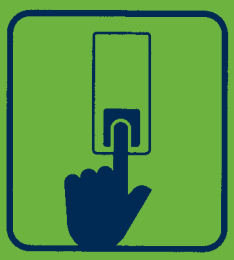
spotlight on surveillance

epic

annual report 2004–2005



CONTENTS

COVER: The Transportation Security Administration, a division of the Department of Homeland Security, has proposed the use of backscatter X-ray technology for passenger screening at several U.S. airports. The technique makes it possible to observe and record detailed images of the human body.

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, D.C., and tax-exempt under IRC section 501(c)(3). EPIC receives support from individual contributors, private foundations, the sale of publications, and legal awards. Contributions to EPIC are tax-deductible.

EPIC maintains one of the Web's most popular Internet privacy policy sites — epic.org — and publishes the online EPIC Alert every two weeks with information about emerging civil liberties issues. 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 (gilc.org), the Internet Democracy Project (internetdemocracy.org), and the Trans Atlantic Consumer Dialogue (tacd.org). EPIC maintains the Privacy Site (privacy.org) and coordinates the Public Voice coalition (thepublicvoice.org), the Privacy Coalition (privacycoalition.org), and the In Defense of Freedom coalition (indefenseoffreedom.org). EPIC also established the National Committee on Voting Integrity (votingintegrity.org).

the architectures of surveillance reform(ed)

There is a scene in "Terminator 2: Judgment Day" where the menacing T-1000, a shape-shifting cyborg, is struck by a rifle blast. Its metallic body is blown to little pieces, and silver beads are strewn across the dark, asphalt street. But then, like mercury from a broken thermometer on a kitchen table, the silver globules join together and the cyborg is reformed.

So, it seemed appropriate that shortly after we celebrated the end of John Poindexter's Total Information Awareness, the defeat of the National ID card, and the collapse of the state-based MATRIX database, that we should look more closely at what happens to the architectures of surveillance when they are hit by the force of public opposition.

In this edition of EPIC's annual report, we share with you our successes from the past year as well as our ongoing efforts to identify and respond to emerging challenges to civil liberties.

We also look more closely at some of the new techniques of surveillance that are being formed around us. They are no longer called "Carnivore" or "Total Information Awareness," but they may be just as far-reaching.

Under our banner "Spotlight on Surveillance," EPIC has taken a particular interest in the research agenda of the Department of Homeland Security. It would be too easy to say that the agency is quickly becoming "Big Brother's laboratory." But it would be a start.

The featured items in this year's annual report examine video surveillance, border monitoring, passenger screening, biometric identification, visitor profiling, and new

"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.

techniques that literally allow the government to strip naked a person suspected of no crime. Much of the initiative and funding for these programs have come from the Department of Homeland Security and the Transportation Security Administration.

Many have discussed the need to "connect the dots" to prevent future terrorist acts. But we should also consider what happens when the enormous surveillance capabilities of the government are joined together.

This is not a debate that occurs in the abstract. Documents should be obtained from government agencies and disclosed to the public to promote informed decisionmaking. Indications of abuse should be investigated. Congressional oversight committees should ask tough questions of agency heads. Judges should determine whether proposals comply with both legal and Constitutional safeguards. (Already the Department of Homeland Security seems on course to break new records for exceptions to Privacy Act obligations.) And the public must ultimately decide what price it will pay for the sense of security.

Through EPIC's litigation, research, open government efforts, and advocacy, we hope to contribute to this debate.

"Terminator 2" ends with the destruction of the T-1000. But it took more than a single rifle shot. And it will take far more work to restore public control over the new architectures of surveillance.

MARC ROTENBERG
President
Electronic Privacy Information Center

epic program

FREE SPEECH

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

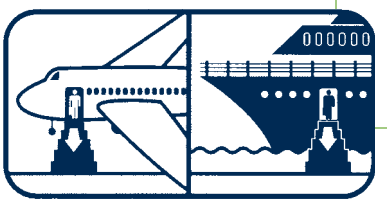
"The most participatory form of mass speech yet developed." That is how Judge Stewart Dalzell described the Internet in the landmark court decision striking down online censorship. As a leading publisher of policy materials covering the Internet, EPIC joined with other civil liberties and computer industry 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.

