

Classified by SP  
Declassify on: OADR

REPRODUCTION CONTAINS  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

Dep. Dir. \_\_\_\_\_  
DD Adm. \_\_\_\_\_  
DD Inv. \_\_\_\_\_  
Asst. Dir.:

- Adm. Servs. \_\_\_\_\_
- Crim. Inv. \_\_\_\_\_
- Ident. \_\_\_\_\_
- Info. Mgnt. \_\_\_\_\_
- Insp. \_\_\_\_\_
- Intell. \_\_\_\_\_
- Lab. \_\_\_\_\_
- Legal Coun. \_\_\_\_\_
- Tech. Servs. \_\_\_\_\_
- Training \_\_\_\_\_
- Cong. Affs. O. \_\_\_\_\_
- Off. of EEO \_\_\_\_\_
- Off. Liaison & \_\_\_\_\_
- Int. Affs. \_\_\_\_\_
- Off. of Public \_\_\_\_\_
- Telephone Rm. \_\_\_\_\_
- Director's Off. \_\_\_\_\_



ANNUAL REPORT

# epic2001

**Sed quis custodiet ipsos custodes?**

But who will watch the watchers?



## mission & programs

The Electronic Privacy Information Center is a public interest research center in Washington, DC. It was established in 1994 to focus public attention on emerging 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 is tax-exempt under IRS section 501(c)(3). EPIC receives support from individual contributors, private foundations and companies. 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 news about important Internet issues, new publications, and upcoming events. EPIC also publishes *Privacy and Human Rights*, *Cryptography and Liberty*, *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 (**gildc.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 Privacy Coalition (**privacypledge.org**) and the In Defense of Freedom coalition (**indenseoffreedom.org**).

# in defense of freedom

## **Defending Civil Liberties After September 11**

September 11 was a bright, sunny day in Washington, DC. On that day, when we would normally gather for the staff meeting in our conference room in our offices in Dupont Circle, a few blocks from the White House, the TV was on. We were watching CNN. We were watching the World Trade Center billowing smoke. We watched the plane fly into the second tower; and then a little while later, we watched the towers collapse.

That same day, from our office overlooking Connecticut Avenue, we looked out on the street and saw federal employees leave Washington. For several hours, cars moved slowly up the street, and then later in the day, no cars at all. A strange silence fell on the city. No sounds from Reagan National Airport because all air travel in the United States had been suspended. Then a new sound that we heard increasingly in the weeks that followed: the sound of helicopters overhead, the sound of sirens on the street.

We received many calls from the media after September 11. Reporters asked, "What is the future of privacy in America?" "What is the future of civil liberties?" "How are we to balance freedom with the need for public safety?" We couldn't say anything at that point. There was a shock and a numbness that anyone who was in Washington on that day probably still feels today.

The week of September 11 was also the week that the Senate took up the annual budget request from the Department of Justice. If we had met on that Tuesday morning, we would have discussed the provisions contained in the funding measure that might raise privacy concerns—allocations for new systems of surveillance, new database proposals, new investigative authority—that we would, as routine, try to assess in light of our constitutional traditions and legal protections.

One of the Senators said the country must move quickly to provide new tools to law enforcement to ensure that the horrors of September 11 are never repeated. He urged rapid adoption of new authorities for the police and new restrictions on civil liberties. But the Chairman of the

Senate Judiciary Committee Patrick Leahy offered a warning. Senator Leahy said, "We must proceed at this time very carefully. We have been faced with a great challenge, and this challenge can either coarsen us or it can harden our resolve to protect those things that we value: the system of government, the rule of law, the right of individual freedom that we cherish."

The next day the New York Times asked this question: "If the idea takes root that civil liberties should not be permitted to stand in the way of a war on terrorism, at what point do security measures start to corrode the very society they are designed to protect?"

And in the days that followed a new coalition formed in Washington. Civil libertarians, religious leaders, educators, Arab-Americans, experts in Immigration law gathered in defense of freedom. We issued a statement that said, "we need to ensure that actions by our government uphold the principles of a democratic society, accountable government, and international law, and that all decisions are taken in a manner consistent with the Constitution." More than 150 organizations, across the political spectrum, 300 law professors, and 40 leading computer scientists endorsed the statement.

In the legislative debate that followed there were some victories. New oversight mechanisms were established for "Carnivore," an Internet sniffing program that captures electronic traffic that could be used covertly, arguably in violation of electronic surveillance laws. There was a critical sunset provision, at least for some electronic surveillance powers.

