Computers Freedom & Privacy

Friday April 7th, 2000

CHALLENGING THE ASSUMPTIONS

BERTELSMANN REPORT SPARKS CONTROVERSY AT CFP

ERNEST MILLER

In September 1999, the Bertelsmann Foundation issued a report on "Self-regulation of Internet Content" addressing several issues regarding Internet content, including the protection of vulnerable parties, finding and evaluating information, and detection of electronic crimes. Some of the recommendations of the report were controversial when it was presented in Munich and the controversy continued at CFP [editor's note: the author contributed to the Bertelsmann's report].

Panelist Dianne Martin from George Washington University provided context for the multi-layered approach to content labeling and filtering in the Bertelsmann proposal by tracing the recent development of labeling and filtering systems, starting with RSAC and console game ratings through the development of W3C's Platform for Internet Content Selection (PICS) and ending with ICRA. Martin explained that the Bertelsmann proposal was a significant improvement upon previous systems because it separated labeling from the filtering. More importantly, she noted that the proposal was both more technically and socially complex, permitting greater context and multiple cultural values systems.

The history lesson took a different turn as Christopher Hunter, Ph.D. candidate at the University of Pennsylvania, analogized the system to the Catholic Church's list of banned books during the Middle Ages. Hunter feared that the system would not remain voluntary as the report recommended, but that governments would make compliance a legal requirement. Nevertheless, he claimed, many sites would remain unrated and be banished to a "no man's land where browsers fear to tread."

Jordan Kessler from the Anti-Defamation League supported the proposal and was pleased by many aspects of the system, including the choice it provides consumers to choose different red/green lists and templates, the use of encryption to prevent upstream filtering and most importantly the default setting that unrated sites not be filtered. The role of the user was of key importance argued Kessler, saying that "users are not sheep. If users are smart enough to turn the default settings off, they are smart enough to find and use white lists."

The final speaker was Barry Steinhardt of the ACLU who listed a number of the problems he found with the proposal. The biggest problem, claimed Steinhardt, was that websites would face a dilemma: either self-label and be blocked or fail to rate and be blocked. He also saw the scheme as too burdensome for website creators, citing one artists' website with over 25,000 pages of content. Steinhardt also reiterated Hunter's point that the voluntary nature of the proposed system was illusionary.

A number of questions from the audience followed, but the questions revealed that the audience was as divided as the panelists on the issue.

JORDAN KESSLER, BARRY STEINHARDT, CHRISTOPHER HUNTER AND DIANNE MARTIN

TODAY'S HOT TOPIC: HEALTH PRIVACY

LINA TILMAN

Historically, a puzzling dichotomy has been present and visible in the prevailing attitude towards health privacy on behalf of healthcare consumers in the United States. While most agree that medical data inherently merits high expectation of privacy, and hence strong legal protection, consumers have traditionally acknowledged and accepted that they actually possess little or no control over access, distribution and use of their personal medical records. The paradox resulted from the apparent conflict between the consumers' culturally accepted notion of and approach to sensitive personal information and a virtually unregulated freedom on behalf of healthcare providers, health plans, clearinghouses, and law enforcement agencies, to obtain and employ health records.

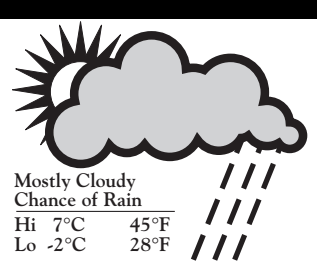
Rapid proliferation of information and communication technologies have forced healthcare consumers to redefine, reevaluate and readdress their privacy expectations and needs. It has been empirically established that there exists today an inversely proportional relationship between personal control over one's medical data and the patient's privacy protective behavior, which adversely affects the abilities of the patient's healthcare provider to research and treat health conditions. A survey by the California Health Care Foundation found that one out of every six individuals engages in some form of privacy-protective behavior to shield themselves from the misuse of their health information (including lying to their doctors, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and avoiding care altogether). Individuals who fear that their sensitive medical data will be distributed and/or misused thus withhold participation or actually interfere with the effectiveness of their healthcare.