In 2004, EPIC focused on the most recent challenge to anonymity in a case before the Supreme Court, opposing a state law that permitted the arrest of a person who failed to provide his identity.

OPEN GOVERNMENT

"EPIC keeps tabs on those who are keeping close tabs on us, and on important legal issues." — SAN DIEGO UNION-TRIBUNE

In 2004, the American Library Association presented the James Madison Award to EPIC. The ALA cited EPIC's use of the Freedom of Information Act to make public government records concerning the FBI's Carnivore surveillance system and disclosures of airline passenger data. The James Madison Award honors "those who have championed, protected, and promoted public access to government information and the public's right to know." See EPIC's FOIA Gallery *(epic.org/opengov/foiagallery)* for highlights of EPIC's FOIA work.



BORDER SURVEILLANCE

"America's Shield" is estimated to cost $2 billion through 2010, but the border security program's aging sensor equipment wastes time and money because it cannot distinguish between humans and animals.

PRIVACY

"EPIC filed a complaint with the U.S. Department of Transportation's Office of Aviation Enforcement and Proceedings, and accused [Northwest] airline of violating its own privacy policy." — THE WASHINGTON TIMES

Passenger profiling. Data mining. Radio Frequency Identification. Biometric identifiers. Surveillance cameras. These and many other technologies 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. EPIC is frequently called upon by Congressional committees and government agencies to identify privacy risks and develop 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. The EPIC site is the central resource for the ongoing debate about the future of privacy, and many of its Web pages on key privacy topics are the highest ranked by search engines.

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 organizations 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.

"Thanks for your good efforts supporting our privacy rights." – J.D.

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 Buenos Aires, Dubai, Hong Kong, Honolulu, Ottawa, Paris, Washington, and Wroclaw.

In 2004, EPIC worked in close association with the Public Interest Registry, the managers of the .org domain, to promote the noncommercial use of the Internet, to ensure strong technical management of the domain, to develop good privacy safeguards, to support public participation and transparency, and to encourage the adoption of International Domain Names. In December 2004, EPIC and PIR sponsored a Public Voice event in Cape Town, South Africa.

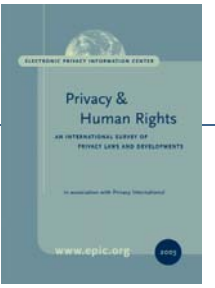
"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor or reputation. Everyone has the right to the protection of law against such interference or attack."

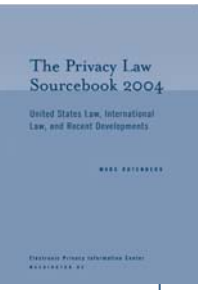
— ARTICLE 12, UNIVERSAL DECLARATION OF HUMAN RIGHTS

"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





EPIC's FOIA Manual — "Deserves a place in the library of everyone who is involved in, or thinking about, litigation under the Freedom of Information Act."

— STEVE AFTERGOOD, FEDERATION OF AMERICAN SCIENTISTS

EPIC's Privacy Sourcebook — "A handy compilation of privacy law instruments and a 'must' for anyone seeking guidance about the location and content of the key statutes, treaties, and recent developments." — AMERICAN SOCIETY OF INTERNATIONAL LAW

"The 'Physician's Desk Reference' of the privacy world." — EVAN HENDRICKS, PRIVACY TIMES

EPIC produces several publications each year that are popular among policymakers, 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)*. Discounts for multiple copies are available 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 more than sixty countries around the world. The survey examines a wide range of privacy issues, including data protection, telephone tapping, genetic databases, e-voting, RFID, ID systems and freedom of information laws.

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.

Reports from EPIC

Privacy Self-Regulation: A Decade of Disappointment. (2005)

WATCHING THE WATCHERS: Paying for Big Brother: A Review of the Proposed FY2003 Budget for the Department of Justice. (2002)

WATCHING THE WATCHERS: Your Papers, Please: From the State Drivers License to a National Identification System. (2002)

Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. (2000)

Surfer Beware III: Privacy Policies without Privacy Protection. (1999)

Surfer Beware II: Notice is Not Enough. (1998)

Critical Infrastructure Protection and the Endangerment of Civil Liberties: An Assessment of the President's Commission on Critical Infrastructure Protection. (1998)

Surfer Beware: Personal Privacy and the Internet. (1997)

Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet. (1997)

epic in congress

PASSENGER PROFILING

"The Transportation Security Administration is being investigated after it admitted to collecting and maintaining, through its Secure Flight program, detailed data about thousands of travelers in violation of the Privacy Act."