Reporters asked,  
"What is the future of  
privacy in America?"

"If the idea takes  
root that civil liberties  
should not be permitted  
to stand in the way  
of a war on terrorism,  
at what point do security  
measures start to  
corrode the very society  
they are designed  
to protect?"

—THE NEW YORK TIMES

"We need to ensure that actions by our government uphold the principles of a democratic society, accountable government, and international law, and that all decisions are taken in a manner consistent with the Constitution."

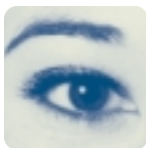
— IN DEFENSE OF FREEDOM

We have too often framed this debate as one involving a balance between security and liberty. But democratic government doesn't work that way. Constitutional democracies do not prosper on that idea.

But there were also defeats. In many critical respects, the U.S. law on electronic surveillance tries to discourage by all possible means this highly intrusive technique. As Justice Brandeis described in his famous 1928 *Olmstead* dissent, writs of assistance and general warrants are but puny means of tyranny when compared to electronic surveillance. The reference is significant—it was the writs of assistance and the general warrants that led the framers of the Bill of Rights to draft the Fourth Amendment.

And so an authority that was once in the words of Congress "an investigative method of last resort" now was looked to as the primary means in the war against terrorism. The standard of proof was reduced, the role of the judiciary was diminished, the means of oversight were curtailed, and this at a time when the technological explosion has made possible forms of surveillance that not even a few years ago could have been imagined.

Also, the Attorney General released a memorandum regarding the Freedom of Information Act, saying that no longer will federal agencies be required to follow the foreseeable harm test, but rather if they have a sound legal basis for withholding public documents that's satisfactory, the Department of Justice will back them up. He also announced that in his opinion it is appropriate for the Department of Justice to intercept confidential communications between lawyer and client in certain circumstances.



You may think we would be discouraged. But this is the work of democracy. We don't have the time, the luxury, or the opportunity to be discouraged. If there are going to be 1,200 people detained without indictment, without trial, post-September 11, then we have the right to know who they are and what the legal basis is for that detention. So EPIC will litigate a Freedom of Information Act case to determine the status of these 1,200 plus detainees.

And if the President of the United States is going to write to the president of the European Union, the Belgian Prime Minister Mr. Verhoefstadt, and recommend that the Europeans modify their privacy laws so as to facilitate law enforcement access to private communications, then EPIC and other NGOs in the United States and Europe are going to join together and write to Mr. Verhoefstadt about the importance of safeguarding the privacy rights of all citizens even after September 11.

And if military tribunals are going to be established, then Senator Leahy once again stands up in the Senate and reminds the White House that if we are trying to build democratic institutions around the world, then for us to allow the use of secret trials, secret evidence and summary judgments will undermine democracy around the world.

And if there's going to be a proposal for a national ID card without a substantive legal basis, without assessment of cost or effectiveness, then EPIC will go to the steps of the U.S. Capitol, with paper identity documents and paper shredders, and lead a "shred-in."

One of my first thoughts on September 11 was Benjamin Franklin's remark, "Those that would sacrifice essential liberty for temporary security deserve neither liberty nor security." I thought of Franklin's words many times since September 11, but in the days following the 11th, they seemed too harsh. They did not comfort families, they did not make people feel safer. But Franklin was right. We have too often framed this debate as one involving a balance between security and liberty, as if there is some grand metaphysical dial that only needs to be adjusted slightly to assure that we can go to bed at night without fear of another September 11.

These are debates that democracy does not simply make possible; these are debates that democracy requires. Your security is not enhanced if you cannot ask these questions, if you cannot debate these questions.

“EPIC has set the benchmark for relentless and principled advocacy on the main issues of public concern about the Internet and computerization.”

— THE LOS ANGELES  
TIMES

But democratic government doesn't work that way. Constitutional democracies do not prosper on that idea, you cannot give over to others the shared responsibility for ensuring freedom and security. Democracy requires oversight and accountability. It requires asking hard questions. And it requires affirming basic political rights, even in a time of crisis: to express dissent, to question military action, and to oppose the expansion of executive authority. There will be disagreements in these debates. But these are debates that democracy does not simply make possible; these are debates that democracy requires.

