Friday

April 19, 2002

CFP

Today at a Glance

Jackie Speier @8:30

Public Records @9:30

Digital Commons @11:15

Box Lunch Sessions

Anonymity in Cyberspace @2:00

Closing with Bruce Sterling @3:45

SEE YOU NEXT YEAR!

Lunch with Larry Irving: The Digital Divide is Still Here

By Drew Harris

Larry Irving, the keynote speaker for Thursday's luncheon, spent much of his keynote speech addressing two myths. First, that the nation has already fixed the Digital Divide. Second, that even if there still is a divide, market forces by themselves will take care of it.

Irving forcefully presented compelling statistics: 60% of African Americans and 70% of Hispanics have no access to the Internet. The disparity is worst in rural areas with high minority concentrations.

Exemplifying the Digital Divide was the composition of the CFP luncheon audience, of whom only five or six were African American.

Some in the current administration say that while there *was* a problem, now libraries and schools are all wired, so the problem is solved. Irving calls this the "Declare victory and go home" approach. "It's one thing to say that the market should fix the problem, but another thing to say that the Digital Divide doesn't exist anymore," chided Irving.

To those who say market forces will fix a problem if one exists, Irving counters that within the black and Hispanic communities lies a huge, untapped online market, but that the market has failed to recognize it and get these groups online. His personal experience attests to this: He and Magic Johnson started a private partnership to encourage high-tech investment aimed at urban communities; that, he mournfully jokes, was yet another failed dot-com.

The Digital Divide indeed persists.

* * *

The second half of the keynote focused on Irving's other two big concerns: privacy, and the growing media oligopolies.

On privacy, in the "age of convenience," consumer protection and good business sense require us to establish effective privacy policies.

On media concentration, companies like AOL Time Warner and Disney own not only the content, but also the means of distribution – a cause for grave concern.

(Ironically, this was an AOL-sponsored luncheon.)

The Big Brother Awards : The "Winners" Are . . .

By Nicole Acton

An enthusiastic crowd gathered Thursday evening to recognize the work of companies and individuals who in 2002 are still striving to achieve 1984.

The first award of the evening went to the **Most Heinous Project**. Nominees were:

- The American Association of Motor Vehicles Administration's National Motor Vehicle ID Card project;
- The Washington DC Video Surveillance System, referred to as "Tourism in a Fish Bowl"; and
- And the "winner"… **Enhanced CAAPS** (Computer Assisted Passenger Pre-screening System), the brainchild of Acxiom, hnc, Equifax, and Accenture.

In the **Worst Government Official or Agency** category, the nominees were:

- Department of Health and Human Services Secretary Tommy Thompson, for his efforts to weaken medical privacy
- California Governor Grey Davis who has repeatedly vetoed workplace and financial privacy bills
- And the "winner"… **U.S. Attorney General John Ashcroft**, for obvious reasons, most notably the USA Patriot Act.

In the **Worst Corporate Invaders** category, the nominees were:

- Qwest, for weakening the concept of consent
- FSCC (Financial Services Coordinating Council)
- And the "winner"… **Oracle CEO Larry Ellison** who foretells of his company running the one global database with all of our info

Finally, the **Lifetime Menace** award nominees included:

- Booz Allen Hamilton for developing "surveillance toys"
- "The Susan Lucci of the Privacy Awards", i.e. the Direct Marketing Association
- And the "winner"… **Admiral John Poindexter** whose resume includes past feats like document shredding during Iran / Contra and the NSDD-145, and who currently runs the Information Awareness Office and Project Genoa.

On a positive note, three Brandeis Awards were given to Champions of Privacy. These real winners included California Senator Jackie Speier for her tireless work on California's financial privacy bill, the "persistent, perceptive, patriotic, privacy pest" Warren Leech, and the San Francisco Chronicle Editorial Page for their relentless coverage of financial privacy legislation in California. Keep up the good work!

Statistics and Slobodan

by Abigail Phillips

"Being an effective advocate for human rights," says Patrick Ball, "often means being able to understand mass phenomena and the data that underlie them."