"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

In 2004, EPIC appeared before several Congressional committees to provide expert testimony on critical privacy and civil liberties issues. EPIC also worked in coalition with other organizations to draw attention to emerging problems, such as spyware, RFID tags, and voting privacy.

Medical Record Privacy

In testimony before the National Committee on Vital and Health Statistics, the official advisory body to the Secretary of Health and Human Services, EPIC discussed the need to improve protection for health information as it moves through the banking system. EPIC argued that banks should not be exempt from the requirements of the HIPAA Privacy Rule and that health information flowing through the banking transaction network should be encrypted.

Airline Passenger Profiling

In March 2004, EPIC testified on the CAPPS II airline passenger screening system before the House Aviation Subcommittee. EPIC warned the committee that there was reason to doubt whether the CAPPS II passenger profiling system could ever function in a manner that protects privacy and provides citizens with basic due process rights. A subsequent report from the Government Accountability Office supported EPIC's position.

The 9/11 Commission

In July 2004, the 9/11 Commission released the final report on Terrorist Attacks Upon the United States. EPIC had testified before the Commission on "Security and Liberty: Protecting Privacy, Preventing Terrorism" in December 2003. Several of EPIC's recommendations were incorporated into the 9/11 report.

Social Security Numbers

In June 2004, EPIC recommended protections for the Social Security Number in testimony to the House Ways and Means Subcommittee on Social Security. EPIC argued that Congress should create legislative protections for the SSN.

In September 2004, EPIC testified before the House Energy and Commerce Subcommittee on Consumer Protection regarding Social Security Numbers. EPIC urged Congress to pass legislation that limits use and dissemination of the SSN in both the public and private sectors. In light of recent security breaches at commercial data brokers, the legislation has been reintroduced and is being considered for passage again.

"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.

RFID — Wireless ID Tags

In July 2004, EPIC proposed comprehensive privacy protections for Radio Frequency Identification in testimony before the House Energy and Commerce Subcommittee on Consumer Protection. EPIC urged Congress to adopt a framework of Fair Information Practices to govern collection and use of personal information obtained through RFID tags and devices.

EPIC also appeared before the Federal Trade Commission in 2004 to recommend the adoption of strong privacy guidelines to protect consumers against potential abuses of the tracking technology.

Spyware and Wireless Directory

In September 2004, EPIC appeared before the Senate Commerce Committee to testify on two bills intended to provide privacy protections against spyware and to prohibit wireless carriers from publishing subscribers' phone numbers in wireless directories without their consent. In the same month, EPIC testified before the same Committee on the need to establish privacy safeguards for wireless phone subscribers.

Voting Privacy

In September 2004, EPIC testified before the Election Assistance Commission Technical Guidelines Development Committee on the impact that new voting technology would have on the privacy rights of voters. EPIC made specific recommendations on standards for election systems and voting technology. The committee is expected to make recommendations to the full Election Assistance Commission in 2005.

litigation

US-VISIT SCREENING

This database records the biographic, biometric and travel information of more than 28 million foreign visitors to the United States each year but Privacy Act safeguards do not apply.

"A name is now no longer a simple identifier: it is the key to a vast, cross-referenced system of public and private databases, which lay bare the most intimate features of an individual's life. If any person can be coerced by the state to hand over this key to the police, then the protections of the Fourth and Fifth Amendments have been rendered illusory."

— EPIC AMICUS BRIEF IN HIIBEL V. SIXTH JUDICIAL DISTRICT COURT (US 2004)

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.

"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.

IDENTIFICATION REQUIREMENTS — Hiibel v. Sixth Judicial District Court of Nevada (Amicus)

This case before the U.S. Supreme Court arose from the arrest of Larry Hiibel under a Nevada law that allows an officer to arrest a person who appears suspicious and fails to identify himself. EPIC filed an amicus brief describing how government databases, such as the National Crime Information Center (NCIC) and the Multi-State Anti-Terrorism Information Exchange (MATRIX), give police officers access to far more information than was previously available. EPIC urged the court to ensure that the police do not use stop-and-frisk situations for fishing expeditions of government computer databases.