The Roman satirist Juvenal, commenting on the willingness of the Roman people to hand over authority to the Centaurs, asked "But who will watch the watchers?" Who will watch the people to whom we entrust our security? That is the question that lies at the heart of civil liberties in a constitutional democracy. What steps will we take as citizens to oversee the authorities that are established to protect our safety? This is not easy work. But it is the work that must be done after September 11. In the world that we defend, we welcome dissent. We hold government accountable. We safeguard the rights of citizens. We preserve security even as we cherish the freedom of every person.

— **Marc Rotenberg**  
epic.org



## 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'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.

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 makes frequent and effective 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 has also made 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).

**“JUST WANTED TO SAY THAT YOU  
ALL ARE DOING A FINE JOB,  
AND YOU HAVE A GOOD CAUSE.”  
— G.G.**

## 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.

## Watching the Watchers

**“Sed quis custodiet ipsos custodes?”**

— JUVENAL

The tragic events of September 11 have posed an enormous challenge to the protection of Constitutional freedoms in the United States. New proposals for monitoring private communications, tracking people in public places, and creating databases to profile personal activities are moving forward with little debate.

EPIC helped establish the In Defense of Freedom coalition to rally public support, and has now undertaken the Watching the Watchers project to promote public oversight of these new forms of government surveillance.

## 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 and Paris.

**“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 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](http://bookstore.epic.org)) and also from the EPIC Bookshelf at Powell’s Books. Discounts are available for multiple copies to educational institutions.

**“THANK YOU FOR YOUR ONGOING WORK IN THE PRIVACY AREA.  
I HAVE BOOKMARKED YOUR SITE AND VISIT IT WEEKLY.” – T.C.**

***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.

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

This annual survey, by EPIC and Privacy International, reviews the state of privacy in over fifty 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.

***Filters and Freedom: 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.

***The Consumer Law Sourcebook: Electronic Commerce and the Global Economy***

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

***Cryptography and Liberty: An International Survey of Encryption Policy***

The first comprehensive survey of encryption policies around the world, *Cryptography and Liberty* finds that the efforts to reduce export controls on strong encryption products have largely succeeded, although several governments are gaining new powers to combat the perceived threats of encryption to law enforcement.

**“THANKS FOR THE LATEST EPIC  
ALERT. I ENJOY READING IT  
ON A REGULAR BASIS AND I AM GLAD  
THAT YOU KEEP AN EYE ON  
WHERE ELECTRONIC PRIVACY  
IS HEADING.” – M.K.**

#### **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*

#### **EPIC Staff Articles, 2001**

Andrews, “International Developments in  
Personal Privacy,” *World Data Protection  
Report*, Volume 1, Issue 6, (June 2001)

Andrews, “Protecting Privacy Through  
Government Regulation,” *The Sedona  
Conference Journal*, Volume 2, Number 2  
(Fall 2001)

Hoofnagle, “Matters of Public Concern and  
the Public University Professor,” *27 Journal  
of College and University Law* 669 (2001)

Madsen, “Homeland Security, Homeland  
Profits,” *CorpWatch* (December 2001)

Rotenberg, “Internet Liberation Theology,”  
*Salon* (November 2001)

Rotenberg, “Fair Information Practices and  
the Architecture of Privacy (*What Larry  
Doesn’t Get*),” 2001 *Stanford Technology  
Law Review* 1.

Rotenberg, “Can We Keep a Secret?”  
*American Lawyer* (January 2001)

Sobel, “Will Carnivore Devour Online  
Privacy?” *IEEE Computer* (May 2001)

## epic in congress



**“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

### Wiretapping

In September 2000, EPIC testified before the House Judiciary Committee on a series of bills covering wiretapping and workplace monitoring. EPIC argued that more oversight and reporting was necessary for the use of the Carnivore Internet surveillance system, and that American workplace monitoring protections should include guidelines from the International Labour Organization. In 2001, Congress adopted reporting requirements for Carnivore outlined in the 2000 EPIC testimony.

### Consumer Privacy

In March 2001, EPIC testified before the House Commerce Subcommittee on Commerce, Trade, and Consumer Protection regarding privacy in the commercial sector. EPIC highlighted the development of privacy law and urged Congress to adopt laws that allow states to provide greater protections.

### Internet Privacy

In July 2001, EPIC testified before the Senate Commerce Committee regarding legislative approaches to protecting privacy on the Internet. EPIC argued that comprehensive privacy legislation would codify a system of fair information practices. Also in July, EPIC issued a statement to the House Judiciary Subcommittee on Courts,

the Internet and Intellectual Property that outlined the free speech and anonymity arguments for supporting only voluntary submission of information to the Whois database.

