In September 1999, the Bertelsmann Foundation initiated an examination of "Networking of Internet Content" addressing several issues regarding Internet content, including the protection of vulnerable parties, filtering 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 paradox resulted from the apparent conflict between the consumers' culturally acknowledging the legitimacy of the proposed labeling 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.

In 1996, the United States Congress effectively acknowledged the legitimacy of the proposed labeling 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.

Rapid proliferation of information and communication technologies has forced the healthcare consumers to reconsider their privacy expectations and needs. It has been empirically demonstrated that there exists 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 health-care 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-shopping 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 used 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-shopping 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 used.

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 conceptualize and practically balance the fundamental right of privacy against need for security and efficiency.

The final speaker was Barry Steinhardt of the ACLU who listed a number of the problems he found with the proposal. The most glaring problem, claimed Steinhardt, was that websites would face a dilemma either self-label and be blocked or fall to rate and be blocked. He also saw the scheme as too burdensome for website creators, citing one artist's 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 divided as the panels on the issue.

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 signal emanating from telephones, 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 businessmen, 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."

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 objectives," according to a copy of the resolution read by Campbell. "Any more of systematic interception cannot be regarded as consistent with the principles" of citizen's rights, even in the fight against international crime.
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

Challenging the Assumptions

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 new problems.

What is lost because of this?

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. 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: 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.

Cranor & Hurley

Visions for the Future

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 another conference, 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 we 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 need 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.

Looking Forward - Looking Back

Friday April 7th, 2000

Cranor & Hurley

Visions for the Future

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 another conference, 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 we 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 need 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.
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 for last year received 20,000 hits, will have his up at www.ima.umn.edu/RogerClarke/DF/ Notes.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. Horwitz, 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-EID 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 a picture of 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-splat the Webcam image itself. In this scenario, only one share is stored on the low 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 low 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 technologies. Publius is a censorship resistant, tamper evident, WWW-based publishing system. It was designed by Lorrie Cranor (AT&T Research), Ari 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.ccs.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

“lt is an interesting time to be at the FTC,” said Commissioner Thompson 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 an 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 pull 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 sites.

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 program for protecting 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 exchange 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 let us know what 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.

CHUCK CRANOR AND COMMISSIONER THOMPSON

“Online rights get lost in the techno-shuffle. Establish and work out the policies first and the technologies will take care of themselves.”
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 coexistence of more mature democratic models with emerging democracies and more authoritarian patterns of government produces an heterogeneous approach to personal privacy protection. Regrettably, 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 proceptive 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.

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 the session in the Pacific Rim could provide a natural observation field to examine opportunities and limits of globalization.

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.

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

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.