Since 1999, Ball has used computers and number-crunching software to study atrocities in Albania during the war in Eastern Europe. In the trial of Slobodan Milosevic, Ball testified about his findings from studies of refugee flow and mass killings data. Yugoslav researchers from the region had posited several possible reasons for peak-and-valley patterns in both sets of data: Kosovo Liberation Army activity, which drove Kosovars from their homes; NATO air attacks; or the Yugoslav government's campaign to force out Albanians.

Examining the available numbers, Ball saw a pattern — which held true over variations in place as well as time — emerge between numbers of people abandoning their homes and numbers of people being killed. Deviations in the two lines of data seemed to occur virtually simultaneously and at similar intervals, suggesting a related causal factor underlying both phenomena.

A correlation of Yugoslav government actions with migration and killing patterns is inarguable.

Ball considered the NATO and KLA hypotheses but concluded that neither was supported by the numbers. When compared to the refugee flow and killings patterns, NATO and KLA activity seemed to have little temporal or regional correlation with periods of pronounced refugee flow and high killing rates.

Ball did, however, find that the statistical evidence was consistent with the premise that periods of heavy refugee flow and killing were in some fashion tied to activities of the Yugoslav government — suggesting that Yugoslav forces conducted a systematic campaign of expulsions and killings. While Ball had little data on the Yugoslav government to work from, he did have an especially salient case of government activity to point to: On April 6, 1999, the Yugoslav government declared that it would halt operations for a period in honor of the Orthodox Easter. Shown over time, the numbers for refugee flow and killings decline dramatically from this date until several days thereafter. After the time that Yugoslav forces resumed their actions, the numbers creep back up.

The correlation of Yugoslav government actions with migration and killing patterns is inarguable. Although causality may be hard to show — and indeed, Ball does not purport to show any relationship beyond the correlative one — the implications of the comparisons are intriguingly suggestive.

Australian Case to Probe Whose Law Applies to Web-Publishers

By Roger Clarke

The *Gutnick v. Dow Jones* case is listed for hearing in the High Court of Australia on Tuesday, 28 May 2002. The question to be determined is the critical issue of "in which jurisdiction(s) is a web-publisher answerable?"

The eventual finding by Australia's highest Court would likely have influence in many other superior courts around the world, and maybe even in the USA, particularly since it might be the first judgment on this specific question by any superior court anywhere.

The Supreme Court of Victoria found that the determination depended not merely on the jurisdiction in which the server was situated (NJ), or the jurisdiction in which the uploading was done (NY), but (in essence) on the jurisdiction(s) in which it was downloaded (in this case, many, but Victoria was found to be a tenable and convenient choice).

On that reasoning, everything anyone is responsible for publishing on a web-page is arguably actionable in any of the (approx. 300?) relevant jurisdictions in the world (i.e. each U.S. and Australian State, Canadian province, Malaysia, PRC, etc.).

CFP Advisory Board Member Roger Clarke is an independent consultant in e-business strategy and policy, and a Visiting Fellow in the Department of Computer Science at the Australian National University in Canberra, Australia. Clarke's notes arising from the expert evidence he provided regarding this and the Macquarie Bank v. Berg *case may be found at: www.anu.edu.au/people/Roger.Clarke/II/DefWeb01.html.*

Meet Kim Alexander, Conference Panelist on Public Records

by Ekta Shalu Narula and Catherine Atz

The California Voter Foundation (CVF) is conducting a nationwide, state-by-state survey on present and potential privacy implications of the use of voter registration data. Kim Alexander, Founder and President of the CVF, hopes that this project will better inform public policy discussions about voter registration information and privacy in the digital age. In addition, she hopes to educate the public about how their personal data is currently being used.

Alexander will highlight the secondary uses of personal data not widely known to the general public. She surmises that many people will forfeit their right to vote in effort to protect their privacy when they learn about the uses of their personal information. "The system that exists now seems to presume that voters will be ignorant about what happens with their data. Accordingly, there is a real need for the government to be upfront about what information will be used and what information will truly be kept confidential."

In addressing these concerns, CVF will make a series of recommendations, which will include a ban on all commercial use of voter registration data as well as a requirement that the registration forms give voters the option to suppress their personal information.

