A Chat with Ari Schwartz – CFP Conference Chair Extraordinaire

By Nicky Ozer

CFP Conference Chair, Ari Schwartz, and his dedicated Advisory Board and Program Committee have been working for over two years to plan for CFP's return to the Bay. In a year fraught with attacks on civil liberties, Ari and the CFP Conference are excited to be back in San Francisco and back to the roots of the conference. Ari promises a conference that "looks at the full range of freedom and privacy issues while continuing to address the important issues of the day such as privacy in anti-terrorism initiatives, intellectual property and freedom, and democracy and voting technologies. You will have the chance over the next three days to listen, eat, agree, and argue with a dynamic group of over 500 activists, engineers, law enforcement officials, policy representatives, academics, students, and businesspeople. But if you are here, you already know that CFP is going to be an amazing event.

Ari's Top Picks

Ari warns not to cut out early because missing Bruce Sterling's closing speech would be a HUGE mistake. CFP last heard from Bruce in 1998. Ari says that it was not only one of the most memorable speeches he has ever heard, but that Bruce ended his talk by inviting everyone over to his house for a party. Ari cannot vouch for another invitation, but who could pass up the chance to hear a great speech with the added incentive of a possible opportunity to relive one's younger years with a raucous house party?

Ari also encourages attendees not to miss the debate set up between Steve Metalitz and John Perry Barlow. Should be interesting…

CFP Conference Chair Extraordinaire also anticipates that "How to Hack an Election" should stir up some passions and be an excellent session.

But as a Washington guy, Ari is ever diplomatic, and says so much work has been put into all the sessions, that every single one will be great. Lucky for you, hardworking students will be taking notes and writing up this newsletter so it will almost feel like you can really be in two places at the same time.

CFP on the Loose – What to Do in the City

Ari will be making his regular pilgrimage to Amoeba Records in Haight Ashbury. This music mecca brings many dedicated record enthusiasts to their knees. Ari encourages everyone to experience it for themselves.

For the equally curious, but more scientific at heart, there is a trip planned to the Exploratorium for Saturday. And for those seeking some artistic exposure, the San Francisco Museum of Modern Art is not far from CFP Central.

Ari, the CFP Advisory Board, Program Board, Sponsors, and the lovely city of San Francisco welcome you to CFP 2002.

Have a great conference!

Supreme Court Strikes Down Child Pornography Protection Act

By Laurel Jamtgaard

Civil liberties won a battle today as the U.S. Supreme Court issued a ruling that struck down Congress's attempt to ban "virtual child pornography" by expanding the definition of child pornography. The Court's decision stated that the law "prohibits speech despite its serious literary, artistic, political or scientific value" and could prohibit content from Shakespeare to award winning movies like "Traffic" and "American Beauty." The statute known as the "Child Pornography Protection Act" was passed by Congress and signed into law in 1996. The law prohibited any visual depiction ``that conveys the impression'' of a minor engaging in sexually explicit conduct.

The 6-3 decision was authored by Justice Anthony Kennedy who noted that the criminal statute could be applied to a psychology manual and would cover many movies that included non-minors who nevertheless appeared to be minors. This would have theoretically subjected people who owned such movies to the severe punishment of up to five years in prison.

"This was an important decision because it reaffirms a series of bed-rock first amendment principles and the strong majority helps send a strong message to Congress," said Mark Morris of the Center for Democracy and Technology.

In his dissent, Chief Justice William Rehnquist said that in the absence of a clear intent of Congress, the court need not interpret the statute to reach adaptations of Shakespearean works or films with other literary or artistic value such as "Traffic" and "American Beauty."

Biometrics Exposed with Dr. James Wayman

by Lisa Wang

Dr. James Wayman explains that iris scans, facial imaging, fingerprinting and speaker verification are a few examples of biometrics – automatic methods of identification that require no intrusive physical contact (as opposed to getting a blood sample) and can often be used without the knowledge of the person being identified. Besides looking for criminals, biometrics has wide application in home and computer security, and for large-scale identification needs such as drivers licenses and national ID cards.

At Super Bowl XXXV last year, Tampa police used facial recognition software to scan every person passing through the turnstiles and compared their faces with mug shots of criminals. The scanned fans didn't know they were being recorded, which led to debate about privacy rights in public places – that is, what happens when biometrics technology is used in conjunction with large databases of personal information and without the knowledge of the watched population?

Since that Super Bowl, there has been growing paranoia about biometrics and the potential for "Big Brother" surveillance. Wayman comments paradoxically: "We are 'paranoid' because of unrealistic expectations for a very uncertain technology. On the other hand, our fears should not be assuaged by the current immaturity of the technology." An understanding of how the technology works and its reliability is crucial to formulating privacy and policy questions.

"Most available 'information' on biometrics is technically incorrect," cautions Wayman. "This is because there has been so little scientific research done, so people rely on their 'intuition' on the subject, which is generally wrong. Most marketing folks don't even understand the technical approach used by their own company's devices." His tutorial focused on the scientific results that are

> *"Most available 'information' on biometrics is technically incorrect."*
> *-- Dr. Wayman*

available for these technologies and a scientific description of how the systems actually work.

Vayman says the major obstacles to the development of biometrics technology and its implementation are matching technology to the application, matching the application to the business *(continued on page 8)*

An Interview with Barry Steinhardt – Civil Liberties and Biometrics

by Laura Quilter

Cyber-liberties expert Barry Steinhardt says biometrics is no simple subject.

Many different applications for biometrics are currently being used or proposed. Probably the one that's attracting the most concern right now, comments Steinhart, is "facial recognition technology, which has proven to be an abysmal failure." It was employed summer 2001 in Tampa, Florida, as street surveillance technology, and although the project is still technically in operation, it was actually abandoned by the police department after a month or six weeks because it was just completely useless, generating zero valid hits for the Tampa PD. The Secret Service also had planned to use facial recognition technology for security at the Super Bowl, though this idea was scrapped because the technology had proved such a failure. Facial recognition consumes a good

> *"Facial recognition technology has proven to be an abysmal failure."*

deal of resources, and generates a great deal of bad data. For instance, in Tampa men were identified as women, and older people were identified as juveniles. Nonetheless, government agencies are still looking at it for airport security and for use in police departments.

While facial recognition technology is unique among biometrics technologies in its applicability for surveillance (the technology can be used without permission or even knowledge from the people being scanned), many other biometrics technologies, such as hand-scans or finger-scans, require the cooperation of the individual. Other uses of biometrics include authentication, such as authentication for the corporate network or ATMs. The ACLU generally does not oppose the use of biometrics for authentication purposes, but holds that the collection and uses of biometric data should be subject to certain principles, for instance fair information principles to protect the data from unauthorized uses.

Matching the technology to the application is also a concern. Some high-security applications cannot afford any errors at all, but other applications allowing alternative authentications can handle some errors. For instance, the corporate network could allow a certain number of false negatives (rejecting the user's log-in), because alternative authentication methods could be available. At ATMs, however, even an error rate of one half of one percent (.005) would be significant.

Government agencies particularly involved in biometrics include the Justice Department, the FBI, the NSA, the CIA, and the Transportation agencies. The ACLU is keeping an eye on the proposals for adding biometrics to various ID cards, which involve large government aggregations of data, and will be watching to see how last summer's Supreme Court decision Kyllo holds up in the post-September 11 era.

Barry Steinhardt, Assoc. Director of the ACLU, Chair of the ACLU Cyber-Liberties Task Force, co-founder of Global Internet Liberty Campaign (GILC) and former President of the Electronic Frontier Foundation (1998-2001), will be speaking on the Biometrics Panel, Plenary #4 on Wednesday, April 17, 3:45-5:00pm.

Mike Godwin on Free Speech Challenges Since September 11th

by Jennifer Elliott

When asked how he feels free speech has fared in the wake of the terrorist events of last September, Mike Godwin responds, "Overall, free speech is doing fine." There are no general indications that speech itself is more limited. Occasionally there have been overreactions – people being attacked for having critical views – but on the whole there does not appear to be a serious problem. So, too, there have been issues with respect to Arab-Americans and Muslims – a certain chill on their self-expression. Still, America has reacted as a culture pretty positively. Most of the government's legal response has been limited to police and intelligence surveillance and prosecution measures rather than limitations placed on speech.

Regarding the American press response, Godwin says the press, like the rest of the American public, at first was reluctant to seem critical of the Administration or of American policy. But there's no law against self-censorship. It's a natural tendency to be reluctant to criticize after such an event – every culture has that to some degree. Compared to the press in the rest of the world, the American press is courageous about printing things that the government wants hidden.

Godwin notes that there were naturally some human flaws in press coverage in the aftermath of the September attacks, when the Internet was cast as a threat and there were calls for renewing restrictions on encryption, despite the fact that few of the terrorist's emails had been encrypted. In fact, contends Godwin, the Internet probably reduced the amount of social panic after the attacks,

as mass communication as a nation was possible. "Contrast it to Pearl Harbor or to the panicky response to Orson Welles' 'War of the Worlds' broadcast – this time, people were able to do their own investigations of the attack using the Internet." Also, people used the Internet as

---

The Internet probably reduced the amount of social panic after the attacks.

---

backup communication at the time of 9/11, when telephone lines were congested.

With regard to Congress, Godwin sees Senator Hollings as having missed the boat in the bill he introduced, the Consumer Broadband and Digital Television Promotion Act. Godwin explains that many members of Congress

"seem to believe that the IT community is technically capable of doing anything, so that if the community does not do something, like coming up with a solution for peer-to-peer file-sharing that amounts to infringement, it's just resistance on the part of the industry." These policymakers fail to see that the things that the community is being asked to do are impossible or damaging or both. By contrast, Senator Leahy ran a balanced and comparatively enlightened hearing. He realizes that there is a fundamental disagreement between the two sides about what is even possible, and instead of trying to force Microsoft or Intel to make some kind of concession, he has tried to get the sides to come to some greater understanding about these basic differences.

In his " Constitutional Law in Cyberspace" tutorial on Tuesday, Godwin discussed a range of Constitutional law as it relates to

cyberspace, such as freedom of speech and other issues that shade into privacy and security. He has taught this tutorial every year since the second CFP. This year's session had the highest enrollment ever.

Mike Godwin served as the first Staff Counsel for the Electronic Frontier Foundation, and is currently a Policy Fellow at the Center for Democracy and Technology. He writes extensively about law and cyberspace in a variety of legal, technical, and popular publications, and is the author of Cyber Rights: Defending Free Speech in the Digital Age (Random House/Times Books, 1998).

Wednesday's BOF Sessions
Something for Every Night Owl

Employee Privacy
(Location: Cathedral A)

It's been estimated that one-third of the online workforce in the US has its web and/or email access under continuous surveillance by employers, using web filtering or email management products such as WebSense or MIMESweeper.

What are the social and legal implications? Are employers giving Employees adequate notice of monitoring? Does running all emails through a virus checker even count as monitoring? Are there reasonable alternatives that employers could be using? What privacy interests do employees have on the job? How does US practice compare with that in other countries? These are some of the questions we might discuss.

Leader: Andrew Schulman, Privacy Foundation

Public Records Issues: Privacy, Anonymity and Obscurity in a Democracy
(Location: Marina/Sea Cliffs)

Ready or not we are hurtling toward a confrontation of the fundamentals of anonymity, privacy, access, and citizenship in the era of e-democracy. Buckle up.

True privacy exists only in a vigorous and constitutional democracy. Can democracy exist without a public inspection of voter rolls? Does that mean that privacy can't exist without some public personal records?

Publius.org has been providing public access to Michigan's voter registration file since 1998 (without incident). We invite all the Birds of this Feather, including the celebrity protectors, anonymous participants, and privacy wonks to come down and sort it all out.

Leader: Vince Keenan, Publius

'Last-Mile' Broadband Issues Roundtable
(Location: Presidio/Pacific Heights)

The challenges in bringing high-speed Internet access to the majority of homes and small businesses draw growing interest. In early 2002, the U.S. National Research Council issued a report on this topic, "Broadband: Bringing Home the Bits," ISBN 0-309-08273-0. That report (and other perspectives) will be the starting point for a free-wheeling discussion of broadband access policy, and its significance for the Internet's openness and diversity.

Leader: Myles Losch, ACM SIGGRAPH Public Policy Program

Current Issues in 9th Circuit Internet Defamation and Invasion of Privacy Litigation

(Location: Telegraph A)
Leader: Ellen L. Batzel, Batzel Palm-Leis

State Wiretap Laws After the Patriot Act (SPECIAL TIME: 7PM)
(Location: Cathedral B)

Passage of the USA-Patriot Act in the wake of 9/11 has spurred proposals in many states to increase the surveillance powers of state and local police. This session will report the initial findings on the topic of the Constitution Project's Committee on Technology and Privacy. (See www.constitutionproject.org for information on the Liberty and Security Initiative.) Peter Swire, who was the Chief Counselor for Privacy in the Clinton Administration, will present information on the state laws, and we will discuss how interested persons can get involved in their own states to slow the rush to ill-considered new surveillance laws.

Leader: Peter Swire, Visiting Professor Of Law, George Washington University Law School

CPSR Get Together
(Location: El Dorado Room)
Leader: Susan Evoy, Computer Professionals for Social Responsibility

An Update on PGP with Phil Zimmerman
(Location: Ballroom)

The Future of Anonymous Remailers (Location: Telegraph B)

This BOF will summarize the proposals thus far, and solicit suggestions on improving Mixmaster, a Chaumian Mix-Net implementation and the premier system for anonymous email. Originally developed by Lance Cottrell, and rewritten by Ulf Moeller, Mixmaster is now being maintained by a collaborative effort of anonymous remailer operators led by Len Sassaman.

In the past six months, development on Mixmaster has picked up considerably after a hiatus, though most of the work being done has been limited to bug fixes and minor feature enhancements. Potential improvements to the security and reliability of the Mixmaster software and the remailer network as a whole will be discussed.

Leader: Len Sassaman, Mixmaster

Wednesday's BOF Sessions (continued)

EFF in Action with Cindy Cohn

By Lisa Wang

Cindy Cohn, Legal Director of the Electronic Frontier Foundation (EFF), describes her organization as "basically the 911 of the Internet. Whenever someone gets attacked for their online activities, we get the call, and whenever we can, we answer it."

A primary concern of EFF is preserving free speech and anonymity online. Cohn explains that the basic right to anonymously criticize a company or post an opinion has been threatened by increased "John Doe" litigation. These cases arise when the target of criticism (usually a company or a person) files a lawsuit and then subpoenas the website or ISP hosting the comment to reveal the anonymous critic's identity. Many ISPs simply offer up the requested information without first notifying their customer; however, some ISPs have created notification policies so that customers can challenge the subpoena. Regardless of the outcome of these lawsuits, this type of action has a broad chilling effect on protected online speech.

"It's important to empower customers to ask their ISPs for notification policies and to change ISPs if the ISP refuses," Cohn says. "We also try to let ISPs know what other ISPs, their peers, are doing. ISPs want to be as good as their peers on these issues." Now that the industry leaders (e.g., Earthlink, AOL, Yahoo,

---

"We want to be sure to give these ISPs credit for standing up for their customers and to help other ISPs who want to do so.".

Infospace) are notifying their users as a matter of course, EFF is trying to encourage smaller ISPs to follow suit. In addition, EFF is working with several ISPs to encourage them to file amicus briefs or otherwise participate directly in protecting the right of their customers to speak anonymously. AOL has already done so in several cases, even filing a motion to request to withhold information on behalf of one of its customers. Yahoo and Infospace have also filed amicus briefs in favor of their

customers in John Doe cases. Cohn emphasizes: "We want to be sure to give these ISPs credit for standing up for their customers and to help other ISPs who want to do so."

Other areas of EFF work relate to two themes of this year's CFP Conference: 1) the growing tension between Hollywood and Silicon Valley – namely, whether future technological advances are going to be held hostage to powerful intellectual property holders, and 2) privacy post 9/11. Hollywood is using the threat of litigation or legislative mandates to force technology companies to lock down inputs and outputs to new technologies and limit the usefulness of all kinds of technology; it is also exerting pressure to create technology standards for controlling devices that inter-operate with digital media. EFF has been attempting to shine light on the civil liberties implications of this type of action. For example, EFF has been attending the working group developing standards for HDTV and encouraging its members and the media to start talking. Cohn urges:

"Some pressure must be put on decision makers now, otherwise by the time the actual products make it to the marketplace, it may be too late." EFF is also watching for cases arising from the sweeping new online surveillance powers granted to the government by the USA Patriot Act.

On Friday afternoon Cohn will be moderating Plenary Session #11: Should We Meet John Doe? Civil Litigation and Anonymity in Cyberspace. Various cases and trends, as well as broader online anonymity issues, will be discussed from a legal and technological perspective.

Additional information is available at the Chillingeffects.org website and also the websites of the EFF, Public Citizen, EPIC, the ACLU, and JohnDoes.org. And of course folks can always call or email EFF, Public Citizen, EPIC or the ACLU with specific questions or for help locating an attorney who is familiar with these matters.

Nicky's Picks: Stock up on Great Books at the Conference!

Haven't bought a book outside of cyberspace for a while? Stacey's Bookstore will have a table here at CFP and they have stocked up on plenty of titles on the CFP Summer Reading List and books authored by CFP2002 speakers, so don't miss out on buying some great books at fabulous prices.

Books Available by Conference Speakers

James Bamford:
- PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY
- BODY OF SECRETS

Sonia Arrison and Roger Gibbons:
- WESTERN VISIONS: PERSPECTIVES ON THE WEST IN CANADA

Rubin Avi:
- WHITE HAT SECURITY ARSENAL: TACKLING THE THREATS
- WEB SECURITY SOURCEBOOK

Ann Cavoukian
- WHO KNOWS: SAFEGUARDING YOUR PRIVACY IN A NETWORKED WORLD

James Dempsey:
- TERRORISM AND THE CONSTITUTION

Lawrence Lessig
- CODE AND OTHER LAWS OF CYBERSPACE
- FUTURE OF IDEAS

Jessica Litman
- DIGITAL COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET

John Markoff & Katie Hafner
- CYBERPUNK

Timothy Muris:
- THE BUDGET PUZZLE: UNDERSTANDING FEDERAL SPENDING

Peter Neumann:
- Computer-Related Risks

Peter Neumann:
- DEVELOPING TRUST: ONLINE PRIVACY AND SECURITY

Bruce Sterling:
- DISTRACTION;
- GLOBALHEAD;
- HACKER CRACKDOWN;
- HEAVY WEATHER;
- HOLY FIRE;
- ZEITGEIST;
- SCHISMATRIX PLUS

Peter Swire:
- NONE OF YOUR BUSINESS

W3C Officially "Recommends" P3P: Makes Announcement at CFP

SAN FRANCISCO.

By Laurel Jamtgaard

Yesterday, the World Wide Web Consortium (W3C) announced the long-awaited official recommendation of the Platform for Privacy Preferences specification, or "P3P," version 1.0. To put this in perspective for the process of W3C specifications, "If it were a child, it has reached kindergarten" explained Janet Daly, of the W3C.

Tim Berners-Lee, W3C Director, addressed an information session held at CFP via webconference. "P3p is an important step in addressing the 'privacy policy problem'", began Berners-Lee."

"If P3P were a child, it has reached kindergarten today" Janet Daly of the W3C.

According to Berners-Lee, P3P does two things (1) it is the bridge for layout out the various ways that Privacy Policies differ; and (2) it enables automatic privacy policy comparisons.

Berners-Lee gushed with particular thanks to Lorrie Cranor for chairing the P3P Working Group and shepherding P3P though the development process.

"It has been a long path but was worth the effort. I think we have put together something that will have a real positive impact on helping people protect their privacy." commented Lorrie Cranor at the CFP information session.

"P3P: It is what it is and it is a lot!" noted Information and Privacy Commissioner of Ontario, Ann Cavoukian.

Ari Schwartz, Director of the Center for Democracy and Technology, commented that, "P3P sets up a fundamental base line to build upon."

John Borking, of the Dutch Data Protection Authority, commented that "With P3P, the user has a set of questions in front of him or her and this will stimulate the process of privacy protection. This will create a demand for more P3P-enabled technologies."

Jason Catlett, of Junkbusters, voiced some criticisms of P3P stating that in his opinion automatic privacy policies aren't any good if the underlying privacy policies aren't backed by privacy legislation. Ann Cavoukian responded that while privacy policies are not perfect and are governed by varying degrees of regulation around the world, in her opinion P3P offered an important tool for improving those privacy policies.

P3P may be in kindergarten now but many expect great things from this precocious child.

See   www.w3c.org/P3P and p3ptoolbox.org for more information about P3P.

CFP Word Search

```
GILBRSCIRTEMOIB
RNUVDIEAHPOCKE
AYECRUOSNEPOCN
RYHPARGOTPYRCO
TXUIWBIOCSYKEI
USAPATRIOTACTT
OPEERSNYONRNEA
FAIEEGRYCUIERC
METRHOREUOPHYI
ORHTTEASKSCUOT
LEIOOBNURCWAIN
FREPRIVACYAMJE
ALCEBLAURERH2H
LIBEGMARYOTERT
ESURIAENWAZRDU
PRIVBYTIMYNONA
```

Find the following words or phrases:

* Biometrics
* Cryptography
* USA Patriot Act
* Open Source
* Big Brother Awards
* Peer to Peer
* Anonymity
* Fair Use
* Privacy
* Hackers
* Authentication

Preview of Tomorrow at CFP

- How to Hack an Election @8:45
- Privacy Identity and Location Services
- Activism Online @2:15
- DMCA and You @3:45
- BOFs @9:30

www.cfp2002.com

Sponsors HP and Sun Pitch in for Student Scholarships

Special thanks go out to CFP sponsors Sun and HP for generously donating money to be used for student scholarships. Ari Schwartz, CFP Program Chair noted "There are many students who are fascinated by the issues raised at CFP and who wanted to participate but could not have done so without some financial assistance. HP and Sun have been great sponsors for this year's event and deserve some special recognition."

Biometrics with Wayman (continued from page 2)

process, and finding quantifiable benefit for the business process. Issues in this area that have not received much attention but are important or will become more critical include cost/benefit analysis, "human factors" in sensor design, and large-scale design issues.

Dr. James Wayman, Director of the U.S. National Biometrics Test Center at San Jose State University in California, gave a biometrics tutorial at the CFP conference on Tuesday. His current projects include research on "Authentication Technologies and Their Implications for Privacy" for the National Academies of Science; testing and reporting practices for biometric devices; and development of international standards and policies.

If you have something to contribute to CFPDaily2002 for the Thursday or Friday editions, please send email by 4:00 pm the day before to ljamtgaard@worldnet.att.net with "For CFP Newsletter" in the subject line. THANKS!