ELECTRONIC PRIVACY INFORMATION CENTER

==========
E P I C A l e r t
==========
Volume 11.03 February 11, 2004

Published by the
Electronic Privacy Information Center (EPIC)
Washington, D.C.

http://www.epic.org/alert/EPIC_Alert_11.03.html

==========
Table of Contents
==========

[1] EPIC FOIA Docs Show Acxiom Was Considered as TIA Data Source
[2] Pentagon Cancels Internet Voting Project
[3] FBI Asks FCC to Delay Discussion of Internet Phone Rules
[4] DHS Deputy Secretary Questioned About Passenger Profiling
[5] EPIC and PI Open Nominations for Brandeis, Big Brother Awards
[6] News in Brief
[7] EPIC Bookstore: Protecting America's Health
[8] Upcoming Conferences and Events

==========
[1] EPIC FOIA Docs Show Acxiom Was Considered as TIA Data Source
==========

EPIC has obtained a document under the Freedom of Information Act containing internal communications among Defense Advanced Research Project Agency (DARPA) employees considering data broker Acxiom as a supplier of personal information for the Total Information Awareness (TIA) program. In an e-mail dated May 21, 2002 to TIA developers John Poindexter and Robert Popp, a DARPA employee writes that "Acxiom is the nation's largest commercial data warehouse company ($1B/year) with customers like Citibank, Walmart, and other companies whose names you know. They have a history of treating privacy issues fairly and they don't advertise at all. As a result they haven't been hurt as much as ChoicePoint, Seisint, etc by privacy concerns and press inquiries."

The e-mail claims that Jennifer Barrett, Acxiom's Chief Privacy Officer, provided recommendations that would help quell public scrutiny of the transfer of data from the company to the government: "One of the key suggestions she made is that people will object to Big Brother, wide-coverage databases, but they don't object to use of relevant data for specific purposes that we can all agree on. Rather than getting all the data for any purpose, we should start with the goal, tracking terrorists to avoid attacks, and then identify the data needed (although we can't define all of this, we can say that our templates and models of terrorists are good places to start). Already, this guidance has shaped my thinking."

The employee continues: "Ultimately, the US may need huge databases of commercial transactions that cover the world or certain areas outside the US. This information provides economic utility, and thus provides two reasons why foreign countries would be interested.

Acxiom could build this mega-scale database."

In response, Robert Popp asked the employee about estimated costs associated with having Acxiom participate in the "TIA critical experiment," and for the company's assistance in helping Rand "identify all the relevant databases."

DARPA E-mail Obtained by EPIC under the Freedom of Information Act:

http://www.epic.org/privacy/profiling/tia/darpaacxiom.pdf

For more information about TIA, see the EPIC Total Information Awareness Page:

http://www.epic.org/privacy/profiling/tia/

For more information about consumer profiling, see the EPIC Consumer Profiling Page:

http://www.epic.org/privacy/profiling/

==========

[2] Pentagon Cancels Internet Voting Project

==========

Citing security concerns, the Pentagon has cancelled an Internet voting project designed to let military and other personnel overseas vote in the 2004 local and general elections. The Defense Department decided not to implement the program "in view of the inability to ensure legitimacy of votes, thereby bringing into doubt the integrity of the election[.]"

The Pentagon decision to abandon SERVE came two weeks after the release of a security review that recommended cancellation of the program because of numerous security risks. The report, authored by a panel of computer science experts, found the system vulnerable to hacking, noted the lack of a paper audit, and pointed out the danger to election data's validity. The report concluded that the security weaknesses inherent in voting over an Internet-based system were "fundamental," and fixing those weaknesses would require a redesign of the Internet itself. Because these security risks could not be mitigated, the computer security experts recommended the cancellation of the SERVE program.

In other electronic voting news, EPIC obtained an independent security and verification audit of Diebold voting machines commissioned by the Maryland Legislature. The legislative report agreed with an earlier independent study of Diebold e-voting machines by Computer Security expert Dr. Avi Rubin, at Johns Hopkins. Like the Rubin study, the legislative report found numerous security vulnerabilities in the Diebold system. The report also found that the Diebold system failed to incorporate strategies to counter component failure, or any system failure.

