CFP

Saturday

April 20, 2002

Author Bruce Sterling Brings CFP2002 to a Close

by Nicole Acton

Bruce Sterling began his rich keynote address by comparing the state of his email in 1990, the year of the first CFP, to now. After comparing the volume and content (5 messages/day from engineers to 44 messages/day mostly from spammers) and the level of viruses, he concluded that email is a mixed blessing. After looking out into a crowd of attendees pecking away at computers connected to a wireless network, he announced that he had left his computer at home (alongside his cell phone) and had seriously contemplated bringing his manual typewriter. But because he couldn't find a ribbon, he resorted to writing his speech with a fountain pen and without access to Google.

CFP2002 was a great success!

Thanks for coming.

See you next year!

Sterling's speech included commentary on the DMCA: Is fear of prosecution the explanation for why, among the hundreds of experts staying at the hotel, not one person lodged a complaint about how Channel 19 played the same 7 seconds of a scratched DVD all week? And surely that creepy "Dell guy" must have a hard-drive crammed with infringing works. As for the Indian movie industry, it was regrettable that the movie-star he worshipped would never be compensated adequately.

The remainder of Sterling's speech defended the Bush Administration, recognizing that it is hard to keep a level head in the face of a "decapitation scenario." He began with John Ashcroft, saying that griping about him was akin to hissing at the villain in a melodrama. According to Sterling, Ashcroft is the designated heavy. As for the rest of the Administration, the fact that they don't want to get killed goes far in explaining what others might see as bizarre behavior. After all, how many major companies, NGOs or law firms have contingency plans for the annihilation of their headquarters?

Sterling does not think that courage is the problem considering that Colin Powell is a *General* and he is the "softie" of the group. Rather, he just wishes the Administration wouldn't treat the rest of us (and that includes Congress) like children.

Even though Sterling left his computer at home for this CFP conference, what he really lamented was the absence of his Swiss Army knife. He concluded that while he could survive just fine without the laptop, he had a hard time accepting his ragged, dirty fingernails…

Peer-to-Peer Legal Battles Continue as New Middleware is Announced

by Eddan Katz

Amidst a backdrop recounting the legal obstacles facing the development of peer-to-peer networks and the effect of legal activity on Internet service providers (ISPs), Frank Hausmann, Chairman and CEO of Centerspan, introduced his company's new product C-StarOne, having announced this content delivery platform publicly just that week. Centerspan has struck a deal with Sony to deliver content through their network and is in negotiation with major Hollywood companies to do the same. Dubbing the project a "bridge-building effort," Hausmann explained that C-StarOne will enable copyright owners to distribute high-quality streams and on-demand downloads at half the cost of other delivery solutions in a secure environment, providing a "legal alternative" to file-sharing networks like Napster, Morpheus, and others. End-users who subscribe to the content delivery services of Centerspan's clients will dedicate 50-100MB of obfuscated cache on their hard drive to pieces of content distributed throughout the network, which will be available for delivery to a consumer's computer without being slowed down by a congested central server.

While the innovative C-StarOne product was generally welcomed with interest, some audience members pointed out that the network abandoned some core features of peer-to-peer networks, such as the ability of end-users to publish their own files. Responding to concerns that consumers will be forced to share their computing resources to use the network and that the product requires a large installer base to work, Hausmann explained that the minimal space requirements and segmentation of content will be nearly invisible to any individual computer. Hausmann also explained that the C-StarOne network will allow digital content to be delivered without embedding digital rights management (DRM) systems and privacy-invasive data collection due to layers of security inherent in the distributed network and the segmentation of files.

No peer-to-peer case has actually come to trial yet, but several are pending. --Fred von Lohmann.

Fred von Lohmann, Senior Staff Attorney at the Electronic Frontier Foundation (EFF), provided a review of the legal landscape concerning existing peer-to-peer technologies prior to Hausmann's announcement. Von Lohmann reviewed the systematic legal attack by content owners against the development of file-sharing technologies. The variety of legal tactics described included seeking a preliminary injunction based on contributory copyright claims against a technology (as in Napster), driving company

(continued on page 2)

ICANN in Year Three: At a Crossroads or a Dead End?

by Abigail Phillips

ICANN has hit another crossroads—or is it the same one? The broad consensus today is that ICANN hasn't worked. The goal for tomorrow is to fix it. Center for Democracy and Technology Executive Director Jerry Berman, careful not to stray from his moderator agenda, asks the driving question: What are ICANN's essential functions and what role should ICANN have in the future? ICANN will not spontaneously cede power and rethink itself. In order to change it, we need to find a model we prefer and then argue that model into implementation.