In June 2001, EPIC testified before the House Commerce Subcommittee on Commerce, Trade, and Consumer Protection regarding information privacy and technology. EPIC emphasized the need for legislation to compliment privacy enhancing technologies.

In October 2000, EPIC testified before the House Commerce Committee on developments in privacy protection for consumers. EPIC argued that self-regulation was insufficient to protect individuals' personal information.

Also in October 2000, EPIC testified before the Senate Commerce Committee on three Internet privacy bills. EPIC argued that there is public support for legal protections over personal information, and that a bill embodying fair information practices was necessary to protect individuals.

In June 2000, EPIC testified before the Senate Commerce Committee on Internet Privacy. EPIC argued that baseline legislation to protect privacy could be supplemented with privacy enhancing technologies.

## **Computer Security**

In February 2000, EPIC testified before the Senate Judiciary Committee on privacy, FIDNET, and plans to increase critical infrastructure protection. EPIC presented Justice Department memoranda obtained under FOIA to show that the plans would violate federal wiretap law and that FIDNET would involve tracking of credit card and toll billing information.

## **National ID**

As the House Committee on Government Reform held a hearing on National ID in November 2001, EPIC and other groups held a “National ID Shred-In” on Capitol Hill. EPIC and other advocates shredded National ID cards and brought attention to the dangers of a National ID card.

## **Social Security and Privacy**

In a series of hearings before the House Ways and Means Subcommittee on Social Security, EPIC has brought attention to the growing problem of identity theft that has resulted from the unrestricted sharing of Social Security Numbers. In May 2000, EPIC testified that there is judicial and legislative support for legal restrictions on the collection and use of the Social Security Number. In May 2001, EPIC explained that legislation to limit the use of the Social Security Number is appropriate, necessary, and consistent with Constitutional principles. In November 2001, EPIC testified on the need to limit the collection, use, and dissemination of the Social Security Number and to establish safeguards in law to protect personal information.

## **International Privacy**

In February 2000, EPIC testified before the European Parliament on data protection. EPIC argued that American self-regulatory approaches failed to protect consumer privacy and that baseline legal standards and privacy-enhancing technologies were necessary to protect privacy.



# litigation

**“The FBI found itself in the middle of a firestorm last year when its failure to provide sufficient details about [Carnivore] resulted in a lawsuit filed by the Electronic Privacy Information Center (EPIC). Through this litigation, EPIC has been seeking further details concerning the program under the Freedom of Information Act (FOIA).”**

– COMPUTERWORLD

## **INTERNET ARCHITECTURE— IN RE MICROSOFT (FTC)**

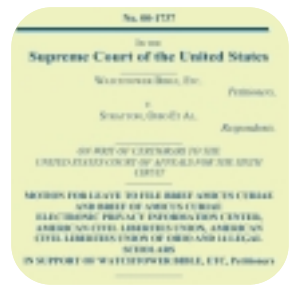
EPIC is bringing public attention to fundamental changes in the architecture of the Internet that could limit the privacy and freedom of Internet users. In July and August 2001, EPIC and fourteen other public interest groups urged the FTC to investigate Microsoft for unfair and deceptive trade practices relating to the Passport ID service. The online identification system requires individuals to disclose personal information before accessing the Internet. EPIC is seeking to prevent Passport and other similar services from restricting online access.

## **PRIVACY ENFORCEMENT—EPIC V. FTC**

With public concern about the enforcement of privacy rights mounting, EPIC filed suit against the Federal Trade Commission for the release of information detailing the agency’s handling of consumer privacy complaints. Those documents revealed that the FTC’s complaint processing procedures require extensive overhaul. Several changes were subsequently adopted by the FTC.

## **CONSUMER PROFILING—EPIC V. DOJ & TREASURY**

In 2001, the Wall Street Journal reported that federal law enforcement agencies were purchasing personal information from private-sector profiling corporations. To focus debate on these activities, EPIC submitted FOIA requests to the federal agencies. Documents obtained from the IRS show that the agency contracts with private data vendors for desktop access to citizen’s personal information. EPIC filed suit to compel other agencies to disclose their use of such databases.