The SERVE Security Analysis Report:

http://www.servesecurityreport.org/

The Maryland Legislature Study of Diebold Voting Machines:

http://www.epic.org/privacy/voting/mdvote1.04.pdf

http://www.epic.org/privacy/voting/mdvote1.04app.pdf (appendix)

Dr. Avi Rubin's Study of Diebold Voting Machines:

http://avirubin.com/vote.pdf

Verified Voting Coalition:

http://www.verifiedvoting.com

For more information on electronic voting, see EPIC's Voting Page:

http://www.epic.org/privacy/voting/

==========

[3] FBI Asks FCC to Delay Discussion of Internet Phone Rules

==========

The Federal Bureau of Investigation (FBI) recently sent a letter to the Federal Communications Commission (FCC) asking the FCC to put off any discussion concerning the regulation of Voice over Internet Protocol (VoIP). VoIP is a technology that allows Internet users to make phone calls over high-speed Internet connections. The FBI, along with the Department of Justice (DOJ) and Drug Enforcement Agency (DEA), want to delay the discussion until the FCC addresses how VoIP communications can be monitored by law enforcement.

At the center of the debate is the 1994 Communications Assistance to Law Enforcement Act (CALEA). CALEA requires telecommunications service providers to provide wiretapping access to law enforcement. However, VoIP is currently an information service rather than a telecommunications service and is therefore not subject to CALEA. The DOJ, FBI and DEA (DEA) are petitioning the FCC to regulate Internet telephony in such a way that CALEA can be legally and technically applied. VoIP providers would have to rewire their networks to government specifications so that law enforcement officials could more easily listen in on VoIP calls. The FCC remains hesitant to regulate the technology.

In December, EPIC sent a letter to the FCC urging the agency to adopt privacy protections for VoIP. The letter states, "EPIC maintains our strong reservations regarding the application of the Communications Assistance to Law Enforcement Act (CALEA) requirements to this service. It is simply not coherent to argue that VoIP services should be free of government regulation and then for the government to require that communication service providers, hardware manufacturers, and network developers incorporate the most extreme communications surveillance requirements of the Federal Bureau of Investigation. Communications technologies like VoIP should be designed for precisely what they are intended for: to enable communication between people, not to allow surveillance on private citizens."

According to FCC spokesman Michael Balmoris, the agency has decided to press on with its review of VoIP this week despite the FBI's request. The FCC is holding an open meeting Thursday, February 12, 2004 to consider VoIP and related issues. The meeting is scheduled for 9:30 a.m. in Room TW-C305 at 445 12th Street SW, Washington, D.C.

Audio/video coverage of the meeting will be broadcast live over the Internet from the FCC's Audio/Video Events web page at:

http://www.fcc.gov/realaudio

The FCC's VoIP Page:

http://www.fcc.gov/voip

EPIC's letter to the FCC:

http://www.epic.org/privacy/voip/fccltr12.15.03.html

For more information on Voice over Internet Protocol, see EPIC's VoIP Page:

http://www.epic.org/privacy/voip/

==========

[4] DHS Deputy Secretary Questioned About Passenger Profiling

==========

Department of Homeland Security Deputy Secretary Admiral James Loy encountered skepticism about the controversial Computer Assisted Passenger Prescreening System (CAPPS II) program when he recently testified before the National Commission of Terrorist Attacks Upon the United States (9-11 Commission). The 9-11 Commission is an independent, bipartisan panel chartered by Congress and President Bush to investigate and report on the circumstances surrounding the September 11, 2001 terrorist attacks, and make recommendations on how to prevent such attacks in the future.

After Admiral Loy testified on developments in transportation security since the 9-11 attacks, Commissioner Fred F. Fielding asserted that the expansion of CAPPS II from an aviation security measure to a law enforcement tool demonstrated "classic mission creep." Admiral Loy resisted the characterization of the program, but stated that CAPPS II "should be as pristine as we can make it, focused on exactly what we want to use it for." In response to further questioning from Commissioner Fielding, Admiral Loy conceded that CAPPS II is "gameable," and noted that the system as currently designed would label approximately 14.5 percent of air travellers "selectees" subject to, at a minimum, secondary screening.

Today the Associated Press reported that a General Accounting Office report on CAPPS II commissioned by Congress and scheduled for release on February 13 states that the Transportation Security Administration has not adequately addressed privacy and security concerns presented by the program. The findings of the report will weaken Congressional support for CAPPS II and throw the program's future into doubt.

In related news, The Article 29 Working Party (WP29) has released its opinion on the December 16, 2003 agreement between the Department of Homeland Security and the European Commission (EC) on the disclosure of passenger data between the European Union (EU) and the United States. The opinion concluded that the agreement is inadequate under EU data protection laws.

The WP29 opinion recommends: 1) restricting the purpose of the disclosure to the fight against terrorism, 2) implementing shorter and more proportionate data retention periods, 3) not using data for implementing and/or testing CAPPS II or similar systems, 4) providing passengers with access to an independent redress mechanism, 5) making the agreement fully binding on the United States, and 6) strictly limiting further disclosures of passenger data to other government or foreign authorities. The WP29 opinion, though not binding on the EC, may have an impact on Members of the European Parliament when they vote in March on whether to adopt the EC's decision of adequacy, as well as on EU Member State data protection authorities in their

decisions to pursue complaints by passengers for breach of EU privacy laws by airline companies.

Article 29 Working Party Opinion 2/2004 (WP 87) on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States Bureau of Customs and Border Protection:

http://www.epic.org/redirect/opinion_22004.html

European Commission's Communication to the Council and Parliament on the Transfer of Air Passenger Name Record Data:

http://www.epic.org/redirect/pnr.html

For more information on the transfer of passenger information between the European Union and United States, see EPIC's EU-US Airline Passenger Data Page:

http://www.epic.org/privacy/intl/passenger_data.html

For more information about CAPPS II, see EPIC's Passenger Profiling Page:

http://www.epic.org/privacy/airtravel/profiling.html

[5] EPIC and PI Open Nominations for Brandeis, Big Brother Awards

In April 2004, EPIC and Privacy International (PI) will hold the sixth U.S. "Big Brother Awards" to name and shame the public and private sector individuals and organizations that have done the most to invade personal privacy in the United States in the past year. Three distinctive "Orwell" statues of a golden boot stomping a head will be presented to the government agencies and officials, companies and initiatives that have done the most to invade personal privacy in the previous year. The "Admiral John M. Poindexter Lifetime Menace" award will also be presented to an organization that has systematically invaded privacy over a long period of time.

The judging panel, which consists of lawyers, academics, consultants, journalists and civil rights activists, is currently inviting nominations from members of the public. Nominations can be submitted via the PI website.

Previous "winners" include the Federal Bureau of Investigation, the National Security Agency, DoubleClick, ChoicePoint, Delta Airlines, Trans Union, Oracle, the FAA's BodyScan system, the Department of Commerce and Microsoft.

"Brandeis" awards will also be given out to champions of privacy. The Brandeis Award is named after U.S. Supreme Court Justice Louis Brandeis, who is considered the father of American privacy law, describing privacy as "the right most valued by civilized" persons. The awards are given to those who have done exemplary work to protect and enhance privacy. Previous winners include Phil Zimmermann, creator of PGP; Beth Givens, founder of the Privacy Rights Clearinghouse; and Robert Ellis Smith, editor of the Privacy Journal.

The Big Brother Awards are celebrated internationally. There have also been ceremonies in the UK, Germany, Austria, Finland, Japan, Bulgaria, Belgium, Spain, Switzerland, Hungary, France, Denmark and

the Netherlands.

Big Brother Awards France (BBAF) recently held the year's first Big Brother ceremony to "honor" six French individuals, initiatives and companies with Big Brother prizes. BBAF also presented a Voltaire Award to a group of teachers who resisted government pressure to become police informers against their students.

Big Brother Awards:

http://www.privacyinternational.org/bigbrother/

Submit a nomination:

http://www.epic.org/redirect/bba_nomination.html

Big Brother Awards France:

http://bigbrotherawards.eu.org/2003/presse.html#4

==========
[6] News in Brief
==========

MATRIX UNLOADED: UTAH BACKS OUT OF CONTROVERSIAL PROGRAM

Utah has ceased participation in a controversial data mining program, joining other states that have either left the program or are scrutinizing their continued participation. Last week, Utah Governor Olene Walker withdrew Utah from the Multistate Anti-Terrorism Information Exchange (MATRIX) program, which allows law enforcement officials to instantly request information on a person from multiple data sources, both public and private. Neither Governor Walker nor the Utah Legislature had been briefed on Utah's involvement with the program. Under former Utah Governor Mike Leavitt, Utah was to have shared drivers license information, criminal records, and other records with MATRIX. Connecticut legislators have also begun to examine whether their state should remain in MATRIX, while Georgia recently terminated all connections with the MATRIX program, citing privacy concerns. Six states remain enrolled in MATRIX out of the original thirteen states that participated in the prototype program.

EPIC's amicus brief before the Supreme Court in Hiibel v. Nevada describing MATRIX:

http://www.epic.org/privacy/hiibel/hiibel_amicus.pdf

MATRIX program webpage:

http://www.iir.com/matrix

BUSH REQUESTS INCREASED FUNDING FOR CAPPS II, JUSTICE DEPT. IT

President Bush has proposed greater funding for homeland security initiatives in the administration's fiscal year 2005 budget request. The administration requested that $60 million be allotted for the Computer Assisted Passenger Prescreening System (CAPPS II), a significant increase over the $45 million proposed for the program in fiscal year 2004. The administration has also requested that the Justice Department be given $2.2 billion for information technology programs, which would constitute a 6 percent increase in the agency's overall budget from fiscal year 2004. $34 million is slated to go

toward the integration of fingerprint systems maintained by the FBI and former INS. A combined $64.5 has been requested for the Terrorist Screening Center, which will consolidate existing terrorist watch lists, and the Terrorist Threat Integration Center, which will allow law enforcement and the Department of Homeland Security to share information in terrorism investigations.

The Bush Administration's 2005 Budget Request:

http://www.whitehouse.gov/omb/budget/fy2005/

NJ COURT ENHANCES PROTECTIONS FOR FINANCIAL INFO

A New Jersey appeals court has issued a decision that provides stronger protection for financial records than is currently afforded by federal law. To acquire an individual's financial records from a financial institution, the State now will have to obtain a search warrant or a grand jury subpoena and notify the target of the investigation. In most circumstances, federal law requires only that individuals be given notice and an opportunity to object before a bank or other specified institution can disclose personal financial information to the federal government for law enforcement purposes. Notably, the New Jersey court specifically rejected a 1970s Supreme Court decision that refused to recognize privacy rights in information held by third parties. That decision has allowed police to obtain information from a vast array of businesses without notice to individuals or involvement with an independent magistrate.

The New Jersey appellate decision is available at:

http://www.judiciary.state.nj.us/opinions/a6521-01.pdf

For more information about federal financial privacy law, see EPIC's Right to Financial Privacy Act Page:

http://www.epic.org/privacy/rfpa/

CONFERENCE EXPLORES INTERNATIONAL IMPACT OF SPAM

The Organization for Economic Cooperation and Development (OECD) held a workshop on spam in Brussels last week to allow representatives of OECD Member State governments, the European Commission, consumer groups, and business stakeholders explore the problem of spam, focusing on its international dimension. Panels discussed sources and characteristics of spam as well as its societal, economic, business and technical impacts; approaches to combat spam; and the next steps to increase international cooperation to fight spam.

OECD Background Paper for the OECD Workshop on Spam:

http://www.epic.org/redirect/oecd_spam.html

European Commission January 22, 2004 Communication on Unsolicited Commercial Communications or "Spam":

http://www.epic.org/redirect/ec_spam.html

Trans Atlantic Consumer Dialogue February 2004 survey on spam:

http://www.tacd.org/docs/?id=225

Trans Atlantic Consumer Dialogue February 2004 Resolution:

http://www.tacd.org/docs/?id=224

For more information on spam, see the EPIC Spam Page:

http://www.epic.org/privacy/junk_mail/spam/

SWIPE PROJECT INTRODUCES DATA TOOLKIT

Artists Beatriz da Costa, Jamie Schulte, and Brooke Singer have created the "SWIPE Toolkit," a collection of web-based utilities that allow individuals to read the barcode on their driver's license and request personal information from data brokers. The Toolkit also features a "data calculator" that shows the fair market value of personal information, and the sources from which data brokers collect the information. The Toolkit is part of a larger performance, installation, and workshop that heightens awareness about automated collection of personal information. In March 2004, a SWIPE installation and performance will be exhibited at the Beall Center at University of California-Irvine.

The SWIPE Toolkit:

http://www.turbulence.org/Works/swipe/

The SWIPE Project:

http://www.we-swipe.us/

Beall Center SWIPE Performance:

http://beallcenter.uci.edu/calendar/swipe.htm

==========
[7] EPIC Bookstore: Protecting America's Health
==========

Protecting America's Health, The FDA, Business, and One Hundred Years of Regulation, by Philip J. Hilts (Knopf 2003).

http://www.powells.com/cgi-bin/biblio?inkey=1-037540466x-5

I have been interested in the history of the Food and Drug Administration for some time. The agency's development follows a policy debate of central importance: in protecting public health, to what degree will we adopt precautionary principles for food and drug safety and purity? The stakes are large, because regulation too strict will increase food prices, while as Hilts demonstrates, pure or even limited self-regulation results in serious harms to the public. Before the process of establishing precautionary principles in food and drug law took hold, manufacturers would lie, falsify evidence, and withhold information on the dangers of drugs. Food companies would mislabel products, for instance, by passing off laboratory-created glucose with added honeycombs and dye as pure honey. Patent medicine quacks would sell colored water as a cure for cancer, and products containing opium to sooth children.

Hilts' book is also interesting because drug and food policy debates closely track modern privacy law issues. The same arguments used to fight food and drug laws in 1900 are used today to prevent privacy protection. Invocations of "innovation" and free enterprise rights

repeatedly stopped Congress from enacting food and drug safety laws until people died and were disfigured by reckless behavior. In hindsight, we know the food and drug manufacturers' arguments were boguslaws that required safety and purity, although imperfect, reduced fraud and led to modern pharmaceutical science. We also know that not all innovation is good -- both in food and drugs and in technology. For instance, one well-known "innovation" quashed in the early days of the FDA was the practice of collecting abandoned horses in Manhattan for resale as "beef" in New Jersey.

In the conclusion, Hilts visits a now famous experiment that tested the ethics of business school students. In it, Wharton students were placed in a role-playing situation where their profitable company is reaping $1 million a month by continuing to market an ineffective, unsafe drug. A large majority of the students consistently chose the profit-maximizing role, one that kept the drug on the market without warnings, and actively frustrated government intervention. Perhaps the book should start with that study. It suggests that for all the talk of the benefits self-regulation, the most privileged business students will act like the charlatans of the 1900s (and believe that it is their duty to shareholders to do so). Hilts' book is a reminder that there still is a strong role for law in consumer protection to shield the public from less than ethical business behavior.

- Chris Jay Hoofnagle

==========

EPIC Publications:

"The Privacy Law Sourcebook 2003: United States Law, International Law, and Recent Developments," Marc Rotenberg, editor (EPIC 2003). Price: $40. http://www.epic.org/bookstore/pls2003/

The "Physicians Desk Reference of the privacy world." An invaluable resource for students, attorneys, researchers and journalists who need an up-to-date collection of U.S. and International privacy law, as well as a comprehensive listing of privacy resources.

==========

"FOIA 2002: Litigation Under the Federal Open Government Laws," Harry Hammitt, David Sobel and Mark Zaid, editors (EPIC 2002). Price: $40. http://www.epic.org/bookstore/foia2002/

This is the standard reference work covering all aspects of the Freedom of Information Act, the Privacy Act, the Government in the Sunshine Act, and the Federal Advisory Committee Act. The 21st edition fully updates the manual that lawyers, journalists and researchers have relied on for more than 25 years. For those who litigate open government cases (or need to learn how to litigate them), this is an essential reference manual.