Here's how ICANN Board Member Karl Auerbach puts the question: "If ICANN vanished, what would happen?" Not all that much, it seems. The Internet is no more, Auerbach avers, than a mechanism that moves IP packets. The naming service that we happen to layer on top is optional. While he's convinced that it's critical to keep the packets flowing, he's not so sure that the names part is indispensable. At the least, Auerbach concludes, ICANN is working full time at a part-time job.

The broad consensus today is that ICANN hasn't worked.

Auerbach envisions three main responsibilities for ICANN: managing technical parameters (i.e. the classic IANA function of assigning numbers), managing IP address space, and managing domain name space. This includes administering the root zone file and ensuring that the root servers are run responsibly. At the same time, ICANN needs affirmatively to stay out of other arenas, in particular trademark law and management of "whois" databases.

Auerbach proposes a structure for ICANN that divides responsibilities among six legally and bureaucratically independent areas – three with purely administrative functions, three with more discretionary, policymaking roles.

Susan Crawford, a partner at the law firm of Wilmer, Cutler & Pickering, agrees that ICANN is in need of an overhaul. She thinks the organization has been hijacked from within, and that its actions evidence a fundamental misunderstanding of what it should be doing. For one, Crawford says, ICANN's job is decidedly not Internet governance; it is not – and in fact it's unrealistic to think it might be – a vehicle of democracy serving the interests of diverse users. Nor does ICANN need to be an international consumer watchdog protecting users against predatory registrars. It does not have to perform a technical role either. In the end, ICANN should exist only to set a few global domain-name policies. She cautions us to remember that however bad ICANN may seem, it's better than the alternative.

Crawford also makes a rare plug for ICANN's Uniform Dispute Resolution Policy (UDRP). While most seem to see UDRP as one of the unfortunate fruits of the organization, Crawford likes it. Its genius, she says, lies in the fact that it doesn't attempt to mirror the trademark law of any one nation. It is a novel system that helps trademark owners cope with the domain name system and establishes a relatively inexpensive, simple, and quick way of resolving disputes – as compared to the court alternative, that is.

Peter Neumann, Principal Scientist at SRI International Computer Science Laboratory, echoed the advocates for a narrower role for ICANN. He is concerned with having concrete proposals for concrete solutions as a necessary step toward reform of the organization. Appropriately, he has collaborated on a detailed solution that he has published online: http://www.pfir.org/statements/icann. Check it out.

Peer-to-Peer Panel *(Continued from page 1)*

executives into bankruptcy (as in Aimster), and suing search engines facilitating the location of files on these networks (as in MP3Board.com). Von Lohmann reminded the audience that no peer-to-peer case has actually made it into court yet and to pay attention to the MGM v. Grokster case expected to come to trial in the Central District of California in October 2002. Summarizing these legal developments, von Lohmann said the status quo "gives veto power to copyright owners over the development of new technologies, while causing a great deal of collateral damage along the way."

Deutsch lambasted the Hollings Bill pending before Congress as an attempt to unravel the safe-harbor provisions (sec. 512) of the Digital Millennium Copyright Act (DMCA).

Sarah Deutsch, Vice President and Associate General Counsel at Verizon Communications, discussed the impact of legal activity brought by content owners on ISPs. Deutsch lambasted the Hollings Bill pending before Congress as an attempt to unravel the safe-harbor provisions (sec. 512) of the Digital Millennium Copyright Act (DMCA) and to undermine the statutory limitations on the liability and enforcement responsibilities of ISPs regarding their customers. Under the proposed bill, ISPs would be forced to purchase a lot of new equipment in order to retrofit their systems to be compliant with the copy protection required. Deutsch also related how the careful procedure of notice and takedown of infringing material has been reduced to a "flogging of notices generated by bots of some content owners" and Verizon's attempts to automate the process of responding to those letters.

Privacy in Times of Cross-Border Security Cooperation

by Abigail Phillips

The tragic events of September 11 supposedly created new incentives to forge international security cooperation agreements. Yet was this day truly a watershed? Or was it simply an excuse to justify and accelerate a movement that had already been underway for several decades? 9/11 may simply have provided an opportune occasion to consolidate macro trends toward world uniformity on a variety of security policies.

Friday's lunch session on international security cooperation and privacy examined these international efforts for convergence of legal and technical standards, especially in light of their dealings with cybercrime and the concomitant declines in individual privacy and recognition of citizens' privacy rights in general.

To showcase the underpinnings of post-9/11 behavior, Simon Davies (the moderator) of Privacy International discussed the gradual erosion of financial privacy that had begun with the Bank Secrecy Act of 1970. The legislation had triggered cooperation on interests between law enforcement and the banking industry. Today, virtually no one retains any secrecy in his or her banking activities. Banks have made as many as 77 million reports of suspicious transactions to the government; yet of those 77 million, the U.S. Treasury has reported only 580 convictions for currency transactions violations. Compounding the problem, Davies states, is the fact that privacy-compromising mechanisms established by the United States are typically quickly replicated around the world.

> Privacy-compromising mechanisms established by the United States are typically quickly replicated around the world.

Gus Hosein of the London School of Economics says that calling the international efforts a movement toward harmonization, or toward convergence of interests and policies, is "too kind." In truth, what often takes place is regulatory arbitrage in the guise of society-friendly goals. During the encryption debate of the mid-90s, he states, we discussed how individuals could use regulatory arbitrage to their advantage; today, however, governments are the typical beneficiaries of regulatory arbitrage, for example choosing a stringent jurisdiction to carry out criminal enforcement.

The Council of Europe's Cybercrime Convention is a significant recent effort at establishing international norms, including a universal definition for cybercrime and assurance that signatory countries have similar statutory allowances – such as interception of Internet communications or collection of real-time traffic data – for investigations. The Convention also provides for cybercrime investigations across international borders, a provision motivated by the ILOVEYOU virus debacle. The treaty, which appeared to have limited support before 9/11, has since been signed by nearly 30 EU member countries, plus the United States and Canada, among others. It is largest mutual assistance treaty ever created relating to crime. Indeed, while its stated focus is cybercrime, in truth it is a vehicle for establishing international powers to deal with *any* crime. As a result, law enforcement officials can opt to pursue a particular crime in the country whose laws are most suited to their needs.

We probably don't have to worry that U.S. courts will enforce judgments by other countries that violate civil liberties enjoyed by U.S. citizens, Anne Beeson of the ACLU reassures. For example, a district court recently held that Yahoo's activities within the United States are not bound by a French court ruling that suppressed First Amendment-protected activity, and the Ninth Circuit is apt to uphold the decision. The problem lies in the chilling effect of such international adjudication – which likely will persist regardless of whether judgments that violate civil liberties can be enforced in the U.S.

Consumer Education and Privacy Protection: Back to Basics

by Jen Elliott

The polls are in: 93% of consumers want privacy policies, and only 29% of consumers trust websites that sell products or services. So why do only 3% of these very same consumers actually review privacy statements most of the time, and why is it that a whopping 60% don't even glance at privacy statements provided to them? The problem may be one of consumer education.

But consumer education about what? Jim Harper, Editor of Privicilla.org, suggests that we first need to come to some consensus as to what issues are encompassed by the term "privacy", and what we mean by privacy rights with relation to the Internet. For example, the term might include everything from general security, to spam, to identity fraud. He would define the term as a subjective condition that exists when one has the legal power to control information about oneself and is able to exercise control over that information in a manner consistent with one's values and interests. Diane Ditzler, a privacy officer from the U.S. Postal Service, thinks that the standard tenets of fair business practice should be included: notice, choice, disclosure, and access. Sarah Andrews, from the Electronic Privacy Information Center (EPIC), also sees privacy as a question of control and autonomy, but emphasizes that the concept of privacy is not necessarily about blocking the sharing of information, but rather about learning about what uses are being made of the information and gaining some control over those uses. Ken McEldowney, Executive Director of Consumer Action, would add that consumers need to know how their information is being combined with other kinds of information, and how best to opt out of (or preferably, opt into) such uses.

> "If you want simple privacy rules, you've come to the wrong planet."
> -- Jim Harper, Privicilla.org

Even granting some agreement on what we mean by privacy,

(Continued on page 4)

Online Activism: Too much of a Good Thing?

by Drew Harris

This Thursday session focused on the experiences of Bay Area online activists.

Some of the panelists proudly demonstrated their activist websites – for example, those of Activist.org and Globalexchange.org. Others discussed the role of technology in organizing the WTO protests in Seattle. The panel even steered briefly into electronic civil disobedience.

However, the panel concluded that perhaps there is *too much* online activism, and that what activists really need to do is to turn off the computer, go outside, and meet face-to-face.

The benefits of organizing activists online are obvious. Websites and email provide cheap communication for organizing activists worldwide, a means which is critical to under-funded groups in developing countries. Panelist Jason Mark of Global Exchange put it succinctly: "If you ever try to call a labor group in Cambodia, you'll find it's a real task. It's much easier to send an email."

Online activism is also convenient. The panelists discussed a successful right-wing activist website named *60-Second Activist Club*. (I tried this website for kicks, and within thirty seconds, I was supporting "a new silver-backed currency.")

But there are plenty of obstacles to making online activism really work. Heather Mansfield, who runs eActivist.org, talked about the obvious logistical problems of financing a website and coordinating volunteers.

A less obvious obstacle is the digital divide. If people don't (or can't) regularly access a computer, online activism simply won't reach them. Even worse, as an audience member noted, many activist sites are basically just "geek portals," not accessible (or comprehensible) to the average websurfer.

Despite the many benefits of online activism, it likely will never replace old-fashioned, "pounding the pavement" approaches.

Ironically, one of the biggest problems is that there is simply too much online activism. Who has time to spend hours in front of a computer, wading through endless information about countless noble causes?

One of the panelists noted a recent *New York Times* article stating that Congressmen pay little or no attention to their constituents' email. Email is too convenient, and politicians receive too much to make any sense of it.

In the end, panelists generally concluded that despite the many benefits of online activism, it likely will never replace old-fashioned, "pounding the pavement" activism. To be truly successful, activism requires real people meeting each other in person. That is how relationships are made and how movements succeed.

Consumer Education *(continued from page 3)*

there's still debate about what measures should be taken to educate the public. Ditzler observed that her office routinely receives questions that demonstrate the general lack of public understanding of basic terms like "cookie" or "session", indicating that any consumer education effort regarding privacy must be couched in language that people can relate to their own experiences. Harper suggested that a standardized information-use label (something along the lines of a nutritional label) would be appropriate. McEldowney thinks that industry should bear the major responsibility for consumer education, but is aware that as of now industry has little commitment, monetary or otherwise, to such efforts – a position Ditzler disagreed with, saying that the Postal Service has made major strides in educating its 760,000 employees in privacy matters. Andrews asserted that there is an inherent conflict of interest in laying education at the feet of industry. McEldowney observed that opt-out instructions such as AT&T's "if you don't want to receive valuable information about our products and services" are hardly a fair presentation of privacy issues and risks.

The panel consensus was that privacy concerns today will last only one generation.

Andrews believes that a better route to consumer protection and education is through government action, though McEldowney is skeptical, saying that while government agencies might claim to want consumer education, few of them are putting money into such an effort. However, the panel agreed that legislation and regulation cannot be the complete answer, because once legislation has passed, consumers need to be sufficiently educated to know the rules are enforced; otherwise, the public will have no more effective privacy rights than they did before. There was also some feeling that such regulations are bound to be complex and difficult for the average person to understand. As Harper stated: "If you want simple privacy rules, you've come to the wrong planet."

In the end, concerns about consumer education on privacy may be temporary. As Fran Maier (TRUSTe) pointed out, her own children already seem to have an excellent grasp of privacy issues on the Internet. The panel consensus was that privacy concerns today will last only one generation, because children understand much better how their personal information may or may not be used, and this understanding will affect uses and their regulation tomorrow.

Ron Plesser on Policy-Making Through Class Action Litigation

by Drew Harris

Ron Plesser (Piper Marbury Rudnick and Wolfe, LLP) is no stranger to CFP, having served on many panels in the past. This year, he served as moderator for Friday's session on "Privacy and Private Litigation." This panel sought to determine, in Plesser's words, whether "class action litigation is an appropriate way to create privacy policy." To Plesser, the answer, probably, is "No."