In 1996, the United States Congress effectively acknowledged the legitimacy of the increasing privacy concerns regarding health records in the integrated digital world when in passed the Health Information Portability and Accountability Act. Last November, the Clinton Administration submitted a proposal to Congress that further dealt with the growing concern regarding the nation's weak or non-existent federal regulation of access to hard-copy and digitally stored health data. Since its submission, the document has created notable controversy on two accounts: the first was its failure to propose meaningful restriction with regards to law enforcement agencies access to medical data; the second, Congresses' inability to meet its August deadline for passing a comprehensive health privacy legislation.

Two primary barriers to improving medical care exist in the United States: the incomplete, disintegrated nature of medical data collection, management and storage; and the lack of enforceable privacy standards with regards to access, distribution and use of private medical data. While meaningful integration — which presupposes facilitated access and use — would greatly improve the efficiency of both the healthcare and the criminal justice systems, it must be viewed and evaluated in the light of the direct affect on privacy and personal control that such consolidation entails. Healthcare consumers, along with care providers, privacy advocates, and legislators, will continue to conceptually and practically balance the fundamental right of privacy against need for security and efficiency.

What's Inside

Today's Weather



Mostly Cloudy
Chance of Rain
Hi 7°C 45°F
Lo -2°C 28°F

CFP IN THE NEWS

WATSON, ECHLON NEEDS YOU

DREW CLARK
REPRINTED WITH PERMISSION FROM NATIONAL JOURNAL'S TECH DAILY

The chairman of a key committee in the European Parliament has drafted a resolution condemning Echelon for invading European citizens' privacy, the author of one of the crucial reports on the American-led surveillance system said Thursday.

The resolution is expected to be introduced on Thursday by Graham Watson, chairman of the European Parliament's Committee on Citizens' Freedoms and Rights, said author Duncan Campbell at the Computers, Freedom and Privacy conference. The measure, which could likely pass, calls upon member countries of the transnational body to "take necessary diplomatic steps to prevent third party countries from carrying out any form of interception on the territory" of the European Union.

"All interception must have a legal basis, be in the public interest, and be strictly limited to the achievement of the intended objections," according to a copy of the resolution read by Campbell. "Any more of systematic interception cannot be regarded as consistent with the principles" of citizens' liberties, even in the fight against international crime.

The resolution adds to the privacy storm over Echelon, part of an increasingly discussed U.S. and British-led system of intelligence gathering of the electronic signals emanating from telephone calls, faxes, and apparently e-mail communications.

According to a European Parliament report written by Campbell, the system has been used to systematically spy on diverse collection of non-U.S. targets including French businesses, the Red Cross, Pope John Paul II, and the late British industrialist Robert Maxwell.

The U.S. House Select Committee on Intelligence is scheduled to hold a public hearing Wednesday addressing the legalities under which signals intelligence systems, including Echelon, gather information about U.S. citizens.

"It is apparent that the public has concerns that it has not seen answers to," said an Intelligence Committee staffer. "There is hope that this hearing will go at least a part of the way to informing the public."

National Journal's Technology Daily is published every weekday, except holidays, by National Journal Group, 3129 Mt. Vernon Ave., Alexandria, VA 22305, and is available to subscribers on the Web at: www.nationaljournal.com/pubs/techdaily

Selected articles from the PM Edition are reproduced by permission for the duration of Computers, Freedom & Privacy 2000 conference.

Information about subscribing and obtaining a 30-day free trial can be obtained by contacting Sales Director Libah Jane Grossman at lgrossman@nationaljournal.com or at 703-518-8722.

Looking Forward · Looking Back

Friday April 7th, 2000

CHALLENGING THE ASSUMPTIONS

On Friday, at the conference's last session, we will celebrate 10 years of CFP with a special panel featuring some of the most influential and memorable participants throughout the conference's storied history. In preparation, we asked the past CFP chairs about their view of where the conference has been and where it is going.