## **INTERNET FREE SPEECH**

Online content control legislation threatens to stifle the growth of the Internet as an open and democratic medium. EPIC participated as plaintiff and co-counsel in the landmark lawsuit that invalidated Congress' first attempt to censor the Net, and is now back in court challenging new censorship laws. (ACLU v. Reno, Ashcroft v. ACLU, ALA v. United States)

## **ANONYMITY—WATCHTOWER BIBLE V. CITY OF STRATTON (AMICUS)**

EPIC continues to focus on important cases before the Supreme Court. In 2000 EPIC filed an amicus brief in *Condon v. Reno*, a case in which the Court ultimately upheld the Drivers Privacy Protection Act. In 2001, EPIC filed an amicus brief in the Supreme Court, supported by 15 law professors, in defense of the right of anonymity.

## **TELEPHONE PRIVACY— IN RE CPNI RULES (FCC)**

Telephone companies, seeking to use call-billing information for marketing purposes, attacked the privacy provisions of the 1996 Telecommunications Act. In response, EPIC coordinated a “friend of the court” brief endorsed by consumer groups, privacy organizations, law professors and privacy scholars that emphasized the paramount interest in protecting communications privacy. EPIC subsequently filed comments in the regulatory proceeding with the support of 18 privacy and consumer organizations.

## **GOVERNMENT SURVEILLANCE— EPIC V. DOJ & FBI**

When the existence of the FBI's Carnivore Internet monitoring system was first reported, EPIC immediately filed suit seeking the expedited release of relevant documents. Under pressure from the court, the FBI began releasing material that brought critical facts to the public. Because many of the system's details remain secret, the litigation is continuing to determine whether the FBI has improperly withheld relevant information.

## **GOVERNMENT OVERSIGHT**

In a series of high-profile FOIA cases, EPIC has sought public release of government documents on the key issues of the digital age, including encryption policy, electronic surveillance and computer crime investigations. The resulting disclosures were widely reported in the national press and led to Congressional hearings and reforms in agency practices.

## **ADMINISTRATIVE PROCEEDINGS**

EPIC participates in the agency rule-making process as an advocate of the public interest. Such proceedings address issues like location privacy, public access to electronic court records and communications security. EPIC typically works in close association with privacy and consumer organizations, technical experts, and legal scholars.

# internet public interest opportunities program

**"SEEING MY WORK INCLUDED... THE COURT HEARING IN PHILADELPHIA...  
BEING PART OF THE FTC COMPLAINT... RESEARCH FOR THE AMICUS BRIEF...  
ASSIGNMENTS WERE GREAT... THE VIBE AROUND THE OFFICE... PREPARING FOR  
CONGRESSIONAL HEARINGS... IT'S BEEN A GREAT EXPERIENCE."**

**–2001 IPIOP FELLOWS**

**"Founded in 1994, the Electronic Privacy Information Center has emerged as a leading public-interest advocacy organization. During its relatively brief lifespan, it has helped uncover the FBI's controversial Internet monitoring system, Carnivore, helped ease government restrictions on the use of encryption, and played a central role in ACLU v. Reno. EPIC continues to be at the forefront of protecting civil liberties."**

**– TEXAS LAWYER**



The EPIC IPIOP Program promotes opportunities for law school students to work on public interest issues concerning the future of the Internet. The program gives law 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 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.

A grant from the Glushko-Samuels Foundation established the Internet Public Interest Opportunities Program (IPIOP). There are summer and school semester internships available for outstanding law students with a strong interest in civil liberties interests relating to the Internet, particularly free speech, privacy, open government, and democratic governance.

## 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 decision makers. 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 (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 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 strategy in key cases with significant impact on critical Internet issues. Clerk activities include drafting memoranda, 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 the National Association of Public Interest Law ([napil.org](http://napil.org)).

## Applications

Submit a letter of interest, a writing sample, a résumé, and a recommendation letter to: IPIOP, Electronic Privacy Information Center, 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 150 applications were received for the first year of the IPIOP program.

## epic affiliated sites

**“THANK YOU FOR HAVING SUCH A GREAT INFORMATIONAL SITE, THIS IS SO COOL AND I WILL CONSTANTLY CHECK WITH YOUR SITE DAILY TO REVIEW THE LATEST TO KEEP ME ABREAST OF TODAY’S CHANGES.” –D.M.**

**“The Electronic Privacy Information Center, which follows the issue of privacy on the Net, has established an excellent international resource, with mailing lists, newsgroups, lists of conferences, and other info. This online guide is a fantastic window to issues, information, and organizations, which all share the common goal of protecting electronic privacy and individual rights.”**

– NETGUIDE’S BEST OF THE WEB



### **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.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**

**<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.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**

**<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 Ottawa, Paris, Hong Kong, and Dubai.

## epic board & staff

### EPIC Staff

Marc Rotenberg  
*President and  
Executive Director*

David L. Sobel  
*General Counsel*

Megan E. Gray  
*Senior Counsel/  
IPIOP Director*

Sarah Andrews  
*Research Director*

Chris Jay Hoofnagle  
*Legislative Counsel*

Mikal J. Condon  
*Staff Counsel*

Kate Rears  
*Policy Analyst*

David Leshner  
*Technology Director*

Wayne Madsen  
*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

D. James Bidzos

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  
*Board Member*

Austin Hill

Deborah Hurley  
*Board Member*

Prof. Jerry Kang  
*IPIOP Advisory Committee*

Judy Krug

Prof. Gary Marx

Dr. Denise M. Nagel

Peter G. Neumann  
*Secretary*

Prof. Eli Noam

Prof. Pamela Samuelson  
*IPIOP Advisory Committee*

Bruce Schneier

Prof. Paul M. Schwartz  
*IPIOP Advisory Committee*

Barbara Simons  
*Treasurer*

Robert Ellis Smith

Prof. Frank Tuerkheimer  
*IPIOP Advisory Committee*

Willis Ware

David Stern  
*Executive Director,  
National Association  
of Public Interest Law,  
IPIOP Advisory Committee*

# finances

## EPIC

### Statement of Activities

December 31, 2001

#### Support and Revenue

Contributions	\$ 340,073
Grants	1,104,921
Publications	22,349
Interest Income	<u>22,324</u>
<b>Total Support and Revenue</b>	<b><u>\$ 1,489,667</u></b>

#### Expenses

Program	\$ 567,884
Administration	56,308
Fundraising	27,843
<b>Total Expenses</b>	<b><u>\$ 652,035</u></b>

Change in Net Assets \$ 837,632

Net Assets, Dec 31, 2000 \$ 294,963

**Net Assets, Dec 31, 2001** **\$ 1,132,595**

*Based on report compiled by Friedman & Associates, CPA, Rockville, MD*



**EPIC**  
**Statement of Financial Position**  
**December 31, 2001**

**Assets**

Current Assets	\$ 630,006	
Fixed Assets	40,753	
EPIC Trust	<u>498,324</u>	
<b>Total Assets</b>		<u>\$ 1,169,083</u>

**Liabilities**

Accounts payable	<u>\$ 36,488</u>	
Total		\$ 36,488

**Net Assets**

General	\$ 394,653	
Projects	239,618	
EPIC Trust	<u>498,324</u>	
Total		<u>\$ 1,132,595</u>

<b>Total Liabilities and Net Assets</b>		<u>\$ 1,169,083</u>
---	--	---------------------

*The EPIC Trust, a Fidelity Charitable Gift Fund established in memory of Paul Simons, was transferred to EPIC Inc. during 2001.*

## supporters

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

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

Open Society Institute

Red Hat Center

Rockefeller Family Fund

Sherman Family Fund

Simons Foundation

Sun Microsystems

Zero Knowledge Systems

Additional support is provided by contributions from individual donors and the sale of publications.

## lend your voice

**“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

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.



**“THIS IS TO LET YOU KNOW THAT I FIND THE  
EPIC NEWSLETTER INCREDIBLY HELPFUL. I AM BECOMING  
INCREASINGLY ACTIVE IN THE COMMUNITY OF PRIVACY  
ADVOCATES, AND I USE THE ALERTS TO KEEP MYSELF UP TO DATE.  
THANKS SO MUCH FOR DOING A GREAT JOB.” – G.B.**

**“I ABSOLUTELY LOVE YOU GUYS! I’M CONSTRUCTING AN  
AFFIRMATIVE FOR DEBATE ABOUT MEDICAL PRIVACY  
AND HALF OF MY EVIDENCE COMES FROM YOUR WEB SITE  
INCLUDING MY PLAN (BASED ON YOUR PLAN GUIDE LINES).  
I CANNOT BEGIN TO THANK YOU FOR THIS.” – J.W.**

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

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

Classified by SP  
Declassify on: OADR

THIS INFORMATION CONTAINS  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

Asst. