

# epic

annual report 2003-2004

67E1

## **contents**

- 1 mission & programs
- 2 privacy & transparency
- 4 program
- 6 publications
- 9 EPIC in congress
- 11 litigation
- 14 agency proceedings
- 17 internet public interest  
opportunities program
- 19 EPIC affiliated sites
- 21 EPIC board & staff
- 22 finances
- 24 supporters
- 25 FOIA gallery



## mission & programs

THE ELECTRONIC PRIVACY INFORMATION CENTER is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, freedom of expression and constitutional values in the information age. EPIC pursues a wide range of activities, including policy research, public education, conferences, litigation, publications, and advocacy.

EPIC is incorporated in Washington, DC and tax-exempt under IRC section 501(c)(3). EPIC receives support from individual contributors, private foundations, the sale of publications and attorneys fees. Contributions are fully tax-deductible.

EPIC maintains one of the web's most popular Internet policy sites—**epic.org**—and publishes the online EPIC Alert every two weeks with key information about issues affecting the rights of Internet users. EPIC also publishes *Privacy and Human Rights, Litigation Under the Federal Open Government Laws, Filters and Freedom*, the *Privacy Law Sourcebook*, and the *Consumer Law Sourcebook*. EPIC litigates high-profile privacy, First Amendment, and Freedom of Information Act cases. EPIC advocates for strong privacy safeguards. EPIC works in support of several NGO coalitions, including Privacy International (**privacyinternational.org**), the Internet Free Expression Alliance (**ifea.net**), the Global Internet Liberty Campaign (**giloc.org**), the Internet Democracy Project (**internetdemocracy.org**), and the Trans Atlantic Consumer Dialogue (**tacd.org**). EPIC also maintains the Privacy Site (**privacy.org**) and coordinates the Public Voice coalition (**thepublicvoice.org**), the National Committee for Voting Integrity (**votingintegrity.org**) the Privacy Coalition (**privacypledge.org**) and the In Defense of Freedom coalition (**indefenseoffreedom.org**).

SECRET

## privacy & transparency

**PRIVACY IS A PARADOX. To protect some information we must disclose other information.**

**To understand the impact of government policies on personal privacy, we need access to information about these policies. Openness enables privacy.**

From the beginning, EPIC has sought to use the Freedom of Information Act to better assess new challenges to privacy. In the past year, our FOI cases produced significant information about the Total Information Awareness program, the passenger screening system, and the growing number of privacy complaints that consumers have sent to federal agencies. These documents have been the subject of Congressional hearings and news reports across the country.

Not surprisingly, as we have become more successful in these cases, the government has become more aggressive in its legal strategy. After we pursued documents concerning John Poindexter's plan for a massive system of national surveillance, the Department of Defense challenged our status as a non-profit requester, a claim that no other government agency had made in our ten year history of pursuing these cases.

Last year a federal court rejected the Defense Department's position and ruled in favor of EPIC. The decision affirmed the right of all non-profit requesters to make effective use of our country's open government laws. (Samples of documents we obtained under the FOIA will be found at the end of this report.)

This edition of our annual report also describes our many activities during the past year. EPIC continues to be on the front lines of the most significant privacy and civil liberties issues. During the past year we testified in Congress, pursued open government cases, and filed amicus briefs in federal courts. In the Supreme Court, we submitted briefs in three cases, concerning such issues as resolving privacy and open government claims, damages for violations of the Privacy Act, and the compelled disclosure of personal identity by the police.

EPIC worked in coalition with other organizations to draw attention to emerging problems, such as the surveillance of the homeless and the problems of data mining. EPIC also participated in a wide range of agency proceedings. The topics ranged from traditional privacy concerns, such as financial medical privacy and information security, to new issues, including online identification, air travel privacy, biometrics and the WHOIS database.

“

EPIC’s work is of consistently high quality...it is a leader in the causes of information privacy and electronic civil liberties ... EPIC is both pioneering and effective. – M.F.

”

EPIC launched a new web site—the National Committee on Voting Integrity—to address growing public concerns about the reliability of electronic voting systems. The secret ballot requires ensuring both the integrity and privacy of the voting process. Several members of the EPIC Advisory Board are experts in this field. We will be working to promote stronger voting standards.

EPIC also undertook a significant upgrade of The Public Voice web site, and we have recently published a new sourcebook to promote civil society participation in the World Summit on the Information Society, an important forum established by the United Nations to promote global dialogue on the future of the Internet and the information society.

The EPIC web site continued as the leading privacy resource for Internet users. According to Google, EPIC maintains the top ranked web pages for “privacy,” “Total Information Awareness,” “Patriot Act,” “passenger profiling,” “digital rights management,” “the public voice,” and “in defense of freedom” among others.

Much of the focus today in Washington is on developing more widespread surveillance of the public with some modest privacy safeguards. The belief is that massive data mining can be made “privacy friendly.” Given our experience with the Clipper encryption scheme and the Carnivore Internet monitoring plan, we believe good privacy technology is unlikely to result when the end goal is surveillance.

We have recently joined with the University of Ottawa Law School to launch a new project on Anonymity and Identity. The goal is to find new approaches for robust technical methods that will safeguard privacy.

With technical standards, as with law, openness enables trust and will help ensure better protection for privacy.

**MARC ROTENBERG**

*President*

*Electronic Privacy Information Center*



## program

### FREE SPEECH

*"A great resource on civil liberties and First Amendment issues."* —WIRED MAGAZINE

"The most participatory form of mass speech yet developed." That's how Judge Stewart Dalzell described the Internet in the landmark court decision striking down on-line censorship. As a leading publisher of policy materials on the Internet, EPIC joined with other civil liberties and computer industry organizations and served as both co-counsel and co-plaintiff in that historic litigation. EPIC has continued to play a leading role in defense of free expression, including the right to receive and distribute information anonymously.

And because there are no borders in cyberspace, EPIC co-founded the Global Internet Liberty Campaign ([www.gilc.org](http://www.gilc.org)), the first international coalition dedicated to preserving on-line freedoms throughout the world.

### OPEN GOVERNMENT

*"EPIC's Freedom of Information Act work attracts widespread praise."* —LEGAL TIMES

EPIC is a recognized leader in the use of the FOIA to obtain information about government policy on emerging technology issues. Public disclosure of this information improves government oversight and accountability—in the words of one federal official, EPIC's work contributes to an "honorable and civilized debate" on critical policy questions.

EPIC's research underscores the words of James Madison, who said "a people who mean to be their own governors, must arm themselves with the power knowledge gives." Information obtained by EPIC has been featured in national publications and cited in government reports. EPIC also makes scanned images of formerly classified documents, obtained through the FOIA, available to Internet users around the globe at the EPIC web site—[epic.org](http://epic.org).

### PRIVACY

*"Anyone concerned about the civil rights implications of the Clipper chip, the Digital Telephony proposal, national ID cards, medical record privacy, credit records and the sale of consumer data will find this Washington public interest research center invaluable."*

—THE ATLANTA JOURNAL AND CONSTITUTION

Automated health care records. Electronic mail. On-line commerce. Surfing the World Wide Web. These and many other technological innovations bring with them emerging challenges to personal privacy. EPIC is a leader in examining the issues and offering solutions to protect personal information from misuse, and is frequently called upon by Congressional committees and government agencies to assess new approaches for privacy protection.

With the world's most comprehensive archive of privacy resources, EPIC's award-winning Web site demonstrates the educational potential of the Internet. Accessed by thousands of people every day, the EPIC site is a significant source of information critical to today's consumers.

## THE PUBLIC VOICE

*"There is an increasing recognition that we must involve all stakeholders including the voice of civil society. The Public Voice meeting and its contribution to the Forum have been constructive and positive."* —OECD UNDER-SECRETARY GENERAL

The rise of the Internet and the creation of global markets have created new challenges for democratic governance. International institutions now make many decisions once made by national and local governments. The concerns of citizens are too often not represented when government officials and business representatives gather.

EPIC has worked to promote the participation of NGO leaders in decisions affecting the future of the Internet on issues ranging from encryption policy and privacy to consumer protection, Internet governance, and the role of emerging market economies. Through international conferences, reports and funding for travel, EPIC seeks to strengthen the Public Voice and to increase the presence of NGOs at meetings across the globe.

In cooperation with the OECD, UNESCO, and other international organizations, the Public Voice project brings civil society leaders face to face with government officials for constructive engagement about current policy issues. Public Voice events have been held in Dubai, Hong Kong, Ottawa, Paris, Washington and Honolulu.

**"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor or reputation. Everyone has the right to the protection of law against such interference or attack."**

—ARTICLE 12, UNIVERSAL DECLARATION OF HUMAN RIGHTS

**"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart ideas through any media and regardless of frontiers."**

—ARTICLE 19, UNIVERSAL DECLARATION OF HUMAN RIGHTS



## publications

*“A survey released on the eve of important government hearings on Web privacy suggests users are extremely vulnerable to cyberspace spying and other personal intrusions by Internet businesses. The results could help frame one of the most fundamental debates in the evolution of the Internet as a commercial marketplace: Whether the industry can police itself or the government must step in to protect millions of personal computer users.”* —ASSOCIATED PRESS

EPIC produces several publications each year that are popular among policy makers, scholars, and advocates both in the United States and around the world. EPIC publications are available for sale at the EPIC Online Bookstore ([bookstore.epic.org](http://bookstore.epic.org)) and also from the EPIC Bookshelf at Powell’s Books ([powells.com/features/epic/epic.html](http://powells.com/features/epic/epic.html)). Discounts are available for multiple copies to educational institutions.

### **The Privacy Law Sourcebook: United States Law, International Law, and Recent Developments**

Updated annually, the *Privacy Law Sourcebook* is an invaluable resource for students, attorneys, researchers and journalists who need a comprehensive collection of U.S. and International privacy law, as well as a full listing of privacy resources.

### **Litigation Under the Federal Open Government Laws**

The fully updated edition of the manual that lawyers, journalists and researchers have relied on for more than 25 years, this standard reference work covers all aspects of the Freedom of Information Act, the Privacy Act, the Government in the Sunshine Act, and the Federal Advisory Committee Act.



### **Privacy & Human Rights: An International Survey of Privacy Laws**

This annual survey, by EPIC and Privacy International, reviews the state of privacy in over sixty countries around the world. The survey examines a wide range of privacy issues including data protection, telephone tapping, genetic databases, ID systems and freedom of information laws.

### **The Public Voice WSIS Sourcebook Perspectives on the World Summit on the Information Society**

This publication is intended to promote understanding of the WSIS and to encourage greater civil society participation in the current phase of the summit.

### **Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls**

Often characterized by their proponents as mere features or tools, filtering and rating systems can also be viewed as fundamental architectural changes that may, in fact, facilitate the suppression of speech far more effectively than national laws alone ever could. This collection of essays, studies, and critiques of Internet content filtering should be carefully considered if we are to preserve freedom of expression in the online world.

#### **Other Reports from EPIC**

- Surfer Beware: Personal Privacy and the Internet
- Surfer Beware II: Notice is Not Enough
- Surfer Beware III: Privacy Policies Without Privacy Protection
- Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the Report of the President's Commission on Critical Infrastructure Protection
- The Public Voice and the Digital Divide: A Report to the DOT Force
- Network Advertising Initiative: Principles not Privacy
- Pretty Poor Privacy: An Assessment of P3P and Internet Privacy
- Paying for Big Brother: A Review of the Proposed FY2003 Budget for the Department of Justice
- Your Papers, Please: From the State Drivers License to a National Identification System
- WHOIS Privacy Issues Report

“

EPIC and its services, particularly its e-mail alerts, have always been among the most useful to me in my law practice, and your most recent assistance to me is just further proof. Please keep up your efforts.

– P.J.B.