KENT WALKER LOOKS BACK

Q: *HOW HAVE THE ISSUES AT CFP CHANGED SINCE THE CONFERENCE THAT YOU CHAIRED?*

A: *"CFP 97 WAS A TRANSITIONAL YEAR, SHIFTING FROM THEMES OF GOVERNMENT VERSUS INDIVIDUALS INTO A BROADER DISCUSSION OF THE INTERACTIONS (POSITIVE AND NEGATIVE) BETWEEN INDIVIDUALS (AS INDIVIDUALS, AS CONSUMERS, AND AS CITIZENS) AND GOVERNMENT, BUSINESS, AND THE BROADER COMMUNITY. NEW TECHNOLOGICAL DEVELOPMENTS, BUSINESS MODELS, AND GOVERNMENT INITIATIVES REQUIRE A CONTINUAL RE-EXAMINATION OF THOSE CRITICAL UNDERLYING THEMES."*

— KENT WALKER, CFP CHAIR '97

BUILDING DIVERSITY

ISSUES OF DIGITAL DIVIDE TO BE EXPLORED

NOAH ROMER

Before the Internet came into common use the online world tended to be a monocultural place, a world that consisted primarily of technologically advanced males in the industrialized West with higher than average income levels. This has changed substantially, but the demographics and attitudes of the online world still do not reflect the greater diversity of the general population. What is lost because of this?

For those already online there is the loss of differing viewpoints on numerous issues ranging from discussions of flaming and spamming to technical details such as how to expand the number of top level domains. The online community is also harmed because a lack of diversity often leads to "cultural inbreeding," increasing occurrences of previously pathological situations and decreasing ability of the community to respond to or even identify risks. Cultural inbreeding can also create an inability to ask fundamental questions about the place of technology in the lives of people who will be affected by it. The Internet is changing the lives of people, even those who have little or no direct contact with it. There is a responsibility to examine the intended and unintended consequences of technology — and not only after technologies have been implemented, but while they are being conceived and designed. We must therefore ask how this can be done effectively if people from a more diverse range of geographies and cultures are not part of the online world.

The Internet provides a vast, if rather unorganized, source of research information. The Internet provides a rich source of knowledge and skill, but only to those who have access to it. The question, then, is how can diversity in the online world be built? Such efforts will be discussed in the opening panel on Friday.

CRANOR & HURLEY

VISIONS FOR THE FUTURE

CFP newsletter editor Patrick Feng caught up with Lorrie Cranor, chair of this year's conference, and Deborah Hurley, chair-designate of next year's conference, and asked them to reflect on their experiences with CFP.

Patrick Feng: You've been involved in a number of CFPs. What changes have you observed over the years?

Lorrie Cranor: Well, the issues have evolved over time. For example, crypto was discussed a great deal in the early CFPs, but now not so much. Also, the Internet has moved from being something centered around a small group to much more of a public space.

"...WHAT WE MEAN BY FREEDOM AND PRIVACY HAS CHANGED. FOR EXAMPLE, THREATS TO PRIVACY FROM BIG CORPORATIONS ARE AN ISSUE NOW, SOMETHING THAT WAS NOT DISCUSSED EARLIER ON."

— LORRIE CRANOR CFP CHAIR '00

PF: Freedom and privacy have been important issues for CFP. Are there any other issues that you'd like to see addressed in these conferences?

LC: I think the people at this conference should still concentrate on freedom and privacy, but what we mean by freedom and privacy has changed. For example, threats to privacy from big corporations are an issue now, something that was not discussed earlier on. Back then, the online world was not a corporate world. Now it's much more corporate — this has brought lots of positive changes, but also new problems.

PF: Are there any directions you'd like to see CFP take in upcoming years?

LC: I'd like to find ways for CFP participants to get more directly involved in enacting change and improving the world.

Patrick Feng:: You've been involved in a number of CFPs. What changes have you observed over the years?

Deborah Hurley: Computers, freedom, and privacy have been the central issues of this conference, but of course the emphasis has shifted over the years. A few years ago there was maybe more focus on freedom; the last few conferences have been more focused on privacy.

I'd also look at the similarities between conferences. CFP has really strong community; the conference serves as a space to meet one another. For a conference with no permanent steering committee, there is a great deal of work that goes into this. People commit lots of time to this conference. At some other conferences people go shopping or skip sessions — CFP attendees stay in their sessions.

PF: Freedom and privacy have been important issues for CFP. Are there any other issues that you'd like to see addressed in these conferences?

DH: Well, computers, freedom, and privacy are three very broad categories. I don't think we need any more top-level domains, so to speak. But underneath those broad domains, I think we need to begin grappling with the ubiquity of information. Also, we need to get tools into people's hands, so that they can deploy those tools widely.

PF: As chair of next year's conference, what directions would you like to take next year? Where to now?

DH: These issues are global phenomena with significant local impact. The people who attend CFP know that. The conference acts as a modality to meet with like-minded people. I think we want to focus more on how to address the global aspects of computerization and on how to build technology so as to affirm our social and economic values.

Computers Freedom & Privacy

Friday April 7th, 2000

CHALLENGING THE ASSUMPTIONS

NOTICES

DON'T FORGET EVALUATION FORMS

The organizing committee spent many many hours putting together this conference. Now it is your turn to contribute a few minutes to the organization of future CFP meetings. Please be sure to fill out the CFP2000 Evaluation Form that was included in your packet.

Remember to use the back of the form to identify your favorite session(s) and share any additional thoughts you may have on the conference. Remember, your feedback will help improve future meetings! And your responses will be kept confidential. :)

Look for the big boxes in the back of Harbour Ballroom to deposit your forms.

OPEN SOURCE NOTES

Following a tradition begun by Lorrie Cranor, several attendees are making their private notes from the conference publicly available. Roger Clarke, whose notes and commentary last year received 20,000 hits, will have his up at www.anu.edu.au/Roger.Clarke/DV/NotesCFP2K.html as early as tomorrow. Privacy Place's Tom Maddox has his up throughout the Privacy Place site www.privacyplace.com.

STUDENT AWARDS

We would like to commend the winners of the CFP2000 Student Paper Competition for their outstanding contributions.

The Competition was held to highlight the work of up and coming young scholars interested in cyberpolicy issues. The committee judging student papers received numerous submissions, representing a wide range of issues, from students around the world.

Christopher D. Hunter, from the Annenberg School for Communication of the University of Pennsylvania was awarded $500 for his Most Outstanding Student Paper, "Internet Filter Effectiveness: Testing Over and Underinclusive Blocking Decisions of Four Popular Filters," which examines the effectiveness of four commonly used Internet content filters.

Patrick Feng, of the Rensselaer Polytechnic Institute was awarded $250 and Honorable Mention for his essay, "When Social Meets Technical: Ethics and the Design of 'Social' Technologies," which addresses the social and ethical concerns raised during the technology development process.

Finally, Mark V. Hurwitz, a Senior Fellow at the Space Sciences Laboratory at the University of California — Berkeley who was unable to attend the conference, was recognized for his Honorable Mention paper, "Quantum 'Encryption." This paper examines the workings of quantum encryption technology and its profound implications for security on the Internet.

A REALIZATION OF NEAL STEPHENSON'S "SECRET-SHARING" SECURITY SYSTEM

OP-ED MARC WALDMAN

During his April 5th CFP talk, author Neal Stephenson pointed out that it is now possible to monitor your home from just about anywhere in the world via the Internet. Of course one needs a persistent connection to the Internet, Webcams and perhaps other Internet enabled devices, but these are all minor details. The main concern is privacy. While it is great to be able to monitor your home over the Internet you want to prevent others from monitoring your home as well. Secret key mechanisms can be used but Neal Stephenson pointed out another alternative. Instead of simply storing the Webcam images on your own PC why not store them on several web servers, perhaps one owned by law enforcement or a security service. This brings us back to the privacy problem. While we want law enforcement to be able to view a picture of someone committing an illegal act, we may not want law enforcement to view all our Webcam pictures. Stephenson's solution is to use a technique called secret sharing to store so called shadows on each of the Web servers rather than storing the Webcam image itself. Secret sharing is a technique that is used to split a password (or any collection of bits), into n pieces called shadows or shares such that only k of them are necessary to reconstruct the original item — the password in this case. The value k can be less than or equal to the value of n. For example a password can be split up into 10 shares such that only 5 of them are needed to reconstruct the password. Combining less than k shares does not reveal the password. Instead of the password, Stephenson suggests we secret-split the Webcam image itself. In this scenario, only one share is stored on the law enforcement Web server instead of the whole Webcam image. This can safely be done because the solitary share is useless by itself. However if we want law enforcement to view a particular image we just send them the other k-1 shares.