In a narrow 5–4 opinion, the Supreme Court upheld the Nevada law. Justice Anthony Kennedy's majority opinion noted, however, "[a]s we understand it, the statute does not require a suspect to give the officer a driver's license or any other document. Provided that the suspect either states his name or communicates it to the officer by other means — a choice, we assume, that the suspect may make — the statute is satisfied and no violation occurs."

INFORMATION BROKERS — EPIC v. FBI

In August 2004, a federal judge in Washington, D.C., directed the FBI to release documents, sought by EPIC, concerning Choicepoint, a major information broker. The FBI had claimed that the documents were exempt from the FOIA, citing national security concerns. The court also rejected the FBI's request for a two-year delay for review of the documents.

PASSENGER PROFILING — EPIC v. TSA

In August 2003, EPIC requested from the Transportation Security Administration materials that the agency had prepared on the controversial Computer Assisted Passenger Profiling System (CAPPS II). TSA agreed to process the documents, but failed to respond to EPIC's request for expedited processing. Though EPIC applied for an emergency court order, TSA refused to release the documents, claiming that they were exempt from disclosure under the Freedom of Information Act. In June 2004, Judge Colleen Kollar Kotelly ordered TSA to review the documents for material that is factual and thus must be released under the FOIA. TSA released portions of three privacy impact assessments reflecting a dramatic expansion over just three and a half months in the ways passenger information collected for CAPPS II would have been shared.

PASSENGER PROFILING — EPIC v. NASA

Following a FOIA request in 2003, EPIC obtained documents revealing that Northwest Airlines disclosed millions of passenger records to NASA for use in data mining and passenger profiling research. But the agency withheld some documents that were responsive to EPIC's request. EPIC filed suit in January 2004 to obtain additional documents about the Northwest disclosure. Through negotiation, EPIC obtained hundreds of additional records from NASA.

PASSENGER PRIVACY — EPIC v. Northwest Airlines

Based on documents obtained from NASA under the Freedom of Information Act, EPIC filed a complaint against Northwest Airlines with the Department of Transportation, alleging that Northwest committed an unfair and deceptive trade practice by disclosing millions of passenger records to NASA in violation of the airline's publicly posted privacy policy. However, the Department eventually held that this was not an unfair or deceptive trade practice.

FREE SPEECH — Ashcroft v. ACLU

EPIC was co-plaintiff and co-counsel in the second challenge to efforts by Congress to limit free speech on the Internet. This case attacked the constitutionality of the Children's Online Privacy Protection Act, a law that would have required commercial Web site operators to "card" Web patrons before providing access to information that some communities might deem "harmful to minors." In June 2004, the Supreme Court found that the government has not shown that there are no "less restrictive alternatives" to COPPA, and that "there is a potential for extraordinary harm and a serious chill upon protected speech" if the law goes into effect.

PATRIOT ACT — ACLU and EPIC v. DOJ

In October 2003, EPIC, the ACLU, and allied library and booksellers' organizations submitted a FOIA request to the FBI seeking information about the agency's enforcement of Section 215 of the USA PATRIOT Act. When the FBI denied expedited processing, EPIC and the ACLU filed suit in federal court seeking the immediate release of the requested records. In May 2004, Judge Ellen Huvelle ordered the FBI to expeditiously process the request. Judge Huvelle also determined that "EPIC is indeed 'primarily

engaged in disseminating information' for the purposes of expediting [a FOIA] request." Records were released in June and July showing the government's interpretation and use of Section 215.

DNA PRIVACY — Maryland v. Raines (Amicus)

This case challenged the Maryland DNA Collection Act, which allows the state to collect DNA from individuals who have committed felonies and certain misdemeanor offenses. Profiles of the DNA are then added to a state DNA database, which feeds into a national DNA database that is maintained by the FBI. Charles Raines argued that compelled DNA production constitutes an unreasonable search and seizure in violation of the Fourth Amendment and the Constitution of Maryland. EPIC submitted an amicus brief arguing that in many areas Maryland provides stronger privacy protection than the federal Fourth Amendment. EPIC also rebutted the government's claim that DNA collection is no different than fingerprint collection. In July 2004, however, the court upheld the Maryland DNA collection law.