Kim Alexander will serve as a Panelist for Plenary Session #9: "How Public Is Too Public? – Public Records and Personal Privacy", Friday, April 19, 9:30-10:45am.

Privacy: Experts Spar Over Merits Of Industry's Web-Based Services

By *Drew Clark*

SAN FRANCISCO -- Privacy advocates want to make Web-based services the next major battleground for Internet privacy, but businesses running the services said Thursday that because they are sold on the concept of privacy, consumers do not have to fear abuses.

Although still an amorphous and evolving concept, Web services such as Microsoft's .Net and the Liberty Alliance -- a group of dozens of companies spearheaded by Sun Microsystems -- have been much disputed in technology-standards bodies and interjected into the antitrust case against Microsoft. Both Microsoft and Sun have attempted to impugn the others' credentials to safeguard the detailed personal information that such services require.

After mentioning disparaging comments about consumers' right to privacy made by Sun CEO Scott McNealy and Oracle CEO Larry Ellison in a panel discussion, Microsoft Vice President of .Net services Brian Arbogast said, "I fundamentally disagree with that view of the world." Web services like .Net present a "tremendous opportunity for technology to roll back the clock" on the losses to privacy caused by technology and to grant consumers more control over how their personal information is used, Arbogast said at the Computers, Freedom and Privacy conference here. He also said Microsoft had dropped its "opt out" policy and adopted an "opt in" approach with Passport, meaning that no customer data would be shared without affirmative customer consent. Jason Catlett, president of Junkbusters and a vocal privacy advocate, did not buy that argument and compared Microsoft's Passport -- its first major Web service and the backbone of its still-developing .Net initiative -- to those issued by government. A key element of Passport is that it assembles an array of personal information on Microsoft Web servers that can be accessed in order for third parties to offer location-based services to Microsoft customers. "Privacy advocates don't like deep databases with historical data of personal information when governments seek to impose them," Catlett said, referencing previous criticisms of national identity cards made at the conference. "We don't like them when abusive monopolists seek to impose them, and we don't like them when an oligopoly seeks to impose them." Avi Rubin , a researcher at AT&T labs, concurred in part with Catlett's criticisms. "I think the Passport concept is the enemy of privacy. Even if it is opt in, it is a bad idea" because it centralizes large amounts of data in one location and becomes a tempting prize for hackers. He described a world of two scenarios for Web service, one of which was based on anonymity while the other was premised on business keeping track of all personal information. Some services -- like finding a hotel reservation at the next stop for a driver cruising the highway -- require more information, but that does not mean system architects should avoid building privacy into their systems.

"You cannot build a system and suddenly add privacy features without having to trust" the bona fides of a company like Microsoft or Sun. "Privacy-preserving services are inherently more expensive to build, have inherently fewer features, and will always meet resistance from vendors. The incentives are all in the wrong direction" unless the "the masses [can be] educated about the dangers of privacy-invading technologies."

"Privacy-preserving services are inherently more expensive to build, have inherently fewer features, will always meet resistance from vendors."
-- Avi Rubin, AT&T labs

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

More on the Location Services Panel

by Osbaldo Cantu

"I'm not a target!"

As mobile web-enabled and other wireless-ready devices offer convenient services to users, the protection and use of personally identifiable information becomes a greater concern. Potential services provided by cell phones, PDAs, the Internet, 802.11 networks, and highway tolls may offer convenience to users, but what happens to the user's data once it is out of the control of the user? Who has ownership and control of the data? Can users trust the entities that will handle such sensitive information?

One approach to these questions is to say if a user is concerned with the privacy implications of technology, "don't use it." These potential services are designed to maximize service to users. Privacy preserving services are expensive, and vendors won't want to spend more money for privacy.

In today's panel discussion, Avi Rubin, of AT&T, suggested a Catch 22: If scientists don't build in privacy protections up front, the opportunity is pretty much lost; however, consumer reaction is required for companies to spend the money to respect privacy, and there won't be this outcry until the privacy-lacking technology is out. Rogger Cochetti, VP of Global Policy for Verisign, pointed to the difficulty companies face, as exhibited in the Commerce Department requiring Verisign to make some database information, acquired in the merger with Network Solutions, available for sale. Microsoft representative Brian Arbogast stated that his company can afford to follow good business sense: "respect what the users want, and never make decisions based on short term profits." To achieve long-term profits, consumer trust is a must. Hence, protecting and securing consumer data is a priority. Jason Catlett of Junkbusters wouldn't buy any of it.

How to Hack an Election

By Jennifer Elliott

Prompted by public outrage over the resolution of the most recent presidential election, there has been a call for reform in the way elections are conducted from a technical standpoint. Congress is currently considering legislation to reform election systems, particularly the Help America Vote Act of 2001 (H.R. 3295) (recently amended to include the text of the Equal Protection of Voting Rights Act of 2001 (S. 565)).

If the goal is to design a system in which you can believe that your vote as cast is identical to your vote as counted, what kind of system would that be? The panelists were divided on this issue, particularly over the necessity of a paper record of an electronic vote. Peter Neumann observed that the systems in use at the moment have "weakness in depth" -- every part of the process is currently a weak link. He underscored the importance of verifiability, and observed that simply having the code be open source in a voting machine system by no means assures that the system will be either more reliable or more secure; it merely affords more opportunity for scrutiny. Andy Neff (Votehere) maintained that transparency of the code itself is critical to understanding how the machine may be subverted; simply being able to tally the registered votes yourself offers little confidence that the registered votes were legitimate to begin with. Keeping in mind that any individual device may be suspect, Neff proposed that a set of very strict standards be developed against which any voting machinery may be measured.

If the goal is to design a system in which you can believe that your vote as cast is identical to your vote as counted, what kind of system would that be? .

Ernie Hawkins, the Sacramento County Registrar of Voters, recalled that elections in the U.S. are largely governed by state law, leading to wide variances in practices. Such differences in turn make it difficult to produce machinery and software that will work in more than one state, let alone all fifty, says Joe Taggard (Election Systems and Software). Furthermore, each jurisdiction will effectively be making its own independent decision about which new election technology to implement, in turn fostering corruption and the use of inferior systems if local election officials have ties to the manufacturers of the new equipment.

The DMCA and Me??

By Laura Quilter

The DMCA panel launched with a highly amusing skit and finished with a lively debate between panelists and audience.

The skit starred Ed Felten as Our Hero, Fred Elten, a computer science graduate student in a Skylarov situation, arrested on the conference floor givng a talk. Bill Keane played himself as an Assistant US Attorney, pondering the difficulties of the case and explaining ISPs to his supervisor; Daralyn Durie played the defense attorney, arguing that Elten's work should be protected by the First Amendment; Lance Hoffman played the anxiety-stricken conference organizer, concerned with his own liability; and Dan Gillmor played a reporting ace trying to get a scoop. The scenario ended up with Our Hero out on bail and swearing off research and the United States…

Barbara Simons (ACM) moderated a lively follow-up panel arguing about the promises and the pitfalls of the DMCA. Ed Felten (Princeton University, computer scientist) contrasted his real-world experience with the DMCA with his counterpart's in the skit, observing that although he was not prosecuted under the criminal charges, the civil penalties which could have cost him his home were nonetheless a very big deal, and cast a real shadow and chill on speech and research. Robin Gross (EFF, attorney) reminded us that fair use is the breathing space between the First Amendment and copyright law, and that while the DMCA addresses the tools and not the use, it may be impossible to make the uses without the tools. As an exclamation point to the skit, Gross also noted that post-Skylarov, the nation of Russia has issued a travel advisory about the dangers of traveling to the USA. "What we're seeing is a world in which copyright holders want all of the benefits of copyright law, but none of the responsibilities like making sure that works fall into the public domain," she said. "EFF's position is that the DMCA needs to be repealed to restore the balance to copyright law."

Fair use is the breathing space between the First Amendment and copyright law.

Allan Adler (Association of American Publishers) was stalwart in holding up the pro-DMCA side. Reminding the audience that the various copyright industries are not fungible and have different industries, he argued that the DMCA's anti-circumvention provisions served a useful purpose in helping copyright-holders enter new markets. Adler further argued that fair use was irrelevant, because the DMCA prohibitions did not affect fair use, and that furthermore, no specific use could ever be considered fair by definition. Adler then stated that the number of cases was limited, and he discounted the idea that the statute created any chilling effect, apart from people's misunderstanding of the statute.

Jessica Litman (Wayne State University, law professor) pointed out that many copyright lawyers consider the Sony Betamax decision to have been wrong and see the DMCA as an attempt to revise Sony — but that the motion picture industry should be very happy that they lost Sony, since the industry has profited so greatly from the home video industry. Litman also contradicted Adler's contention that any chilling effect was merely a result of confusion: although copyright-owners argued during lobbying that the DMCA was narrowly tailored, since the law was passed, they have pushed a broader interpretation and have been "extraordinarily aggressive," suing not pirates, but scientists and the journalists who write about them.

Open Source, Standards, and Aristotle

By Jennifer Urban

A surprise guest, Janet Daly of the World Wide Web Consortium, kicked off the standards discussion for the Open Source session with a short history of the W3C's patent policy working group. As the working group was formed in response to the threat of a patent infringement lawsuit over W3C's P3P standard, and as it has been criticized for a draft policy that included the possibility of including standards that would require obtaining RAND patent licenses, her story set the stage for a discussion of standards for the Internet.

The question posed by Erwin J. Basinski, Of Counsel at Morrison and Forrester and an expert on software patents, was how to create useful and open standards in a world where the participants' incentives and values can vary greatly. After a description of the divergent interests represented, Basinski concluded that a starting point might be to get players from diverse interests and backgrounds (companies with revenue streams that are dependent on patent license revenues, companies which depend on selling software or hardware and folks in the open source community) to come to the table to help Congress or the FTC create a "standard for standards bodies" that encourages participation and disclosure.

Brian Behlendorf of CollabNet (and Apache fame) first pointed out that the open source community and "standards" need one another in the software arena. DNS, HTTP and other protocols relied on by the Internet depend on "standardization" of some type, whether or not it goes by that name. Behlendorf questioned the advisability of standards covered by patents, pointing out that "reasonable and non-discriminatory" is difficult to define in a useful way, and that requiring royalties substantially increases the transaction costs of creation. For this reason, Behlendorf wonders why we should be concerned about patented standards, as they will always lose out to open standards that are easier to implement, even if the patented standards seem to provide "better" functionality.

> "The open source model is a set of beliefs, not a set of licenses."
> -- Tim O'Reily

Tim O'Reilly (appropriately) gave a literary note to the discussion, quoting Aristotle's assertion that "a plausible impossibility is better than an implausible possibility." Thus, what people believe to be true becomes true as they act on their beliefs. The openness of the Web is a good example of this statement because developers, acting on a belief of openness, copied each other's HTML code without knowing what the licensing terms might really have been. The open source model, asserted O'Reilly, "is a set of beliefs, not a set of licenses" that is driven by an "architecture of participation" resulting from low "transaction costs." Explosions in creativity have occurred, therefore, when standards were "open enough" even if not entirely open—e.g., IBM opened up some aspects of its system standard but not others, and the PC market exploded. O'Reilly called upon both the open source community and IP rightsholders to avoid a situation where the transaction costs of participation in building standards become so high that we "lose the power of collaborative development that we've seen in the past."

As moderator John Morris of the CDT pointed out, these questions are particularly timely—the W3C should finalize its policy in the next 6 or 7 months; the IETF may be instituting a patent policy working group soon. Now is the time to weigh in. The present draft from the W3C working group is available at www.w3.org.

Ian Goldberg on the Future of Privacy Technology

By Abigail Phillips

Five years ago, Ian Goldberg, Chief Scientist for Zero-Knowledge Systems, was predicting a rosier future for privacy-enhancing technologies than he sees today. At the end of the '90s, he says, "we were optimistic about where things would be today." Anonymous remailers seemed on the way to becoming commonplace, and encryption of email was increasingly pervasive. It was assumed by many in the industry that by 2002 everyday use of privacy enhancing technologies such as anonymization and encryption would be the norm.

> ***Adequate privacy tools for the average web surfer exists… the problem is deploying them.***

maintains, is not the lack of technologies. Adequate privacy tools for the average web surfer exist. Rather, the problem lies in deployment of these privacy-enhancing technologies. The hurdles often consist of "getting people to cooperate" in building and maintaining the systems — such as networks that route browser requests through intermediate nodes for anonymous web surfing — which makes certain privacy enhancing behaviors possible. Moreover, employing the systems can be prohibitively expensive and administratively complicated. Goldberg suggests that a peer-to-peer model may be better suited to anonymous browsing, and foresees some developments moving in this direction.

A Familiar Confrontation on the Future of IP

By Martha Winnaker

Moderated by Drew Clark, a reporter from Tech Daily,, the session entitled "The Future of Intellectual Property" was cast as a formal debate between John Perry Barlow and Steve Metalitz, Senior Vice President of the International Intellectual Property Alliance. The proposition: "Resolved: Intellectual property law constrains the development of new technologies." Comments were provided by Greg Wren, Deputy General Counsel International for Yahoo, and Karen Coyle, a California Digital Library librarian. Although Clark described the debate as encompassing the entire set of intellectual property laws, participants focused on the implications of legally reinforced technological protections for copyrighted work.

Barlow challenged the concept of "intellectual property," arguing that the law gives creators temporary monopoly licenses rather than property rights and that ideas cannot be treated as tangible commodities. He prophesied that the copyright industries' proliferating ownership claims would transform a growing "rain forest" of shared ideas into an "arid desert" where industry wields thought control.

Metalitz argued that law constrains technology for public policy reasons. He listed three reasons for strengthening copyright: the contribution of the copyright industries to the economy, the requirements of international treaties, and incentives for creativity and innovation. He pointed to an upsurge in innovation in digital rights management technology research since passage of the DMCA.

Barlow prophesied that copyright industries' proliferating ownership claims would transform a growing "rain forest" of shared ideas into an "arid desert."

Barlow proposed that copyright owners choose between legal and technological protections for individual works. Metalitz rejected such a "Hobson's choice."

Commentator Greg Wren noted the challenge of promoting exceptions to owner's rights for fair use in the face of large amounts of abusive taking without payment. Karen Coyle noted concerns that works protected by technology will be lost if the technology fails and predicted a possible "electronic dark age" if fair use concerns are not accommodated by new technologies. She also called for a political process that involves all members of the public, not just the proponents of major industry sectors.

A Chat with Mark Eckenwiler of the DOJ

By Sky Canaves

Mark Eckenwiler has been coming to CFP since 1995, when he was still in private practice. Today Eckenwiler is Senior Counsel in the Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice.

Eckenwiler says changes in technology have brought changes in the way people communicate, and so have necessitated new methods of investigation by law enforcement officials. Longstanding law enforcement principles in telecommunications thus should be extended to encompass Internet communications.

Commenting on the controversial topic of pen register/trap and trace, in Eckenwiler's view, the Patriot Act does not provide new capabilities for law enforcement officials, but rather codifies pre-existing practices in what may ultimately prove to be a more privacy-protective manner. In addition to establishing compulsory procedures that the government must obey in its investigations, the statute also protects individuals from unauthorized incursions into the privacy of their communications by affirming that regulations protecting the privacy of phone communications also apply in the online context.

With regard to Carnivore, Eckenwiler believes that it's perceived problems have been over-hyped. "Carnivore is just a packet sniffer, but more refined, and private networks use packet sniffers all the time," Eckenwiler says. "Ninety-nine percent of the problem with Carnivore." To Eckenwiler, it is important to emphasize that DCS1000 (as he prefers to call it) never needs to be used when the service provider is willing to collect data. "The DCS1000 approach is privacy enhancing in cases where the provider doesn't want to collect information," he said, since Patriot includes reporting requirements for additional court oversight when DCS1000 is used. "Talking about the lack of accountability and oversight ignores other parts of the Act, including its many safeguards" he concluded.

"People at CFP are the greatest experts and the toughest critics" -- Mark Eckenwiler.

Eckenwiler says that a great advantage of his current job is that it allows him to "be an advocate for privacy within law enforcement," educating his colleagues in the Department on what they can and cannot do in the course of investigations and prosecutions.

When asked what he likes most about CFP, Eckenwiler responded "all the contending viewpoints representing academia, industry, law enforcement, and even librarians." "People at CFP are always the most informed, most engaged in the problems," and they are also "viewpoint ecumenical—people are generally respectful of viewpoints, even when they violently disagree." Though the technology may change and the policy debates may change he commented "it doesn't get old which is why people return year after year—it's where the cluefu people are. People at CFP are the greatest experts and toughest critics."

Prognosis for Use of Health, Medial, and Genetic Information

by Jennifer Elliott

Let's say you go to the doctor for a checkup, you have some lab work done, and maybe you stop by the pharmacy to pick up a prescription for that embarrassing rash you've had for a while. Nothing particularly out of the ordinary, but you suddenly start getting mail at home from pharmaceutical companies advertising a variety of anti-fungal medications. Worse yet, a visit to a therapist for alcohol counseling is soon followed by an increase in car insurance rates. Trivial or serious, these scenarios amount to the same thing: Your private medical information has been released without your authorization. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was designed to prevent such situations.

As Ohio State Law Professor Peter Swire observed, Congress saw that the time was ripe for establishing standards for an electronic privacy and security system, since the health care industry has been in the midst of a major shift from paper to electronic patient records.

Mary Henderson of Kaiser Permanente Health Plan discussed how the health care industry is generally supportive of the new regulations imposed by HIPAA, and there is even some sentiment that the standardization of privacy will result in cost savings for the industry. She added, though, that the industry saw the written consent requirement as a barrier to many patient services such as online and telephone advice, pharmacy refills, and even making appointments. She also argued that patients failing to sign a consent form would be unable to take advantage of emergency notification programs that the provider could offer, and cited Kaiser's contacting of patients who may have been exposed to anthrax last fall as an example.

Readily available medical information is taking a giant leap forward with the advent of genomics and proteomics. Soon it may be possible or even routine to have a complete genetic profile be part of your standard medical file. Dr. Gregory Fowler, Executive Director, Geneforum, and Clinical Associate Professor of Public Health, Oregon Health Sciences University, commented that this information reveals a tremendous amount not only about the person it comes from, but also about that person's parents and children and even grandchildren. According to Fowler, there are over 300 million samples of blood, sperm and tissue already present in labs around the country, growing at the rate of 20 million samples per year. It's possible to extract genetic information from these samples – information that the donors may not even realize exists. Fowler's Geneforum is dedicated to educating and engaging the public and legislators on genetic privacy issues.

In the heath care industry there is even some sentiment that the standardization of privacy will result in cost savings.

Although the HIPAA privacy provisions go into effect next year, there are signs that the Bush administration intends to make a number of changes that may significantly alter privacy rights. Among other changes, a modification of the regulations to eliminate the requirement for signed consent was proposed several weeks ago. Stay tuned at http://www.hhs.gov/ocr/hipaa/.

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.com

Corrections….

The Thursday edition of CFP Daily2002 experienced some formatting problems at the printer. This problem shifted the lead story and hid the name of the author, Mary Rundle.

In the PATRIOT and Privacy article regarding comments by Chris Painter of the DOJ, the statement about URLs should read "asserting that the FBI does not now use pen/trap devices to capture URL information."

Best-Selling Books at the Stacey's Table this Week:

- **James Bamford,**
  PUZZLE PALACE: AREPORT ON AMERICA'S MOST SECRET AGENCY
- **James Bamford,**
  BODY OF SECRETS
- **Larry Lessig,**
  CODE AND OTHER LAWS OF CYBERSPACE
- **Larry Lessig,**
  FUTURE OF IDEAS
- **Cady, Glee & MacGregor,**
  PROTECT YOUR DIGITAL PRIVACY
- **Jessica Litman,**
  DIGITAL COPYRIGHT: PROTECTING INTELLECTUAL PROPERTY ON THE INTERNET
- **Peter Swire,**
  NONE OF YOUR BUSINESS