Although Stephenson suggested this as a possible project, a system named Publius, already does something similar and incorporates several unique WWW publishing mechanisms. Publius is a censorship resistant, tamper evident, WWW-based publishing system. It was designed by Lorrie Cranor (AT&T Research), Avi Rubin (AT&T Research), and Marc Waldman (NYU Computer Science Dept.). Publius allows an individual to publish static WWW-based content (HTML, PDF, GIF, JPG, etc) on several servers at once such that each server cannot tell the type of content it is hosting and any modification to the stored content can be detected. Publius utilizes a secret sharing mechanism but not in the way described by Stephenson, however the net effect is the same. Publius is written in Perl and will soon be freely available for download at the following URL: www.cs.nyu.edu/~waldman/publius.html. A paper describing Publius is also available at the previously stated URL.

Please send any questions concerning Publius to Marc Waldman (waldman@cs.nyu.edu)

FTC COMMISSIONER THOMPSON RELATES U.S. VIEW OF PRIVACY

BRETT BURNEY

"It is an exciting time to be at the FTC," Mozelle Thompson stated after his speech on Wednesday. He sat and spoke with interested listeners for well over an hour and a half before going to dinner. Commissioner Thompson's speech, and his after-speech remarks, focused mainly on the issue of privacy — since the Federal Trade Commission is currently the closest thing that the United States has to an established privacy commission.

It was well noted that the United States was absent from the panel of Privacy Commissioners that spoke right before the FTC Commissioner. Commissioner Thompson himself recognized that the U.S. lacked a formal organization devoted to the issue of individual privacy, but stated that the FTC has been active in the relevant areas of concern. He noted that the U.S. does not actually have direct legislation concerning individual privacy, as other countries do, but that there is existing case law that has repeatedly reiterated our presumption of privacy in the U.S.

Commissioner Thompson passed off the question of whether legislation is "the answer" several times. More than a few people tried to push him into a corner on the legislation issue, asking whether it was going to happen now or later. The Commissioner refused to answer because 1) the issue is fairly controversial, and 2) the Internet is still in its infancy and we need more input — such as the expected report from the recently formed Online Advisory Committee. Commissioner Thompson said he expects to see the report sometime around June.

Instead of dwelling on the legislation question, the Commissioner focused on education. He declared that we need education for both businesses and for consumers, i.e. individuals surfing the Net. We should concentrate on making consumers aware of how information about them is being used and gathered when they surf particular sites. But we also need education on the business/corporate side. Commissioner Thompson suggested that businesses could take an example from IBM and Microsoft which do not advertise on Web sites that do not have a stated and enforced privacy policy for their surfers.

CHUCK CRANOR AND COMMISSIONER THOMPSON

After discussing the above "policy" issues, the speaker then switched to the FTC's primary function of enforcement — citing cases such as GeoCities and the pending issues with Yahoo! and DoubleClick. He pointed out that problems like these cannot be solved by the FTC alone, rather, all levels of enforcement must interact together to create a successful level of privacy on the Internet. There must be interaction among individuals, businesses, and of course, the government. Moreover, it does not stop there. For enforcement to be effective in a wired world, there must be cooperation among different countries. Commissioner Thompson stated that "privacy is a very important issue, but it cannot be viewed in isolation."

The interest from the audience for discussion exceeded the amount of time for questions and answers during the session. The Commissioner continued the conversation with interested attendees in the foyer for over an hour after his talk. He was kind enough to answer everybody's question and exchanged business cards with anyone that offered. This is when he made the statement that working at the FTC is a pretty exciting business these days. He noted that what is happening in the online privacy realm today is not the result of laws, but of companies working together, mostly in their own interests. It may not be the best situation, but Commissioner Thompson reserved comment on what could or will happen in the near future. He stated that fraud is fraud, no matter where it happens — on TV, over the telephone, or on the Internet — and that the FTC is committed to protecting against it.

Before rushing off to dinner, the Commissioner made an important statement to the last remaining listeners about the general purpose of conferences such as these: "it's not about the technologies, it's about the policies." He explained that the technologies will take care of themselves. However, the policies that need to be established and worked out before our online rights get lost in the techno-shuffle.

Computers Freedom & Privacy

Friday April 7th, 2000

CHALLENGING THE ASSUMPTIONS

PRIVACY IN THE PACIFIC RIM

NADIA OLIVERO

Although it is arguable that in the electronic era information and knowledge are no longer limited by being in a certain place, geography can still have a fundamental impact. This is particularly relevant when it comes to issues of personal data privacy. In this regard the Pacific Rim provides an excellent case study because of the richness of its cultural diversity in terms of attitudes towards authority, the role of the state and the role of the individual in society. The co-existence of more mature democratic models with emerging democracies and more authoritarian patterns of government produces an heterogeneous approach to personal privacy protection. Regardless of these different political frameworks, all of the countries in the Pacific Rim are experiencing increasing pressure to conform to externally defined privacy norms.

This session, discussing the latest developments in data protection in Asian Pacific countries, will provide a critical assessment of the actual legislative outcomes. Looking at the range of predispositions towards privacy issues, even these current results are interesting. How will the users adapt to the new views of privacy? Will they accept the proactive role required of them? And how will states and corporations interpret their new obligations?

The immediate future of privacy regulation in the Pacific Rim could provide a natural observation field to examine opportunities and limits of globalization.

PANEL: "SECURITY PROBLEM IN BROADBAND"

LAUREN MATHESON

The results are in. According to the panel of four broadband experts there is a real security problem: default file sharing, viruses, and careless or clueless users are the primary reasons. AT&T expert John Denker proposes that a threat analysis is necessary before trying to tackle the issue of network security. To protect a network against a foreign intruder or cracker requires different measures than against a friend, a host, a legal warrant or tap, a trojan virus, or data miners. The ability to protect is also quite different, especially against trojan horse viruses which users choose to install, but act much differently than expected. Data mining can also be difficult to avoid. A naïve user may voluntarily disclose information, not realizing that it may be kept for a different use or joined to their information elsewhere, a phenomenon referred to by Denker as "getting nibbled to death by ducks."

Solutions, or at least stop-gap measures to some of these problems do exist and are being used by broadband providers. Commonly misconfigured ports — such as that used by the NetBIOS service in Microsoft file sharing — are frequently blocked by default. Modems operating as bridges filter packets at the user level so that they only receive information directed to them and not their neighbors. New modems incorporating firewalls may soon be used, thus enabling a heightened level of security without extra software to install. Similar hardware solutions also bypass the inherent insecurities of some operating systems. The panelists seemed to be in agreement though that configuration and implementation of security solutions must be understood by novice computer users to be effective.

Privacy may become a new arena for market competition. As consumers become increasingly aware of the degree of their exposure they will quite possibly demand higher standards from their ISPs. Freedom may also become a consumer choice as many may choose ISPs, which filter certain types of content, thus creating more consumer options. If technology is the limitation, ISPs will be very competitive as their privacy standards will be comparable. However, this is all contingent upon the consumer's ability to differentiate between products based on privacy — an assumption which might not be valid.

Next, the panel considered the roles of different groups. Governments should be expected to set standards that guarantee personal privacy. However, industry may lead the government standards through as consumer demands grow. As for customers, Dermot O'Carroll longed to be able to expect from them some degree of rational behavior where they would learn to use a machine before pushing the limits. Simson Garfinkel proposed increased liability for software vendors and broadband providers which leave security holes open by default, a view supported by an analogy that certain levels of safety are expected from many other industries. But software is not held to the same consumer standards, and Denker strongly objected that liability is a model that simply does not work.

While broadband network security is a problem, it does not have a simple solution because end users are a part of the problem. However, if users become more knowledgeable and demanding, security failings may well be significantly reduced.