”

### **EPIC Staff Publications, 2003**

Hofmann, "New Hampshire Supreme Court to Decide Question of Third Party Liability for Invasion of Privacy," American Bar Association Media, Privacy and Defamation Law Committee Newsletter, Fall 2002

Hoofnagle, "Public Records and Privacy," Presented to the National Conference of Bankruptcy Judges 77th Annual Meeting , October 17, 2003

Hoofnagle, "Is your life an open book? And who's reading it? If Congress heeds industry groups, a wide audience could see your data," (Knight Ridder/Tribune Information Services) Akron Beacon Journal, September 8, 2003

Hoofnagle (with Kerry E. Smith), "Debunking the Commercial Profilers' Claims," Privacy Journal, August 2003

Hoofnagle, "What About Information Collectors' First Amendment Defenses?," Privacy Journal, February 2003

Hoofnagle, "Protecting the Fundamental Student Right to Privacy," Campus Privacy Review, 2003

Laurant, Observing Surveillance Photographs, reprinted in Deborah Morley & Charles Parker, "Understanding Computers: Today and Tomorrow 2003," (Thompson 2003)

Madsen, "Patriot Act: Drop repressive portions of anti-terror law," Chattanooga Times Free Press, November 30, 2003

Madsen, "USA PATRIOT ACT; Reject greater surveillance power, Milwaukee Journal Sentinel, November 9, 2003

Madsen, "FCC ruling would have a chilling effect on public debate," Bergen County Record, September 8, 2003

Madsen, "Respect Rights of Protest Groups," Miami Herald, September 27, 2003

Rotenberg, "A Vote Against the Computerized Ballot," Technology Review, September 2003

Rotenberg, "Of Church and State: Why History Matters in a Post 9/11 World," The Big Story 27–30, Summer 2003

Rotenberg, "Privacy and Secrecy After September 11," in Bombs and Bandwidth 132–42 (The New Press 2003)

Rotenberg, Mihir Kshirsagar, Cédric Laurant, and Kate Rears, "Exhibit: Observing Surveillance" in Bombs and Bandwidth 142–53 (The New Press 2003)

Rotenberg (with Daniel J. Solove), "Information Privacy Law" (Aspen Publishing 2003)

Sobel, "Internet Filters and Public Libraries," First Amendment Center, November 2003

*"When Big Brother keeps tabs on the people, it is nice to know there are some people keeping tabs on Big Brother."* —NEW YORK LAW JOURNAL

*"EPIC's Bill Track is a good current resource for federal legislation concerning privacy, speech and cyber-liberties,"* —INTERNET LAW RESEARCHER

In 2003, EPIC appeared before many Congressional committees to present testimony on critical privacy and civil liberties issues. EPIC also worked in coalition with other organizations to draw attention to emerging problems, such as the surveillance of the homeless and the problems of datamining.

### **Medical Privacy**

EPIC Executive Director Marc Rotenberg testified before a House Financial Services Subcommittee on the need to expand medical privacy protections within financial privacy laws. EPIC urged Congress to close a loophole that allowed medical information to go unprotected.

### **Financial Privacy**

EPIC submitted comments to the Senate Banking Committee in favor of opt-in protections for affiliate sharing. EPIC argued that the size of modern financial institutions has diminished individuals' control over their personal information, leading to fraudulent telemarketing and heightened risk of identity theft. EPIC submitted comments to the Senate Banking Committee to highlight structural flaws in the credit reporting system that lead to inaccuracy and consumer frustration. EPIC called upon the Congress to strengthen accuracy requirements in the Fair Credit Reporting Act.

EPIC Legislative Counsel Chris Hoofnagle testified before the House Financial Services Committee in opposition to federal preemption of state privacy and identity theft law. Nine leading consumer and civil liberties groups joined EPIC's testimony. EPIC also released new documents obtained under the FOIA indicating that consumer complaints to the Federal Trade Commission regarding the credit reporting agencies have increased dramatically.

### **Spam**

EPIC Executive Director Marc Rotenberg testified before the Senate Commerce Committee in favor of strong, effective measures to curb spam. EPIC supported an opt-in framework, a private right of action for consumers, technical measures, and international cooperation.

## **Data Mining**

EPIC wrote to Congress to formally request a halt to the Department of Defense's "Total Information Awareness" program. EPIC cited the privacy implications of the Pentagon's proposed domestic surveillance system and other "data mining" initiatives, the groups said that "Congress should put such programs on hold and ask the tough policy questions up front, long before domestic surveillance systems scoop up Americans' personal information." Ultimately, Congress cut funding for the controversial program.

EPIC submitted comments to a hearing before the House Government Reform Subcommittee on Information Policy describing the risks to privacy and civil liberties posed by data mining. Relying upon documents obtained through the Freedom of Information Act, EPIC argued that since the government obtains volumes of personal information from private-sector companies, Congress should extend the Privacy Act to cover commercial information brokers.

EPIC joined a broad coalition of national organizations urging Congress to stop the deployment of the second-generation airline passenger profiling system known as CAPPs-II (Computer Assisted Passenger Pre-Screening System). The coalition letter asked Congress to assess the program's effectiveness, its cost, and its impact on civil liberties before allowing the agency to move forward with the surveillance program.

## **International Consumer Protection**

EPIC Executive Director Marc Rotenberg testified before the Senate Commerce Committee on the need to address the growing problem of cross-border fraud. The Committee explored the possibility of expanding Federal Trade Commission authority to pursue marketers and others who engage in unfair or deceptive practices outside the borders of the United States of America.

Marc Rotenberg testified again before a House Commerce Subcommittee on the need to address the problem of cross-border fraud. EPIC supported an effort to expand Federal Trade Commission enforcement powers, but urged Congress to remove provisions that reduced privacy safeguards, limited government oversight, and diminished legal safeguards.

## **Social Security Numbers**

EPIC Legislative Counsel Chris Hoofnagle testified before the House Ways and Means Subcommittee on Social Security in favor of protections for Social Security Numbers. EPIC argued that private and public sector reliance on the identifier exacerbated identity theft and privacy violations.

## **Homeless Surveillance**

EPIC and a coalition of civil liberties groups alerted the House and Senate Banking Committees of the Department of Housing and Urban Development's plans to create a homeless surveillance program. The program, known as Homeless Management Information Systems, collects detailed personal information on the homeless, and enables it to be shared regionally.

The project leader for this effort will be  
gineer (EE) [REDACTED] can be  
703) [REDACTED]

## litigation

*"[EPIC] has used the Freedom of Information Act to monitor the Government's actions, and has been the first to disclose, among other things, the Federal Bureau of Investigation's desire to redesign the telephone system to ease wiretapping."* —THE NEW YORK TIMES

### **EPIC's litigation strategy follows five principles:**

- To vigorously pursue pending matters to a favorable conclusion
- To initiate or defend emerging legal challenges implicating free speech, privacy, anonymity and open access, particularly in an online or electronic environment
- To actively promote the public dissemination of materials obtained under the Freedom of Information Act
- To provide assistance to attorneys, consumer and civil liberties organizations on legal matters as needed, and
- To seek the participation of consumer and civil liberties organizations as well as technical and legal experts as appropriate so as to expand public involvement in emerging legal issues.

### **NEWS MEDIA FEE STATUS—EPIC v. DOD**

In February 2002, EPIC requested documents from the Department of Defense concerning the agency's new Information Awareness Office and its director, retired Admiral John Poindexter. In response to the request, DoD denied EPIC's request for "news media" fee status, thus imposing a substantial financial barrier to EPIC's effort to obtain responsive documents. Noting that DoD's action was the first denial of an EPIC request for preferred fee status in the history of the organization, EPIC filed suit against the agency and moved for a preliminary injunction. In January 2003, a federal district court ruled that EPIC is entitled to "preferred fee status" under the FOIA and ordered the Pentagon to "expeditiously" process EPIC's request. The Defense Department agreed to pay EPIC attorney's fees. The case provides significant benefits for all non-profit users of the Freedom of Information Act who are now entitled to favorable treatment in fee determinations.

### **PRIVACY ACT DAMAGES—DOE v. CHAO (AMICUS)**

This case concerns a class of coal miners whose Social Security Numbers were improperly disclosed by the government to others. The Supreme Court granted certiorari in June 2003 to consider the question of whether an individual bringing suit under the Privacy Act for

wrongful SSN disclosure must prove that he suffered actual monetary damages as a result of the disclosure in order to recover the minimum damages provided by the Privacy Act. EPIC, 12 privacy organizations, and 16 legal scholars and technical experts filed an amicus brief arguing that the Privacy Act provides damages for those who suffer “adverse effects.” The brief points to the dangers of SSN disclosure, the tradition of providing similar awards in other privacy laws, and the history of the Privacy Act.

#### **SALE OF PERSONAL INFORMATION—BOYER v. DOCUSEARCH (AMICUS)**

Amy Boyer was murdered after an information broker provided contact details to her assailant. Boyer’s estate sued the information broker and a private investigator for wrongful death, invasion of privacy, and for “pretexting,” the process of collecting personal information through deception. EPIC filed an amicus brief arguing that the defendants should be liable under all claims. In February 2003, the Supreme Court of New Hampshire held that private investigators and information brokers have a duty to exercise reasonable care when the sale of personal information creates a risk to the individual being investigated. In a significant expansion of privacy protection, the court held that the investigators could be liable for damages resulting from the sale of information obtained through pretexting.

#### **OPEN GOVERNMENT—EPIC v. DOJ**

In September 2003 EPIC asked the Department of Justice for documents related to a memorandum sent to federal prosecutors that urged the prosecutors to lobby members of Congress on PATRIOT Act issues. The DOJ refused to expedite processing of EPIC’s request on the grounds that the memorandum is not a subject of exceptional media interest, and raises no questions about the government’s integrity that might affect public confidence. In October 2003, EPIC filed suit in federal court and asked that the DOJ be ordered to release immediately the requested material.

#### **OPEN GOVERNMENT—EPIC v. TSA**

In August 2003, EPIC requested from the Transportation Security Administration materials prepared on the controversial Computer Assisted Passenger Prescreening System (CAPPS II). TSA agreed to process the documents, but failed to respond to EPIC’s request for expedited processing. In September, EPIC applied for an emergency court order requiring TSA to immediately release the requested documents. TSA then refused to release the documents, claiming that they were exempt from disclosure under the Freedom of Information Act. EPIC and TSA are now litigating the extent to which the documents must be released.

#### **OPEN GOVERNMENT—EPIC v. DHS**

In March 2003, EPIC requested from the Transportation Security Administration any privacy assessments of the Computer Assisted Passenger Prescreening System (CAPPS II), and from the Department of Defense information concerning Pentagon involvement in the controversial airline passenger screening system. Neither agency completed processing the requests,

despite their agreement to “expedite” the process. EPIC filed suit in June, alleging that the agencies failed to comply with the disclosure requirements of the Freedom of Information Act, and asking a federal judge to order the disclosure of information concerning the development of CAPPs II.

#### **FREE SPEECH—US v. ALA**

EPIC served as co-counsel in *United States v. American Library Association*, a challenge to a federal law that forces libraries to censor constitutionally protected speech on the Internet through the use of filtering. EPIC argued that the filtering programs routinely and inexplicably block sites that clearly do not fall under the categories proscribed by the law. The lawsuit also challenged filtering on privacy grounds, as individuals had to relinquish their anonymity in asking to have the filters deactivated when they inappropriately blocked a site. The Supreme Court ruled that CIPA is constitutional, and that public libraries can be required to install software designed to block sexually explicit Web sites.

#### **OPEN GOVERNMENT—CITY OF CHICAGO v. BATF (AMICUS)**

EPIC has focused on promoting open government, and innovating solutions that allow oversight of government activities while shielding personal information from exposure. In *City of Chicago v. BATF*, the City of Chicago submitted a request under FOIA seeking disclosure of nationwide data from government gun sales databases. The Seventh Circuit ruled that there was no valid privacy interest in the information requested. On appeal to the Supreme Court, EPIC, and a coalition of technical and legal experts, filed an amicus designed to resolve the apparent conflict that the case presented between open government and individual privacy by illustrating that, through the use of technology, the government can decode the information before releasing it, thereby shedding the necessary sunlight on government activities while protecting individual privacy rights. The Supreme Court remanded the case, without decision, after Congress enacted a prohibition on the expenditure of funds to release the type of data at issue in the case.

#### **PERSONAL INFORMATION ONLINE—SMITH v. DOE (AMICUS)**

EPIC has sought to shield personal information from being posted online by government officials. In *Smith v. Doe*, the Ninth Circuit Court of Appeals invalidated Alaska’s “Megan’s Law” statute, which required posting of information about released sex offenders online. EPIC filed an amicus brief urging the Supreme Court to hold that the Alaska Megan’s law statute violates the Ex Post Facto clause of the Constitution. EPIC argued that the mandatory online dissemination of a sex offender registry is excessive when weighed against the statutory purpose of protecting people in the geographic vicinity of released offenders. However, the Court ruled that the statute, even though it was retroactively applied, did not violate the Constitution.

“  
Thank you for  
all your hard work  
on behalf of civil  
liberties and the  
U.S. Constitution.

– P.S.

”



In 2003, EPIC participated in a wide range of agency proceedings. The topics ranged from traditional privacy concerns, such as medical privacy and information security, to new issues, including online identification, air travel privacy, biometrics and the WHOIS database.

**Online Identification and Authentication**

The European Commission determined that Microsoft violated data protection rules in its implementation of the Passport identification and authentication system. This action followed EPIC’s filing of complaints with the Federal Trade Commission, Attorneys General, and international authorities that detailed the privacy risks raised by Microsoft Passport.

**Air Travel Privacy**

EPIC filed comments at the Immigration and Naturalization Service against proposed rules that would require airlines to submit passenger manifest information on all international travelers. EPIC argued that the requirement violated the Privacy Act and Constitutional guarantees of the right to travel.

EPIC submitted comments to the Transportation Security Administration in opposition to a new database of aviation security screening records. EPIC argued that the system violated Constitutional rights to free association and travel.

EPIC Policy Counsel Cédric Laurant testified at a European Parliament Committee on Citizens’ Freedoms and Rights hearing on traveler profiling. EPIC’s statement identified the threats that extensive US profiling programs raise for European and American travelers’ privacy.

EPIC filed a complaint with the Federal Trade Commission urging the agency to investigate JetBlue Airlines and Acxiom for violations of federal laws. The companies transferred information on passengers in violation of their own privacy policies.

**International Privacy**

EPIC filed comments with the Federal Trade Commission recommending that the agency address the privacy implications of the international transfer of personal information in consumer fraud investigations.



“

Thank you for  
your efforts to  
get congress to  
review the recent  
loosening of  
surveillance and  
investigation  
rules for the FBI...  
Thank you and  
EPIC for the  
vigilance! – J.D.

”

### **WHOIS**

EPIC filed comments with the Federal Trade Commission regarding the law enforcement use of personal information in the WHOIS database. EPIC urged the agency to address the privacy free speech, and consumer fraud implications of requiring domain name registrants to provide personal information.

EPIC issued a report on personal information in the WHOIS database. EPIC's report recommended that WHOIS policies follow the Organization for Economic Cooperation and Development Privacy Guidelines.

### **Biometrics**

EPIC submitted comments to the Organization for the Advancement of Structure Information Standards regarding XML formatters for biometric information. EPIC's comments argued that the standard may respect security standards but that it did not provide privacy protection.

### **Police Databases**

EPIC organized a coalition and online petition drive to urge the Federal Bureau of Investigation to retain data accuracy and integrity standards for the National Crime Information Center, the nation's largest criminal justice databases. The FBI is seeking to exempt the NCIC from its Privacy Act obligations.

### **Financial Privacy**

EPIC filed comments with the Office of the Comptroller of the Currency in opposition to the agency's plans to preempt state consumer protection and privacy laws. EPIC argued that the agency lacked the legal authority to prevent states from enforcing consumer protection and privacy laws against banks and their affiliates.

EPIC submitted comments to the Federal Trade Commission in favor of a framework of Fair Information Practices to address business uses of personal information. EPIC argued that businesses have used personal information to limit consumer choice, to raise prices, and to engage in fraud.

### **Children's Privacy**

EPIC and 11 consumer organizations filed a complaint with the Federal Trade Commission alleging that Amazon.com illegally collected and disclosed children's personal information in violation of the Children's Online Privacy Protection Act. The complaint includes examples of children's information on the site, and marketing efforts to entice children to disclose their personal information online.

“

I just wanted you to know that there are many people (including myself) who really appreciate what you are doing. I admire your passion and commitment and appreciate you working hard to protect the privacy of us all. – D.L.

”

“

I saw your comments on TechTV and I was glad to see your efforts and explaining the gravity of what is happening with the infamous Magic Lantern project. You really spelled it out clearly and I was encouraged to see people like you stepping up to this. I am glad to see what EPIC is doing and will look more into how I might be able to support your efforts. – B.S.

”

#### ***Homeless Surveillance***

EPIC alerted the public to the Department of Housing and Urban Development’s plans to create “Homeless Management Information Systems.” The systems establish the infrastructure for national tracking of homeless persons. In September, EPIC, joined by eight civil liberties groups, urged the agency to end the proposal to track the homeless.

#### ***Medical Privacy***

EPIC and 28 advocacy organizations sent a letter to the Department of Health and Human Services urging guarantees of protection for health data that is transmitted among banks. Financial institutions had expressed plans in using data mining to analyze this health information for marketing and credit risk evaluation.

#### ***Access to Personal Information***

EPIC urged the Federal Trade Commission to investigate Experian, a credit reporting agency, for its marketing of “free” credit reports. The company guaranteed individuals free access to their credit reports, but instead offered an expensive credit monitoring service that individuals must cancel within thirty days to avoid charges.

#### ***Information Security***

EPIC submitted comments to the Department of the Treasury on a proposed guidance on security breach notices to bank customers. EPIC urged the agency to expand the definition of “sensitive consumer information” and to require financial institutions to report statistical information on all security events to federal regulators.



## internet public interest opportunities program

*"My best experience at EPIC was the successful FOIA request. But the most rewarding was helping to prepare testimony and attempt to influence policy... I enjoyed getting an intimate look at the legislative process and the role of a public interest organization in that process. Being involved in that process was unique and rewarding.... The eclectic group. It was obvious that a real effort was made to bring completely different students together and it added a lot to the summer.... Really the best part of the program is the ability to meet and interact with a lot of really diverse and intelligent people, both clerks, staff, and advisory board members.... I will go home having gained much knowledge, skills and a heightened appreciation for public interest law."*

—2003 IPIOP FELLOWS

A grant from the Glushko Samuelson Foundation established the Internet Public Interest Opportunities Program (IPIOP). IPIOP is an intensive, paid legal internship with EPIC that is held during the summer, fall, and spring terms. The internships are available for outstanding students with a strong interest in civil liberties issues relating to the Internet, particularly free speech, privacy, open government, and democratic governance. The program gives students the opportunity to actively participate in valuable programs in Internet law, policy, and legislation. Washington, DC provides an ideal location for an introduction to Internet law and policy. IPIOP clerks attend agency proceedings, policy meetings, Congressional hearings, and visit landmarks in the Nation's Capital. IPIOP clerks also attend weekly seminars led by eminent scholars and practitioners in the field of Internet policy. The work of EPIC's IPIOP clerks has been cited in Supreme Court briefs and articles in *The New York Times* and *The Washington Post*.

“

I want to tell you that I very much appreciate the information offered by your site. As an IT professional I appreciate how easily information use can become information abuse.

– D.C.

”

#### **LEGISLATION**

The legislative process is the critical opportunity for public interest organizations to make a case directly to lawmakers, and to establish connections with key committees and decision makers. IPIOP clerks learn about this process by researching and drafting memoranda on issues before Congress and by attending hearings.

#### **GOVERNMENT OVERSIGHT**

The Freedom of Information Act (FOIA) is a powerful tool for public interest organizations to learn about otherwise inscrutable governmental activities and to promote public oversight. Each IPIOP clerk researches, drafts, and submits a FOIA request to a federal agency. Clerks also assist in litigating pending FOIA matters.

#### **LITIGATION**

Clerks assist EPIC staff in developing litigation strategy in key cases with significant impact on critical Internet issues. Clerk activities include drafting memoranda, meetings with attorneys, and attending court hearings. Clerks also review federal and state court dockets for amicus opportunities.

#### **COLLABORATION**

IPIOP works in association with public interest litigators and law school clinics across the country. A distinguished Advisory Committee oversees the work of IPIOP. Graduating law school students interested in working at EPIC are also encouraged to seek fellowships through Equal Justice Works ([equaljusticeworks.org](http://equaljusticeworks.org)).

#### **APPLICATIONS**

Submit a letter of interest, a writing sample, a résumé, and a recommendation letter to: IPIOP Coordinator, EPIC, 1718 Connecticut Ave. N.W., Suite 200, Washington, DC 20009 or email [ipiop@epic.org](mailto:ipiop@epic.org). The process is competitive. More than 300 applications were received for last year's program.

parate cover will call for the following:

1 b2-2  
E-1

epic affiliated sites

(S)

*"This consumer group provides a wealth of information at its Web site."*

—GOVERNING MAGAZINE

In 2003, EPIC launched a new web site—the National Committee on Voting Integrity—to draw attention to growing public concerns about the reliability of electronic voting systems. EPIC also undertook a significant upgrade of The Public Voice web site, in recognition of the critical role of civil society at the World Summit on the Information Society conference held in Geneva.

**EPIC Bookstore**

**[bookstore.epic.org](http://bookstore.epic.org)**

The EPIC Bookstore offers EPIC publications and a wide range of titles on privacy, free speech, computer security, and civil liberties. The Bookstore also showcases a growing list of featured titles from each issue of the EPIC Alert newsletter.

**Global Internet Liberty Campaign (GILC)**

**[gilc.org](http://gilc.org)**

There are no borders in cyberspace. Actions by individual governments and multi-national organizations can have a profound effect on the rights of citizens around the world. The member organizations of GILC joined together to protect and promote fundamental human rights such as freedom of speech and the right of privacy on the net for users everywhere.

**In Defense of Freedom (IDOF)**

**[indefenseoffreedom.org](http://indefenseoffreedom.org)**

The IDOF coalition was established after September 11 to demonstrate public support for the protection of Constitutional values and to provide an organizing forum for individuals and associations pursuing issues arising from the government's response. The ten-point statement In Defense of Freedom, endorsed by more than 150 organizations, 300 law professors, and 40 experts in computer science, is available on the site.

“  
Thank you for the  
resources you've  
provided which  
I've accessed via  
the web. Please  
maintain your  
efforts, and continue  
your pursuit in  
ending TIA. – s.j.  
”

*“EPIC is a public interest research center based in Washington. It offers a great collection of online resources about privacy and also provides information on how you can act politically to motivate your government representatives to protect your privacy.”*

—CHRISTIAN SCIENCE MONITOR

### **Privacy International (PI)**

#### **[privacyinternational.org](http://privacyinternational.org)**

PI is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations worldwide. PI has conducted campaigns in Europe, Asia and North America to counter abuses of privacy by way of information technology such as ID card systems, video surveillance, data matching, police information systems, telephone tapping, and medical records.

### **The Privacy Site**

#### **[privacy.org](http://privacy.org)**

The Privacy Site, founded in 2000 as a joint project of EPIC and Privacy International, contains the latest news, links, and resources on privacy issues, as well as action items to engage members of the public in personal privacy advocacy.

### **The Public Voice**

#### **[thepublicvoice.org](http://thepublicvoice.org)**

The Public Voice was launched to promote the participation of Non-Governmental Organizations (NGOs) in the deliberations of international organizations, such as the Organization for Economic Cooperation and Development (OECD), in matters concerning Internet policy. Public Voice conferences have been held in Ottawa, Paris, Hong Kong, and Dubai.

### **National Committee for Voting Integrity**

#### **[votingintegrity.org](http://votingintegrity.org)**

The National Committee for Voting Integrity was established in 2003 to promote voter-verified balloting and to preserve privacy protections for elections in the United States. The National Committee is a non-partisan organization made up of leading technical experts, lawyers, journalists, and citizens.

### **Privacy Coalition**

#### **[privacycoalition.org](http://privacycoalition.org)**

The Privacy Coalition web site was launched in 2001 to serve as an organizing tool for a nonpartisan coalition of consumer, civil liberties, educational, family, library, labor, and technology organizations. Members of the Privacy Coalition have agreed to the Privacy Pledge, a framework of privacy protections endorsing limits on government surveillance and the promotion of Fair Information Practices.



## epic board & staff

### EPIC Staff

Marc Rotenberg  
*President*  
*Executive Director*

David L. Sobel  
*General Counsel*

Lillie Coney  
*Senior Policy Analyst*  
*Coordinator, National*  
*Committee for Voting Integrity*

Chris Jay Hoofnagle  
*Associate Director*

Cédric Laurant  
*Policy Counsel*  
*Project Director,*  
*Observing Surveillance*

Marcia Hofmann  
*Staff Counsel*

Frannie Wellings  
*Policy Fellow*  
*Coordinator, Public Voice*

Emily Cadei  
*Communications Associate*

Tiffany Stedman  
*Law Fellow*

Harry Hammitt  
*Senior Fellow*

Wayne Madsen  
*Senior Fellow*

Stephanie Perrin  
*Senior Fellow*

Anna Slomovic  
*Senior Fellow*

### EPIC Advisory Board

*EPIC works closely with a distinguished advisory board drawn from the information law, computer science, civil liberties and privacy communities.*

Prof. Phil Agre

Hon. John Anderson

Prof. Ann Bartow  
*IPIOP Advisory Committee*

D. James Bidzos

Prof. Francesca Bignami  
*IPIOP Advisory Committee*

Prof. Christine Borgman

Prof. James Boyle  
*IPIOP Advisory Committee*

David Burnham

Prof. Anita Allen-Castellitto  
*IPIOP Advisory Committee*

Vinton G. Cerf

David Chaum

Prof. Julie E. Cohen  
*IPIOP Advisory Committee*

Simon Davies

Whitfield Diffie  
*Board Member*

Prof. David Farber

Hon. David Flaherty

Prof. Oscar Gandy  
*Chair*

Austin Hill

Deborah Hurley  
*Board Member*

Prof. Jerry Kang

Judy Krug  
*IPIOP Advisory Committee*

Prof. Gary Marx

Mary Minow

Peter G. Neumann  
*Secretary*

Prof. Eli Noam

Prof. Anita Ramasastry  
*IPIOP Advisory Committee*

Prof. Pamela Samuelson  
*IPIOP Advisory Committee*

Bruce Schneier

Prof. Paul M. Schwartz  
*IPIOP Advisory Committee*

Barbara Simons  
*Treasurer*

Robert Ellis Smith

Prof. Daniel J. Solove  
*IPIOP Advisory Committee*

Prof. Frank Tuerkheimer  
*IPIOP Advisory Committee*

Willis Ware

Paul Wolfson

David Stern  
*Executive Director,*  
*Equal Justice Works*  
*IPIOP Advisory Committee*

“  
I saw you on CNN.  
You kicked Big  
Brother’s ass. Great  
show. Thanks. – J.B.  
”

finances

*EPIC*

*Statement of Activities  
 2001, 2002 and 2003*

	<b>2001</b>	<b>2002</b>	<b>2003</b>
<b>Support and Revenue</b>			
Contributions	\$ 340,073	\$ 251,250	\$ 183,376
Grants	1,104,921	862,167	840,323
Publications	22,349	16,956	22,232
Interest Income	22,324	36,134	40,160
Other	0	(53,398)	39,602
	<hr/>	<hr/>	<hr/>
<b>Total Support and Revenue</b>	<b>\$1,489,667</b>	<b>\$ 1,110,454</b>	<b>\$ 1,125,693</b>
	<hr/>	<hr/>	<hr/>
<b>Expenses</b>			
Program	\$ 567,884	\$ 772,578	\$ 813,456
Administration	56,308	47,141	47,003
Fundraising	27,843	46,903	57,278
	<hr/>	<hr/>	<hr/>
Total Expenses	\$ 652,035	866,622	917,737
	<hr/>	<hr/>	<hr/>
Change in Net Assets	\$ 837,632	\$ 243,832	\$ 207,956
Net Assets, Jan 1	\$ 294,963	\$1,132,595	\$ 1,376,427
	<hr/>	<hr/>	<hr/>
<b>Net Assets, Dec 31</b>	<b>\$ 1,132,595</b>	<b>\$ 1,376,427</b>	<b>\$1,584,383</b>
	<hr/>	<hr/>	<hr/>

Based on report compiled by Friedman & Associates, CPA, Rockville, MD. The current EPIC form 990 is available at the EPIC website and at [www.guidestar.org](http://www.guidestar.org)



*EPIC*  
*Statement of Financial Position*  
*December 31, 2003*

**Assets**

Current Assets	\$ 727,456
Fixed Assets	31,849
EPIC Trust	<u>842,753</u>

**Total Assets** \$1,602,058

**Liabilities**

Accounts payable	<u>\$ 17,675</u>
------------------	------------------

**Total** \$ 17,675

**Net Assets**

General	\$ 98,118
Projects	643,512
EPIC Trust	<u>842,753</u>

**Total** \$1,584,383

**Total Liabilities and Net Assets** \$1,602,058

The EPIC Trust was established in memory of Paul Simons.

## supporters

*Major grants to support the work of EPIC have been received from:*

Counterpane Systems  
Earthlink  
Deer Creek Foundation  
Ford Foundation  
Fund for Constitutional Government  
Glushko Samuelson Foundation  
HKH Foundation  
W.K. Kellogg Foundation  
Irving Kohn Foundation  
Steven Leuthold Family Foundation  
Albert List Foundation  
Lutz Foundation Trust  
Markle Foundation  
Metromail Cy Pres Fund  
Nathan Cummings Foundation  
Norman Foundation  
Open Society Institute  
Red Hat Center  
Rockefeller Family Fund  
Rose Foundation  
San Francisco Foundation  
Scherman Foundation  
Simons Foundation  
Social Science, Humanities and Research Council  
Sun Hill Foundation  
Sun Microsystems  
Working Assets  
Zero Knowledge Systems

*Additional support is provided by contributions from individual donors, attorneys fees, and the sale of publications.*

“  
Enclosed is a  
donation to be used  
to generally further  
the goal of EPIC.  
I would not mind  
being sent a coffee  
mug; caffeine  
is the price of  
eternal vigilance.

– S.B.

”

## support epic

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 [www.epic.org/donate/](http://www.epic.org/donate/). Additional information about the work of EPIC is provided by the GuideStar Database at [www.guidestar.org](http://www.guidestar.org). A complete Form 990 for the current year is also available online.

*“As a former member of Congress and one who has spent much of his public life working to protect Constitutional values, I am very pleased to offer my strongest endorsement to the Electronic Privacy Information Center. EPIC is a powerful voice in Washington. I am constantly amazed by how much this dedicated group accomplishes. I urge you to join me and make a generous contribution to EPIC. Together we will help ensure that civil liberties and privacy are preserved in the Information Society.”*

—HON. JOHN ANDERSON, FORMER PRESIDENTIAL CANDIDATE



United States District Court,  
District of Columbia.

ELECTRONIC PRIVACY INFORMATION CENTER,  
Plaintiff,  
v.  
DEPARTMENT OF DEFENSE, Defendant.

No. CIV.A.02-1233 (JDB) ECF.

Jan. 16, 2003.

As you probably have heard by now, our data mining for aviation security project did not receive any FY2003 funds. My interpretation is that NASA management decided that they did not want to continue working with passenger data in order to avoid creating the appearance that we are violating people's privacy. You may have heard about the problems that JetBlue is now having after providing passenger data for a project similar to ours:

↑  
1

### EPIC Prevailed in Lawsuit Against Pentagon

When EPIC submitted a FOIA request to the Defense Department concerning the agency's new Information Awareness Office and its director, retired Admiral John Poindexter, the agency denied EPIC's request for "news media" fee status, thus imposing a substantial financial barrier to EPIC's effort to obtain responsive documents. A federal judge rejected the Pentagon's attempt to impose financial obstacles upon EPIC's requests, ruling that EPIC is entitled to "preferred fee status" under the FOIA.

↑  
2

### Millions of Records to NASA

Documents obtained by EPIC under the FOIA revealed that Northwest Airlines, in violation of the privacy policy posted on its web site, released records concerning millions of airline passengers to NASA. The information was used to conduct research into government data mining and screening systems. NASA retained the data for almost two years, and returned it to the airline only after the public outcry over a similar improper disclosure by JetBlue Airways.

Diane didn't tell me the number of CD's. When we were at NWA, they said that they gave the FBI one year's data on 6000 CD's. That would suggest that 3 months' data would fill 1500 CD's. However, the sample CD's that they gave us appear to contain one full days' data (Nov 1) on 3 CD's. Which would suggest that 90 days' data would fill 270 CD's. We'll find out next week.

Balloff: You all gave me some flight information on a general aviation plane that was getting ready to land in Ardmore, Oklahoma, and all the information was like perfect. But then I got a . . . this was a Congressional inquiry and then somebody asked me can you find out where the plane was traveling yesterday? Well, we can't really do that 'cause all we're really concerned about is what's in the air right now. Right?

← 3

### **FBI Collected A Year's Worth of Passenger Data After 9/11**

A FOIA document obtained by EPIC from NASA revealed that the FBI acquired a year's worth of passenger information from Northwest Airlines after 9/11.

The story was reported in newspapers across the country, including on the front page of *The New York Times* and in *The Washington Post* and *Wall Street Journal*.

← 4

### **Congressional Leader Used Homeland Security Resources for Political Purpose**

EPIC obtained Federal Aviation Administration transcripts and audio recordings concerning a request by the office of Congressional Leader Tom DeLay (R-TX) to track Democratic Texas legislators leaving the state by air. The state lawmakers were trying to prevent a vote on a partisan re-districting plan supported by Republicans. The FOIA information shows that FAA employees were misled into believing that the request to track the legislators was part of an official Congressional investigation.

**Complaint Summary:**

██████████ CANCELLED AT&T SERVICE ON JULY 1. HE REQUESTED AT THAT TIME THAT AT&T PUT HIS NAME ON A DO NOT CALL LIST. SINCE THEN HE HAS RECEIVED 2-3 CALLS A DAY FROM AT&T SOLICITING HIS SERVICE. HE WANTS AT&T TO PUT HIS NAME ON THE DO NOT CALL LIST AND CEASE CALLING HIM IMMEDIATELY. HE STATES THAT AT&T HAS BEEN VERY AGGRESSIVE AND HE DOES NOT APPRECIATED THE REPEATED CONTACT FROM THEIR REPRESENTATIVES.

Apparent Carrier(s): AT&T Corporation



5

### Complaints Illustrated Need for Do-Not-Call

EPIC used the FOIA to obtain complaints made by individuals to the Federal Communications Commission about telemarketers who ignore or frustrate individuals' requests to stop calling, telemarketers who become abusive or harass individuals, and the frustration that individuals experience as a result of autodialer and prerecorded voice calls. These complaints demonstrated the need for a national Do-Not-Call Registry.

The business records request is not limited to the records of the target of a full investigation. The request must simply be sought for a full investigation. Thus, if the business records relating to one person are relevant to the full investigation of another person, those records can be obtained by a FISC order despite the fact that there is no open investigation of the person to whom the subject of the business records pertain.



### **USA PATRIOT Act Allows FBI to Collect Data About Innocent People**

EPIC and allied civil liberties groups obtained information about the government's implementation of a highly controversial provision of the USA PATRIOT Act, which grants the FBI authority to request an order for business records (defined as "any tangible things") relevant to an investigation of international terrorism or clandestine intelligence activities. Among other documents, EPIC obtained an internal FBI memo acknowledging that the provision may be used to collect information about innocent people.

## OVERVIEW OF THE FOIA

The Freedom of Information Act was first passed in 1966 and subsequently strengthened after the Watergate scandal to ensure public access to information about the government's activities. More recent amendments to the law have provided preferred fee status to academic and media requesters, and allowed for expedited processing when the requester demonstrates a compelling need for the information.

### **Exemptions**

The Freedom of Information Act presumes that all government agency records must be available to the public unless specifically exempted by law. The narrow categories of records that an agency may withhold include national security information; internal agency rules; information specifically exempted by law; business information; predecisional information; law enforcement records; records of financial institutions; and oil well data.

### **Expedited Processing**

The Freedom of Information Act requires an agency to expedite processing of a request when the requester demonstrates a "compelling need" for the information. "Compelling need" includes requests where a requester primarily engaged in disseminating information demonstrates an urgency to inform the public about government activity. EPIC has made effective use of this procedure to cut through the bureaucratic delays that requesters often encounter.

ELECTRONIC PRIVACY INFORMATION CENTER

1718 Connecticut Avenue NW  
Suite 200  
Washington DC 20009  
USA

+1 202 483 1140 [tel]  
+1 202 483 1248 [fax]

[info@epic.org](mailto:info@epic.org)

**epic.org**