls show that people care about personal privacy. We should all be strongly supportive of those in the public eye who are willing to take political risks to preserve privacy. Second, Lockyer, distressed by the low voter turnout in the recent California primaries, urged us to remember that "Democracy is the most extraordinary experiment in human history. Everyone has a voice and everyone counts." Lockyer believes that the many smart people at CFP should be able to figure out solutions to the problems of declining political participation. Send your ideas to billlockyer@aol.com.

Shaffer Van Houweling, a

From the National Journal Tech Daily:

Privacy Report: Call For ID Cards Poses Array Of Questions

by Drew Clark

SAN FRANCISCO -- Proposals for a national identity card pose a dizzying array of questions that must be addressed before acceptance and implementation, according to a report presented Wednesday at the Computers, Freedom and Privacy conference here.

Prepared by an array of technologists and technology policy officials, the National Academies of Sciences (NAS) report from last week argued that the goals of a nationwide identity system must be clearly stated and that a compelling case be made before any such proposal could move forward.

"The nationwide ID system debate has been hampered by the lack of a clear description of the goals of such a system," said Deirdre Mulligan, a University of California at Berkeley law school professor and member of the NAS' Committee on Authentication Technologies and their Privacy Implications.

"There are many complicated policy and technological issues around such system" ranging from its purpose, how IDs would be issued, whether participation would be voluntary, what data would be collected, who would control and have access to the data, and what legal structures would be necessary to accommodate such a system, she said.

Jay Maxwell, president of the information technology subsidiary of the American Association of Motor Vehicle Administrators (AAMVA), also addressed the debate over ID cards. In January, his group proposed that Congress require states to include biometric identifiers like fingerprints on drivers' licenses.

> *"The homeland security budget is pork for the IT industry"*
> *- Andrew Schulman.*

Maxwell took issue with the characterization of AAMVA's proposal -- which has been harshly criticized by privacy advocates -- as a national ID card. But he conceded that the proposal, which also includes linking state motor-vehicle database to include all drivers, amounts to a national identification system under the NAS report, which he praised.

He said, however, that providing more secure driver's licenses would address a host of problems, ranging from driving violations to underage smoking and drinking to combating terrorism. He said that "states are spending a lot of money" to make licenses more secure as part of "a knee-jerk reaction to do something" about terrorism.

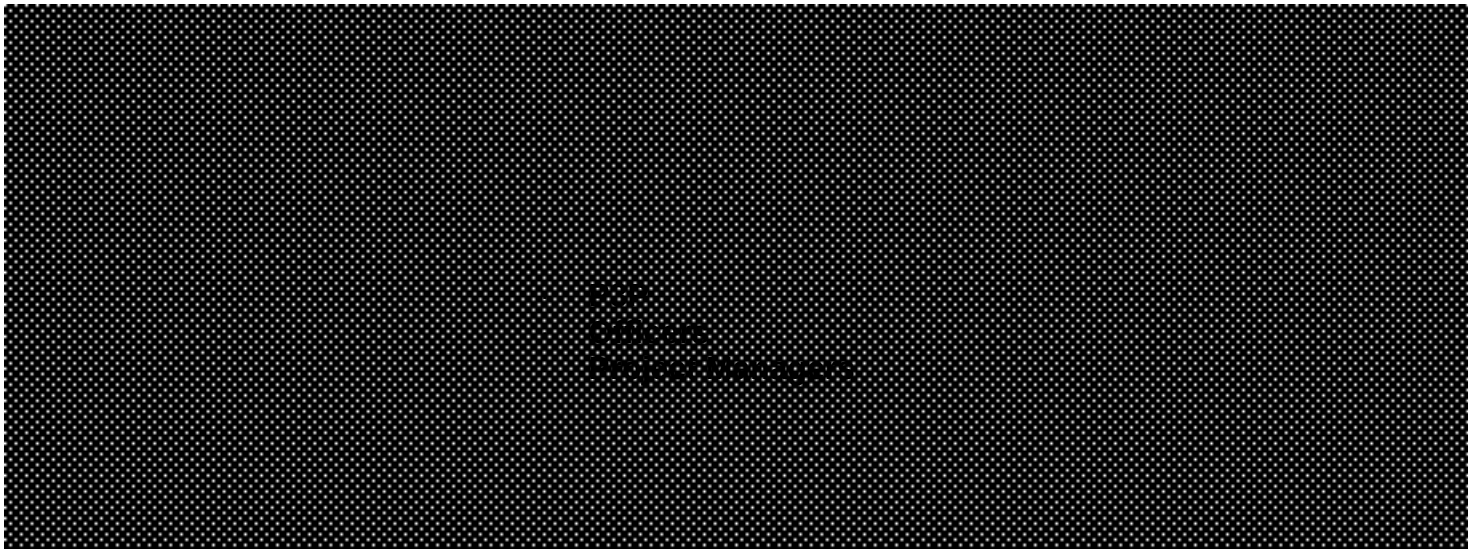
"If there is interoperability, they are going to spend a lot of money, but they are not going to solve anything," Maxwell said.

Andrew Schulman of the Privacy Foundation countered that existing government ID systems fail to serve their ostensible purposes. He pointed to failures in the border-crossing cards issued by the Immigration and Naturalization Service, such as the issuance of machine-readable ID cards with no computerized readers to do so.

"One of the problems in the debate is that a lot of the practicalities are run by the vendors, and privacy advocates have ceded the practicality arguments" to technology companies pushing their own products, Schulman said. "The homeland security budget is pork for the IT industry and I think that is a real problem."

Peter Swire, former President Clinton's privacy counselor and now a George Washington University law professor, moderated the debate. He unveiled details of a report, issued Tuesday by the Constitution Project of the Georgetown University's Public Policy Institute, that analyzes an array of proposed changes to state wiretapping laws since Sept. 11.

National Journal's Technology Daily is a twice-daily online publication exclusively focused on technology politics and policy. For more information, please visit http://www.technologydaily.com or e-mail techdaily@nationaljournal.com.



Thursday's BOF Sessions
Take Back the Night

BOF's meet at 9:30pm

Teaching about Computers, Freedom and Privacy in the College Classroom
(Location: Telegraph A)
Courses focused on the topics of computers, freedom and privacy are emerging across college campuses. Students are eager to learn more about these issues and they are particularly important for professors whose research includes the study of technology and society. This session offers an opportunity for those who are interested in teaching about these issues to come together, share experiences, exchange strategies and network resources.
Leaders: Fred Solop and Phoebe Morgan, Northern Arizona University

---

Database Stockpiling and Temptations to Use Data
(Location: Telegraph B)
Databases and You: You are in the National Directory of New Hires, therefore you exist. We'll talk about databases, their many uses and abuses, and privacy and security issues they pose. Bring your own database stories and questions.
Leader: Linda Ackerman, PrivacyActivism.org

Privacy at Stanford: A Study on Current Attitudes
(Location: Marina/Sea Cliffs)
Leader: Ruchika Agrawal, Stanford University

Gripe Sites and the Law
(Location: Cathedral A)
Designing gripe sites with litigation in mind: How can a consumer or employee or other person, who wants to mount an anti-corporate web site, obtain the best public exposure and maximize effective expression of their point of view while minimizing legal exposure under trademark, copyright, defamation, and other theories? Because defending a lawsuit can be expensive and time-consuming (not to speak of terrifying for most people), it is worth considering defenses before suit is threatened or filed. Options for financing a legal defense, or finding free counsel, will also be discussed. Hopefully, discussion will compare and evaluate alternate strategies in defending such cases.

Speakers:
Paul Alan Levy, Attorney, Public Citizen Litigation Group, has defended many such cases, as well as advising other lawyers and web masters about how to design their web sites to minimize chances of being sued without unduly interfering with effective communication of the message, or how to modify their sites after they have been threatened with litigation. He will offer a written outline of issues that arise and points to raise in litigation and elsewhere, as well as listing resources for conducting a defense.

Hank Mishkoff, the defendant in Taubman v. Mishkoff (Taubmansucks.com) will discuss his experiences defending himself pro se, and what he might do differently with the benefit of hindsight."

Leader: Paul Levy, Public Citizen

Planning CFP2003
(Location: Presidio)
Leader: Barry Steinhardt, ACLU, Chair of CFP2003

P3P First Generation in Retrospect
(Location: Cathedral B)
The Platform for Privacy Preferences Project (P3P) is now an official W3C recommendation. 2 years have passed since consumer privacy on the Internet became a critical issue and P3P itself emerged as one approach to address the problem. Widespread P3P adoption is a relatively new phenomenon but the standard has already made an impact on websites. It may be too early to draw conclusions about long-term effects. Nevertheless this is a good time to reflect on the progress made towards the stated objectives of P3P.