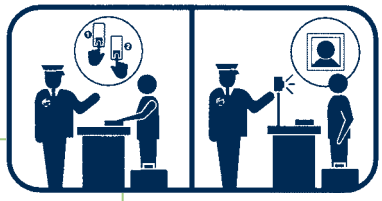
DNA PRIVACY — United States v. Kincade (Amicus)

In this case, the United States Court of Appeals for the Ninth Circuit reheard its prior decision that the compelled production of a DNA sample from a parolee for inclusion in a nationwide DNA database is an unlawful search. This case involved the Fourth Amendment protections against unreasonable government search and seizure and law enforcement accumulation and use of personal information. EPIC filed a "friend of the court" brief that focused on the false notion that DNA and fingerprinting involve the same privacy concerns. In a close 6–5 ruling in August 2004, the court determined that a parolee can be forced to provide a DNA sample for the FBI's vast national DNA database.

DRIVERS PRIVACY — Kehoe v. Fidelity Bank (Amicus)

In September 2004, EPIC filed an amicus brief in Kehoe v. Fidelity Bank, a case under the federal Drivers Privacy Protection Act where a bank purchased over 500,000 motor vehicle records from Florida for junk mail solicitations. The brief argued that individuals are entitled to damages under the law when businesses or data brokers intentionally access motor vehicle information. The 11th Circuit is still considering the case.

agency proceedings



GOVERNMENT ID CARDS

The Department of Homeland Security's new employee access card includes wireless technologies that leave cardholders' personal information vulnerable to criminals.

"Once a biometric identifier has been compromised, there can be severe consequences for the individual whose identity has been affected. It is possible to obtain a new credit card or a Social Security number, but how does one replace a fingerprint, voiceprint, or retina?" — EPIC COMMENTS TO TRANSPORTATION SECURITY ADMINISTRATION ON BIOMETRIC IDENTIFIERS

In 2004, EPIC participated in a wide range of agency proceedings. The topics ranged from traditional privacy concerns, such as the misuse of Social Security numbers and marketing practices, to new issues, including online identification, air travel privacy, biometrics and the WHOIS database, which contains personal imformation on people who register Internet domain names.

Children's Online Privacy

EPIC challenged the Federal Trade Commission to enforce the children's privacy law against Amazon. EPIC and several other privacy organizations recommended that the FTC pursue an investigation of Amazon.com under the Children's Online Privacy Protection Act because its "Toy Store" Web site targets children and collects personal information.

Census Data for Law Enforcement Purposes

EPIC's disclosure of the link between a request from the Department of Homeland Security and the Census Bureau lead to a change in Census policy. The Census Bureau announced that it will no longer provide special tabulations on "sensitive populations" to law enforcement or intelligence agencies unless senior Census Bureau officials approve such disclosure. The policy change follows a public outcry in response to documents obtained by EPIC under the Freedom of Information Act revealing that the Census Bureau provided the Department of Homeland Security demographic information about individuals of Arab American ancestry.

Data Brokers

In December 2004, EPIC urged the Federal Trade Commission to investigate Choicepoint and other data brokers for compliance with the federal Fair Credit Reporting Act. In 2005, the FTC confirmed that it is acting on EPIC's petition and is investigating Chiocepoint.

Do-Not-E-mail Registry

EPIC submitted comments to the Federal Trade Commission in support of the creation of a Do-Not-E-mail Registry. The registry, if created, would serve the same role that the current Do-Not-Call Registry does in protecting consumers from unwanted solicitations by telemarketers.

Spam

In April 2004, EPIC filed comments with the Federal Communications Commission advocating opt-in protections against "mobile service commercial messages," or spam that is sent to cellular phones and other wireless devices. The FCC ultimately ruled that marketers cannot send commercial e-mail to wireless devices without the explicit consent of the consumer, a much stronger protection against spam than that provided by the CAN-SPAM Act passed by Congress in 2003.

"The agency also wishes to acknowledge the Electronic Privacy Information Center, which filed a complaint about Consumerinfo.com with the commission." – Federal Trade Commission, 2005

Air Travel Privacy

EPIC called upon the Transportation Security Administration to suspend the test phase of Secure Flight until the program's significant privacy issues are resolved and the government is willing to be more forthcoming about the program's details. EPIC also urged the Office of Management and Budget not to permit TSA to collect a month's worth of passenger information for Secure Flight testing purposes until the program's privacy and transparency issues are addressed.

US-VISIT—Border Screening

EPIC filed two sets of comments concerning the implementation of the United States Visitor and Immigrant Status Technology program. EPIC urged the Department of Homeland Security to define how Privacy Act obligations affect US-VISIT, to consider the significance of international privacy standards in the collection and use of personal information by the agency on non-U.S. citizens, and to prohibit the expansion of US-VISIT uses outside the program's defined mission.

Biometric Identifiers

EPIC filed comments in response to the announcement that the Arrival Departure Information System would begin to collect biometric and biographic data for use by the United States Visitor and Immigrant Status Technology program. EPIC argued that ADIS should not be exempt from Privacy Act requirements and urged the Department of Homeland Security to reduce ADIS's proposed 100-year data retention period and comply with international privacy standards.

Government ID Cards

EPIC urged the Transportation Security Administration to tightly safeguard personal information in the Transportation Workers Identification Credentialing System and the Transportation Security Threat Assessment System. These systems compile data on a variety of people directly and indirectly related to the transportation industry. EPIC's comments noted the dangers of identity theft and the risks of misappropriation and mission creep if the data collected for these programs are not properly protected.

Internet Telephony

EPIC filed comments urging the Federal Communications Commission to reject the request of federal law enforcement agencies to expand the Communications Assistance for Law Enforcement Act to cover Internet Service Providers and "Voice over IP" services. Such an expansion contravenes Congressional intent, and would allow law enforcement to capture information on non-suspects. Further, law enforcement agencies have not demonstrated a need for expanding CALEA.

IPv6 Deployment

EPIC filed comments with the Department of Commerce urging the use of strong privacy technologies in IPv6, the protocol designed to replace the current Internet protocol. EPIC recommended that all IPv6 vendors make standard privacy and security enhancing features such as encryption. EPIC also warned that IPv6 should not be subject to the Communications Assistance for Law Enforcement Act, as this would threaten both the security of network communications and the stability of the network architecture.

Auto Travel Privacy

EPIC urged the National Highway Transportation Security Administration to create privacy protections for "Event Data Recorders," black boxes in vehicles that record crash data. EPIC noted that the boxes can become platforms for broader surveillance and that information collected by these devices should be subject to fair information practices.

SSN

In comments to the Social Security Administration, EPIC urged the agency not to permit the use of the Social Security Number for state voter registration purposes. EPIC said that state election administrations must first agree not to require voters to present their Social Security cards in order to vote in federal elections.

Opt-out Notice to Consumers

EPIC comments to the Federal Trade Commission urged that federal regulation of financial services companies should include the creation of clear, simple privacy notices and user-friendly opt-out procedures.

internet public interest opportunities program

"It's been a really great experience. The level of organization and meaningful tasks and speakers has been amazing... The fellow clerks were absolutely fantastic... Drafting the litigation memos was particularly interesting... The legislative work — attending hearings, conducting research, preparing testimony, and proposing legislative fixes — was terrific and provides an insight in law, policy, and the legislative process that cannot be gained at school.... Best organized job/internship I've ever had (and I've had a lot).... This has been such a tremendous opportunity for us. Thank you!" — 2004 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. Summer and school semester internships are available for outstanding law students with a strong interest in civil liberties issues relating to the Internet, particularly free speech, privacy, open government, and democratic governance. The program promotes opportunities for law school students to work on public interest issues concerning the future of the Internet. IPIOP also gives law students the opportunity to actively participate in valuable programs in Internet law, policy, and legislation. Washington, D.C. provides an ideal location for an introduction to Internet law and policy. IPIOP clerks attend agency proceedings, policy meetings, and 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 goal of the program is to provide opportunities for clerks to experience first-hand the new and exciting intersection between Internet law and public policy.

LEGISLATION

The legislative process is the critical opportunity for public interest organizations to make a case directly to lawmakers, to engage in discussion about the details of proposed legislation, and to establish connections with critical committees and decisionmakers. IPIOP clerks learn about this crucial process by researching and drafting memoranda on critical issues before Congress and by attending hearings.

GOVERNMENT OVERSIGHT

The Freedom of Information Act 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 on a current Internet issue to one of many governmental agencies. Clerks also assist in litigating pending FOIA matters.

LITIGATION

Clerks assist EPIC staff in developing litigation strategies in key cases with significant impact on critical Internet issues. Clerk activities include drafting memoranda, attending meetings with attorneys, and attending court hearings.

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 the work of EPIC are also encouraged to seek fellowships through Equal Justice Works (*equaljusticeworks.org*).

APPLICATIONS

Submit a letter of interest, a writing sample, a résumé, and a recommendation letter to: IPIOP Coordinator, EPIC, 1718 Connecticut Ave. NW, Suite 200, Washington, D.C. 20009 or e-mail *ipiop@epic.org*. The process is competitive. More than 300 applications were received for last year's program.

epic affiliated sites

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

— GOVERNING MAGAZINE

In 2004, EPIC celebrated its tenth anniversary with the conference "Freedom 2.0: Distributed Democracy, Dialogue for a Connected World" and the launch of the EPIC04.ORG Web site. The site features materials on democracy, transparency, privacy and the Public Voice.

EPIC Bookstore

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 featured titles from each issue of the EPIC Alert newsletter.

Global Internet Liberty Campaign (GILC)

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 Internet for users everywhere.

In Defense of Freedom (IDOF)

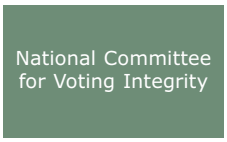
indefenseoffreedom.org

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.

Internet Free Expression Alliance (IFEA)

ifea.net

IFEA was established to ensure the continuation of the Internet as a forum for open, diverse and unimpeded expression and to maintain the vital role the



Internet plays in providing an efficient and democratic means of distributing information around the world.

Privacy International (PI)

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

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

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 Buenos Aires, Cape Town, Dubai, Hong Kong, Honolulu, Ottawa, Paris, Washington, and Wroclaw.

National Committee for Voting Integrity

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

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.

finances

EPIC
STATEMENT OF ACTIVITIES
2001, 2002, 2003 AND 2004

	2001	2002	2003	2004
Support and Revenue				
Contributions	$ 340,073	$ 251,250	$ 183,376	$ 380,205
Grants	1,104,921	862,167	840,323	840,473
Publications	22,349	16,956	22,232	20,319
Interest Income	22,324	36,134	40,160	45,768
Other	0	(53,398)	39,602	(5,171)
Total Support and Revenue	$ 1,489,667	$ 1,110,454	$ 1,125,693	$ 1,332,044
Expenses				
Program	$ 567,884	$ 772,578	$ 813,456	$ 933,864
Administration	56,308	47,141	47,003	66,831
Fundraising	27,843	46,903	57,278	25,461
Total Expenses	$ 652,035	866,622	917,737	1,025,976
Change in Net Assets	$ 837,632	$ 243,832	$ 207,956	$ 306,068
Net Assets, Jan 1	$ 294,963	$ 1,132,595	$ 1,376,427	$ 1,584,383
Net Assets, Dec 31	$ 1,132,595	$ 1,376,427	$ 1,584,383	$ 1,890,451

Based on report compiled by Friedman & Associates, CPA, Rockville, MD. The current EPIC form 990 is available at the EPIC Web site and at **www.guidestar.org**

EPIC
STATEMENT OF FINANCIAL POSITION
DECEMBER 31, 2004

Assets		
Current Assets	$1,332,000	
Fixed Assets	25,690	
EPIC Trust	552,504	
Total Assets		$ 1,910,194
Liabilities		
Accounts payable	$ 19,743	
Total		$ 19,743
Net Assets		
General	$ 704,318	
Projects	633,629	
EPIC Trust	552,504	
Total		$1,890,451
Total Liabilities and Net Assets		$ 1,910,194

The EPIC Trust was established in memory of Paul Simons.

EPIC STAFF

Marc Rotenberg
Executive Director

David L. Sobel
General Counsel

Lillie Coney
Associate Director

Chris Jay Hoofnagle
EPIC West Director

Cedric Laurant
Policy Counsel

Marcia Hofmann
Staff Counsel

Frannie Wellings
Policy Fellow

Melissa Ngo
Staff Counsel

H. Kate Rears
Administrative Director

Ula Galster
International Policy Fellow

Katitza Rodríguez Pereda
International Policy Fellow

R. P. Ruiz
Technology Fellow

Wayne Madsen
Senior Fellow

Anna Slomovic
Senior Fellow

Stephanie Perrin
Senior Fellow

Harry Hammitt
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
UCLA Department of Information Studies

Prof. Anita Allen-Castellitto
University of Pennsylvania Law School
IPIOP Advisory Committee

Hon. John Anderson
World Federalist Association

Prof. Ann Bartow
University of South Carolina School of Law
IPIOP Advisory Committee

Prof. Francesca Bignami
Duke Law School
IPIOP Advisory Committee

Prof. Christine Borgman
UCLA Department of Information Studies

Prof. James Boyle
Duke Law School
IPIOP Advisory Committee

David Burnham
Transactional Records Access Clearinghouse

Vinton G. Cerf
MCI

Dr. David Chaum

Prof. Julie E. Cohen
Georgetown University Law Center
IPIOP Advisory Committee

Simon Davies
Privacy International

Whitfield Diffie
Sun Microsystems
Board Member

Prof. David Farber
University of Pennsylvania Department of Computer and Information Science

Hon. David Flaherty
former Information and Privacy Commissioner, British Columbia

Prof. Oscar Gandy
Annenberg School for Communication
University of Pennsylvania
Chair

Austin Hill
Zero-Knowledge Systems

Deborah Hurley
Secretary

Prof. Jerry Kang
UCLA Law School

Judith Krug
American Library Association
IPIOP Advisory Committee

Prof. Gary Marx
Massachusetts Institute of Technology

Mary Minow
LibraryLaw.com

Peter G. Neumann
SRI International
Board Member

Prof. Eli Noam
Columbia Institute for Tele-Information

Prof. Anita Ramasastry
University of Washington Law School
IPIOP Advisory Committee

Prof. Pamela Samuelson
University of California-Berkeley, School of Information Management and Systems; School of Law
IPIOP Advisory Committee

Bruce Schneier
Counterpane Internet Security, Inc.

Prof. Paul M. Schwartz
Brooklyn Law School
IPIOP Advisory Committee

Barbara Simons
Association for Computing Machinery
Treasurer

Robert Ellis Smith
Privacy Journal

Prof. Daniel J. Solove
George Washington University Law School
IPIOP Advisory Committee

Prof. Frank Tuerkheimer
University of Wisconsin Law School, Madison
IPIOP Advisory Committee

Edward G. Viltz
Public Interest Registry

Dr. Willis Ware
RAND Corporation

Paul Wolfson
Wilmer Cutler Pickering LLP

(affiliations are for identification)

supporters

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

Bauman Foundation
Counterpane Systems
Earthlink
Ford Foundation
Fund for Constitutional Government
Glushko-Samuelson Foundation
HKH Foundation
W.K. Kellogg Foundation
Irving Kohn Foundation
Albert List Foundation
Lutz Foundation Trust
Markle Foundation
Metromail Cy Pres Fund
Norman Foundation
Omidyar Network
Open Society Institute
Quixote Foundation
Red Hat Center
Rockefeller Family Fund
Rose Foundation
Scherman Foundation
Simons Foundation
Sun Hill Foundation
Sun Microsystems
Sydney Stern Memorial Trust
Working Assets
Zero Knowledge Systems

Additional support is provided by contributions from individual donors, attorneys fees, cy pres funds 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

"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

EPIC needs your support. EPIC receives no federal funding, and contributions are welcome and fully tax-deductible. Checks/money orders should be made out to "EPIC" and sent to 1718 Connecticut Ave. NW, Suite 200, Washington, D.C. 20009. EPIC accepts online donations at *epic.org/donate/*.

Additional information about the work of EPIC is provided by the GuideStar Database at *www.guidestar.org*. A complete Form 990 for the current year is also available online.




ELECTRONIC PRIVACY INFORMATION CENTER

1718 Connecticut Avenue NW

Suite 200

Washington DC 20009 USA

T: 202 483 1140

F: 202 483 1248

epic-info@epic.org

epic.org