CFP INTERVIEWS KEN OLTHOFF

Ken Olthoff creates a buzz when he walks through the halls of the CFP conference — "Does he really work for the U.S. super secret National Security Administration (NSA)?" attendees have been overheard asking one another. For those still not in the true CFP spirit, who have been afraid to ask Ken directly, the answer is yes. But, are his annual trips to CFP official business? "They pay my way, but the views expressed are not those of the management," Ken has been known to say.

Ken's official title is Senior Engineer at NSA. He has a long background in the information sector and has been at NSA 16 years. Before arriving at NSA, he was at Purdue University. Ken is also quite proud to be the first person to have a play published as part of an ACM conference proceedings — the forthcoming "New Security Paradigms Workshop."

CFP News — Why do you come to CFP?

Ken — For two reasons:

1) It keeps me intellectually honest. I get exposure to people who can provide an intelligent and rational opposing view to my own. It is easy to argue with someone who is intellectually sloppy.

2) It is the one place to meet with everyone on the cutting edge of legal, technological, social and political fields all at once. I often go to technology conferences where everyone is focussed on the new, bright, shiny things, but not the long-term social implications.

PANEL DEBATES COPYRIGHT CIRCUMVENTION

BRETT BURNEY

Is circumvention a tool for freedom or crime? Thursday's session discovered that there are only a few answers to this question, and they are far between.

The session was well attended and the panel (Robin Gross, Declan McCullagh, Paul Schwartz, Barry Steinhardt, and organizer Alex Fowler) expanded to include John Gilmore, Pam Samuelson, and Jessica Litman. Questions from the floor came from lawyers, techies, and a librarian.

Fowler started out the discussion by allowing Robin Gross, staff counsel for the Electronic Frontier Foundation, to discuss her work on the DVD/DeCSS case. She explained that two of the four cases involving the DeCSS utility hinged on the new Digital Millennium Copyright Act (DMCA). There are two main sections of the DMCA under fire in these cases: 1) the act of circumvention and 2) the creation and distribution of tools that allow the act of circumvention. Panel members pointed out that the second section is no longer an intellectual property issue. Rather, it is a free expression issue given that it is a general prohibition on distribution. However, Gross pointed out that the question remains one of intellectual property simply because there is a potential for copyright infringement.

Barry Steinhardt of the American Civil Liberties Union spoke on the CyberPatrol case. The "tool" in this case was a little program called cphack that 1) allowed users to unmask the list of sites that were blocked by the CyberPatrol program and 2) allowed users to discover hidden passwords. Schwartz pointed out that the significance of this case lies in that it did not involve piracy nor the obtaining of illegal copies of CyberPatrol, rather, the circumvention of certain protections.

Paul Schwartz, an expert on privacy from the Brooklyn Law School, talked about the "quasi-public privacy exception" section of the DMCA. This subsection apparently allows users to circumvent technologies in order to protect their privacy. Pam Samuelson pointed out that if this subsection does indeed allow users to circumvent, other parts of the DMCA prohibit you from creating a tool to allow you to do the circumventing! Samuelson continued that the DMCA appears to be "rife with contradiction" and "totally incoherent." Taking her argument, one could read into the DMCA an embedded right to create the tools, but then a person would still be prohibited from the actual distribution of such tools.

Lastly, Declan McCullagh from Wired News spoke briefly on the difficulty of getting the general public interested in cases involving intellectual property. While he did say it that was possible to get an editor interested in such a story by using creative and catchy headlines, he argued that the general public is not motivated enough to get involved in issues and cases that will affect it more than it realizes.

The session was very enlightening and interesting. Several questions posed difficult but contemporary problems that the panel could not answer, simply because there was no answer. Pam Samuelson noted that she had spoken with several writers of the DMCA and they had purposefully left sections ambiguous so that they could be worked out later in the courts. We can only hope that the right cases land in the right courts and that the question of "freedom or crime" is answered correctly.

ROBIN GROSS, DECLAN MCCULLAGH, BARRY STEINHARDT, PAUL SCHWARTZ, AND ORGANIZER ALEX FOWLER