==========

"Privacy & Human Rights 2003: An International Survey of Privacy Laws and Developments" (EPIC 2002). Price: $35. http://www.epic.org/bookstore/phr2003/

This survey, by EPIC and Privacy International, reviews the state of privacy in over fifty-five countries around the world. The survey examines a wide range of privacy issues including data protection, passenger profiling, genetic databases, video surveillance, ID systems

and freedom of information laws.

==========

"Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls" (EPIC 2001). Price: $20.
http://www.epic.org/bookstore/filters2.0/

A collection of essays, studies, and critiques of Internet content filtering. These papers are instrumental in explaining why filtering threatens free expression.

==========

"The Consumer Law Sourcebook 2000: Electronic Commerce and the Global Economy," Sarah Andrews, editor (EPIC 2000). Price: $40.
http://www.epic.org/cls/

The Consumer Law Sourcebook provides a basic set of materials for consumers, policy makers, practitioners and researchers who are interested in the emerging field of electronic commerce. The focus is on framework legislation that articulates basic rights for consumers and the basic responsibilities for businesses in the online economy.

==========

"Cryptography and Liberty 2000: An International Survey of Encryption Policy," Wayne Madsen and David Banisar, authors (EPIC 2000). Price: $20. http://www.epic.org/bookstore/crypto00&/

EPIC's third survey of encryption policies around the world. The results indicate that the efforts to reduce export controls on strong encryption products have largely succeeded, although several governments are gaining new powers to combat the perceived threats of encryption to law enforcement.

==========

EPIC publications and other books on privacy, open government, free expression, crypto and governance can be ordered at:

EPIC Bookstore
http://www.epic.org/bookstore/

"EPIC Bookshelf" at Powell's Books
http://www.powells.com/features/epic/epic.html

[8] Upcoming Conferences and Events

Living with the New Private Sector - Privacy Law: What Your Organization Needs to Know, a One Day Seminar and Training Session. Riley Information Services Inc. February 16, 2004. Ottawa, Canada. For more information: http://www.rileyis.com/seminars/index.html.

Antiterrorism and the Security Agenda: Impacts on Rights, Freedoms, and Democracy. International Civil Liberties Monitoring Group. February 17, 2004. Ottawa, Ontario, Canada. Email publicforum@iclmg.ca.

SPAM Technology Workshop. Computer Security Resource Center. February 17, 2004. Gaithersburg, MD. For more information:

http://csrc.nist.gov/spam.

Free Seminar on Electronic Advocacy for Nonprofits. Confluence. February 18, 2004. Washington, DC. E-mail info@confluencecorp.com.

IAPP 4th Annual Privacy & Security Summit & Expo. February 18-20, 2004. Washington, DC. For more information: http://www.privacyassociation.org/html/conferences.html.

RSA Conference 2004 - The Art of Information Security. February 23-27, 2004. San Francisco, CA. For more information: http://www.rsaconference.com.

Third Conference on Privacy and Public Access to Court Records. Courtroom 21 Project. February 27-28, 2004. Williamsburg, VA. For more information: http://www.courtroom21.net.

PKC 2004: International Workshop on Practice and Theory in Public Key Cryptography. Institute for Infocomm Research. March 1-4, 2004. Sentosa, Singapore. For more information: http://pkc2004.lit.org.sg.

A Summit on Healthcare Privacy and Data Security: HIPAA and Beyond. Health Care Conference Administrators. March 7-9, 2004. Baltimore, MD. For more information: http://www.hipaasummit.com.

Securing Privacy in the Internet Age. Stanford Law School. March 13-14, 2004. Palo Alto, CA. For more information: http://cyberlaw.stanford.edu/privacysymposium.

Sixth Annual National Freedom of Information Day Conference. First Amendment Center, in cooperation with the American Library Association. March 16, 2004. Arlington, VA. E-mail foidayconference@freedomforum.org.

CFP2004: 14th Annual Conference on Computers, Freedom, and Privacy. Association for Computing Machinery (ACM). April 20-23, 2004. Berkeley, CA. For more information: http://www.cfp2004.org.

2004 IEEE Symposium on Security and Privacy. IIEEE Computer Society Technical Committee on Security and Privacy, in cooperation with the International Association for Cryptologic Research (IACR). May 9-12, 2004. Oakland, CA. For more information: http://www.cs.berkeley.edu/~daw/oakland04-cfp.html.

International Conference on Data Privacy and Security in a Global Society. Wessex Institute. May 11-13, 2004. Skiathos, Greece. For more information: http://www.wessex.ac.uk/conferences/2004/datasecurity04/index.html.

The Third Annual Workshop on Economics and Information Security. University of Minnesota Digital Technology Center. May 13-14, 2004. Minneapolis, MN. For more information: http://www.dtc.umn.edu/weis2004.

Workshop on Privacy Enhancing Technologies. University of Toronto. May 26-28, 2004. Toronto, Canada. For more information: http://petworkshop.org/2004.

Access & Privacy Conference 2004: Sorting It Out. Government Studies, Faculty of Extension. June 10-11, 2004. University of Alberta. Edmonton, Alberta, Canada. For more information: http://www.govsource.net/programs/iapp/conference/main.nclk.

O'Reilly Open Source Convention. July 26-30, 2004. Portland, OR. For more information: http://conferences.oreilly.com/oscon.

First Conference on Email and Anti-Spam. American Association for Artificial Intelligence and IEEE Technical Committee on Security and Privacy. July 30-31, 2004. Mountain View, CA. For more information: http://www.ceas.cc.

Crypto 2004: The Twenty-Fourth Annual IACR Crypto Conference. International Association for Cryptologic Research, IEEE Computer Society Technical Committee on Security and Privacy, and the Computer Science Department of the University of California, Santa Barbara. Santa Barbara, CA. August 15-19, 2004. For more information: http://www.iacr.org/conferences/crypto2004.

2004 Telecommunications Policy Research Conference. National Center for Technology & Law, George Mason University School of Law. October 1-3, 2004. Arlington, VA. For more information: http://www.tprc.org/TPRC04/call04.htm.

==========
Subscription Information
==========

Subscribe/unsubscribe via Web interface:

http://mailman.epic.org/cgi-bin/mailman/listinfo/epic_news

Subscribe/unsubscribe via e-mail:

To: epic_news-request@mailman.epic.org
Subject: "subscribe" or "unsubscribe" (no quotes)

Automated help with subscribing/unsubscribing:

To: epic_news-request@mailman.epic.org
Subject: "help" (no quotes)

Problems or questions? e-mail < info@epic.org >

Back issues are available at: http://www.epic.org/alert/

The EPIC Alert displays best in a fixed-width font, such as Courier.

==========
Privacy Policy
==========

The EPIC Alert mailing list is used only to mail the EPIC Alert and to send notices about EPIC activities. We do not sell, rent or share our mailing list. We also intend to challenge any subpoena or other legal process seeking access to our mailing list. We do not enhance (link to other databases) our mailing list or require your actual name.

In the event you wish to subscribe or unsubscribe your e-mail address from this list, please follow the above instructions under "subscription information". Please contact info@epic.org if you would like to change your subscription e-mail address, if you are experiencing subscription/unsubscription problems, or if you have any other questions.

==========
About EPIC

==========

The Electronic Privacy Information Center is a public interest research center in Washington, DC. It was established in 1994 to focus public attention on emerging privacy issues such as the Clipper Chip, the Digital Telephony proposal, national ID cards, medical record privacy, and the collection and sale of personal information. EPIC publishes the EPIC Alert, pursues Freedom of Information Act litigation, and conducts policy research. For more information, e-mail info@epic.org, http://www.epic.org or write EPIC, 1718 Connecticut Ave., NW, Suite 200, Washington, DC 20009. +1 202 483 1140 (tel), +1 202 483 1248 (fax).

If you'd like to support the work of the Electronic Privacy Information Center, contributions are welcome and fully tax-deductible. Checks should be made out to "EPIC" and sent to 1718 Connecticut Ave., NW, Suite 200, Washington, DC 20009. Or you can contribute online at:

http://www.epic.org/donate/

Your contributions will help support Freedom of Information Act and First Amendment litigation, strong and effective advocacy for the right of privacy and efforts to oppose government regulation of encryption and expanding wiretapping powers.

Thank you for your support.

---------- END EPIC Alert 11.03 ----------

.