Plesser has been recognized as one of "Washington's Top High-Tech / Telecommunications Lobbyists" by *Influence* (December 2000), which he attributes to his position as General Counsel of the Privacy Commission in the 1970s, and his work on most of the privacy legislation that Congress has considered in the last 25 years. He works with many companies who are ISPs and content providers.

"FTC litigation is much quicker – private litigation takes years. Also, FTC enforcement can be much quicker." -Ron Plesser

"Some of the important issues facing Congress are the digital rights management issues," notes Plesser. "Some content owners are seeking to have ISPs provide technical means to protect copyright. This could create great network burdens."

He notes as well that "privacy is quickly becoming an important issue again," with both the House and the Senate seriously considering new privacy legislation. According to Plesser, one reason there have been few class certifications in privacy litigation is that many privacy cases have disparate facts, which do not permit class representation.

In the most famous Internet privacy cases – *Doubleclick* and *eToys* – customer complaints had an impact, but the main reason these companies decided to change their policies was the FTC. When asked if, given the difficulty of class certification, he thought that the threat of private litigation would be more effective than the threat of an FTC investigation, Plesser replied: "FTC litigation is much quicker – private litigation takes years. Also, FTC enforcement can be much quicker."

Responding to the question of whether this suggested privacy should be enforced through government regulation rather than private litigation, Plesser declared: "Basically, I think self-regulation has an important role."

The Promise of Privacy Enhancing Technologies

by Nicole Acton

Friday's concurrent session on "The Promise of Privacy Enhancing Technologies (PETs)" focused on three main questions: (1) *Is* there promise? (2) How can we achieve it? (3) What are the major challenges?

Dr. Ian Goldberg of Zero-Knowledge Systems began the discussion by comparing the status of PETs five years ago (like anonymous remailers, Nym servers, DigiCash) with PETs today, concluding that we haven't made much headway. Goldberg sees deployment issues as the major barrier to widespread use of PETs. He therefore recommends that future development of PETs focus on reducing the need for intermediaries in favor of products deployable by a single party.

Naval Research Lab's Paul Syverson discussed cool new PETs like private information retrieval, location protection, safe cookies and "cookie cookers." He stressed the importance of defining what is meant by anonymity and privacy – in other words, developing the underlying theory *before* developing the technology. He concluded with two main points. First, "reputation is not pixie dust," and we need to explore how reputation markets may enable privacy by reducing the need for information. Second, the notion that privacy and security are at odds is a myth – you can't have one without the other.

Lorrie Cranor from AT&T Labs discussed the Platform for Privacy Preferences Project (P3P). After briefly describing how P3P increases transparency (by checking the privacy policy of each website and comparing the policies with the user's pre-selected privacy preferences), she discussed where P3P is today.

Privacy tools are currently solving a problem that most people don't know they have…

Cranor stated that not only is P3P activated by default in Internet Explorer 6, one-third of the top 100 websites have implemented P3P. She also discussed AT&T's Privacy Bird, a plug-in for IE5 and IE6, that utilizes P3P in a simple, non-intrusive manner where the color of the Bird in the bottom of the user's screen indicates how a particular website's privacy policy corresponds with the user's privacy preferences.

Finally, Marc Levine discussed Benetech's Martus project. Martus is Open Source software designed to encrypt data collected by human rights organizations to ensure the data is safeguarded and disseminated. The software was designed with ease-of-use as one of the primary requirements. Levine's demo showed that after merely entering a user name and password, a user can input data and select which portions should be encrypted. The user interface is based on the email metaphor, using a simple, 3-panel screen. The software is scheduled for beta-testing this summer.

The biggest concern raised in the Q&A was how to address the problem of the technology not being used. The success of Martus was compared to the limited use of privacy tools in other arenas. The conclusion seemed to be that PETs are currently solving a problem that most people don't know they have, so educating the public is the key to unlocking the potential of PETs.

CFP Daily2002

CFP Daily2002 is a publication of the CFP2002 Conference with contributions from law students at Boalt and Stanford. We intend to make the content available on the CFP web site after the conference.

The Editors

www.cfp2002.org

THANK YOU to the CFP Daily2002 Editorial Staff!

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 Elliott
Jennifer Urban
Laura Quilter
Lisa Wang
Martha Winnacker
Nicky Ozer
Nicole Acton
Osbaldo Cantu
Sky Canaves
Will DeVries