This BOF session will serve as a post-mortem on everything from the specification's five-year evolution to 1st-generation implementations such as the AT&T Privacy Bird and MSFT Internet Explorer. It will also function as a feedback forum for implementors. This is a good opportunity to raise concerns, ask questions and provide critiques. Join the discussion and help shape the direction of future P3P development.
Leader: Cem Paya, Microsoft

The International Digital Divide
(Location: Pacific Heights)
Leader: Ethan Zuckerman, Geekcorps

Wednesday's BOF Sessions (continued)

BOF's meet at 9:30pm

How a Coder Cornered Milosevic
(Location: El Dorado)
Patrick Ball will talk about his testimony in the trial of Slobodan Milosevic at the International Criminal Tribunal for Former Yugoslavia in The Hague. He will have already given a plenary talk on the formal side, so in the BoF he hopes to talk less formally.

The group will view video clips from Mr. Ball's streaming video site (hague.bard.edu), and will discuss the use of open source software (linux, apache, python) in the project. Patrick will tell a few anecdotes from the data preparation and trial process. It should be fun, not another formal session.
Leader: Patrick Ball, AAAS

FTC Chairman Addresses CFP: Defends Record on

by Will DeVries

Federal Trade Commission chairman Timothy Muris urged consumers, privacy advocates, private companies and governments to support increased protection of private digital information. Outlining the steps already taken in his term and the FTC's future plans, Chairman Muris called on consumers to use common-sense protections and change their approach to their use of digital media to protect their privacy.

Appointed by President Bush in 2001, Chairman Muris has tackled many of the most common complaints regarding digital privacy. Under his leadership, the FTC has sought to limit intrusions by telemarketers and spammers, to protect private financial information online, to combat identity theft, and to ensure that private companies comply with their published privacy policies. In addition, the Commission intends to keep privacy protection is required as technology develops.

Under Murris' leadership, the FTC has sought to limit intrusions by telemarketers and spammers, to protect private financial information online, to combat identity theft, and to ensure that private companies comply with their published privacy policies.

The Chairman also noted the key role of consumers in the fight for privacy protection. Thanks to consumer demands, he noted, websites today are far less likely to ask for private information and allow "cookies" than they were a few years ago. Consumers need to treat their computers and other digital tools as they do their homes or cars – by locking them up tight when not in use and investing in preventative security measures. Chairman Muris pledged that the FTC will work with consumers to instill a culture of security.

Intellectual Property Panelists Ponder Middle Ground on Anti-Piracy Technology

by Drew Clark of the National Journal Tech Daily

SAN FRANCISCO -- Digital-rights management technology cannot simultaneously meet the desires of both copyright holders and consumers who desire to make "fair use" of copyrighted material, a panel of technologists, lawyers and business officials here agreed during a session Tuesday evening.

The panelists, speaking during a day-long and wide-ranging workshop at the annual Computers, Freedom, and Privacy conference, were debating issues surrounding the technical feasibility of changing digital-rights management (DRM) systems in order to accommodate consumers' fair use to digital material that is subject to copyright protection.

Such systems increasingly are being deployed or considered for use by large media and software companies that want to avoid the fate that has befallen the music industry: large catalogs of copyrighted songs being traded by fans on the Internet.

Critics decry the restriction that DRM technologies place on consumers' ability to play legitimately acquired content on a variety of digital players. These critics and others also avidly oppose legislation by Senate Commerce Committee Chairman Ernest (Fritz) Hollings, D-S.C., to go one step further and mandate the use of DRM systems.

But panelists at the workshop disagreed among themselves about whether consumer desires expressed through the marketplace are sufficient to temper DRM systems enough to permit at least a limited form of copying for non-commercial uses.

"There are some among us who believe that there is a market failure because of the hegemonic control of the copyright industry and that consumers' desires are not thought of at all," Jennifer Granick, director of a clinical program at Stanford University's Center for Internet and Society and the moderator for the workshop's final session, said in attempting to summarize the proceedings. "There are some among us who believe that consumers have the ability to affect the market, and that DRM is good" because it can protect new business models -- like pay-per-read books -- that could stimulate the creation of more copyrighted works.

"There is a funny alliance between critics who don't want us to use DRM" because it could potentially undermine fair use and "the content people who don't use it because we want to sell our plastic CDs" and not undermine fair use and copyright holders, said Tomas Sander, a member of the research team at InterTrust Strategic Technologies and Architectural Research (STAR) Laboratory, a key DRM provider.

But several copyright lawyers, including American University law professor Peter Jaczi and Fred von Lohmann, a senior intellectual property attorney at the Electronic Frontier Foundation, said they worry that DRM technologies will erode or even eliminate fair-use doctrine. They also worry that the quest to define the elements of fair use could lead to its loss.

"The approach should not be, 'Tell me what fair use requires, and I'll build it in,' but rather, 'How can I build something that permits a variety of as-yet unknown uses, so that courts can decide whether those future uses are fair,'" von Lohmann said. "The ambiguity of the fair-use doctrine is not a bug but a crucial feature."

Access to Information Since 9/11 Heightened Sensitivity

by Will DeVries

In the wake of the events of 9/11/01, how should governments and private entities treat information that could impact national security? The panel moderated by Kevin Poulsen of SecurityFocus presented conflicting opinions on the direction and goals of information management in this new era of heightened sensitivity and desire for protection.

Chris Hoofnagle, of EPIC, and Lee Tien, of EFF, outlined the current state of information availability with respect to Freedom of Information Act (FOIA) requests. Since the beginning of the Bush Administration, but especially since 9/11, they argued, the federal government has systematically slowed or impeded the flow of information. Using the drumbeat of homeland security as an excuse, the Administration has widened the scope of FOIA exceptions and attempted to evade the law.

VeriSign's Michael Aisenberg disagreed with the view that all post 9/11 developments have been negative. Industry groups are seeking improvements in federal legislation concerning industry exchange of cyber-security information, and the need for such sharing has neve been greater. Pendin congressional legislation known as the Davis-Mora bill, would establish framework for the sharing o cyber-security informatio and exempt much of suc information from FOI requests. While the proposa engendered arden disagreement from many i the audience and on th panel, Mr. Aisenber contended that adequat avoidance of cyber threat requires that industr groups be protected fro full disclosure.

The Davis-Moran bill would establish a framework for the sharing of cyber-security information and exempt much of such information from FOIA requests.

PATRIOT and Privacy:
Invoking National Security to Increase Surveillance Powers

By Eddan Katz

The USA Patriot Act was enacted quickly in the wake of the terrorist attacks on Sept. 11, and the majority of the distinguished panelists at the PATRIOT and Privacy session expressed their concern that civil rights have been sacrificed by an unbridled justification of increased security. Jerry Berman, executive director of the Center for Democracy and Technology ("CDT"), argued that the very process under which this law was expedited through Congress did not permit the democratic discourse necessary to consider the implications of legislation making such dramatic changes to civil liberties. Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario, concurred about the lack of legislative debate, noting that similar laws expanding the surveillance powers of the government have been hastily enacted in Canada, 7 European countries, and Australia.

There was "ample debate" during the six week period before the passage of the PATRIOT ***Act.***
Chris Painter- DOJ

Further concerns were raised that the PATRIOT Act and the Congressional attitudes it reflects will give rise to a broad interpretation of terrorist activities to include lawful dissent, collapse the division between foreign intelligence activities and domestic law enforcement, and shield government agencies from accountability for abuses.

Chris Painter, of the Department of Justice, argued that there was "ample debate" during the six week period before the passage of the PATRIOT Act and defended the law from the criticism he called "hyperbole." Far from declaring the death of the Fourth Amendment, Mr. Painter argued that even the controversial provisions of the PATRIOT Act were narrowly drafted and that the balance between privacy and security is maintained in the statute. He went on to characterize the claim that section 216 will allow the government to track the web surfing habits of Internet users as a "red herring," asserting that the FBI's capture of URL information is not about the content of an individual's communications.

Mr. Painter began his talk by indicating that the sunset provisions in section 224 of the Patriot Act will allow Congress and the general public an opportunity to evaluate whether the new surveillance powers are being abused by law enforcement in late 1995, when some provisions will be revisited at the end of four years from the passage of the Patriot Act.

The session included discussion of particular provisions of the law as well as its broader implications for privacy and civil liberties. Clint Smith, of UUNet, presented several ambiguities in the law that complicate the cooperation with law enforcement by Internet Service Providers (ISPs), who control the network junctures where the government places their surveillance technologies. Mr. Smith explained that the technical obligations on ISPs (sec. 222) are unclear, that circumstances regarding emergency disclosures of information are vague, and expressed concern that there is no control over the extent of surveillance once the government installs these technologies.

John Podesta, former White House Chief of Staff under President Clinton, argued that the PATRIOT Act relies excessively on the powers of the executive branch without providing for sufficient judicial review. Mr. Podesta pointed out that the failure of law enforcement agencies to prevent the attack on Sept. 11 was not a result of technical

(Continued on page 8)

Internet Luminaries Anointed by EFF with Pioneer Awards

By Eddan Katz

Nearly 200 people gathered for the Electronic Frontier Foundation's 11th annual Pioneer Awards, entering three new individuals in a select group of the Internet's greatest luminaries. Making light of the overbroad provisions of the Digital Millennium Copyright Act (DMCA), guests were provided plastic decoder rings marked "circumvention device" and business cards accrediting them as "Certified Encryption Researchers." John Perry Barlow, co-founder of the EFF, explained that the Pioneer award honors the defining personalities influencing the developing architecture of cyberspace.

Dan Gillmor, technology columnist from the San Jose Mercury News, received the first Pioneer Award for his dedicated coverage of cutting edge technology issues, particularly misuse of copyright and the DMCA. Gillmor, a columnist for the San Jose Mercury News, said that he was deeply honored to be included on "a list of people who actually do things, rather than just writing about them."

Beth Givens, the founder and director of the Privacy Rights Clearinghouse, a nonprofit advocacy, research, and consumer education program was presented with the second award. She started her program in 1992 before "privacy" was such a hot consumer issue. In her acceptance comments, she explained that she has learned a great deal over the years from listening to ordinary people's stories and has appreciated being able to convey those stories to press, legislators and the public.

Award recipient stays home in Norway for fear of prosecution under the DMCA

Jon Johansen, the Norwegian teenager who helped create the controversial DeCSS decryption program at the center of current DMCA litigation. Johansen, on the advice of his lawyers, did not attend the reception for fear of being prosecuted under the DMCA upon his arrival on American soil. Johansen prepared a video acceptance speech, in which he talked about how reporters have never asked him about his DVD collection. "I now have 140 DVDs," he said. "If the MPAA weren't so stupid to sue their own customers, I would have many more."

CFP Daily2002

CFP Daily2002 is a publication of the CFP2002 Conference with contributions from law students at Boalt and Stanford. In the spirit of free expression, feel free to make copies of this periodical.

The Editors

Preview of Tomorrow at CFP

- **Jackie Speier @8:30**
- **Public Records @9:30**
- **Digital Commons @11:15**
- **Box Lunch Sessions**
- **Anonymity in Cyberspace @2:00**
- **Closing with Bruce Sterling @3:45**

www.cfp2002.com

Corrections….

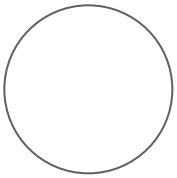
Apologies to John Morris of the Center for Democracy & Technology for calling him "Mark" in the front page article about the important Supreme Court decision yesterday. John came through with a last-minute quote about the decision and we in haste didn't confirm his name. Sorry John!

PATRIOT Act (continued from page 7)

was not a result of technical problems of surveillance, but rather a conceptual problem of focusing on solving criminal cases as opposed to crime prevention.

The efficacy of the PATRIOT Act to combat terrorism through increased surveillance powers remains to be seen in the years ahead. Congress and the general public will have an opportunity to review the legislation in three and a half years. In the meantime, the panelists insisted that there be greater oversight and supervision of law enforcement and intelligence agencies as they implement their surveillance systems.

In response to a question from the audience about the historical abuse of surveillance power by law enforcement, Dr. Cavoukian answered that without the necessary mechanisms for accountability, there would be no way for us to know.



CFP Daily2002 Editorial

Editors-in-Panic
Laurel Jamtgaard
Mary Rundle

Team Leaders
Deirdre Mulligan
Jennifer Granick

Staff Writers
Aaron Burstein
Abigail Phillips
Catherine Jasserand
Shalu Narula
Drew Harris
Eddan Katz
Jennifer Elliot
Jennifer Urban
Laura Quilter
Lisa Wang
Martha Winnacker
Nicky Ozer
Nicole Acton
Osbaldo Cantu
Sky Canaves
Will DeVries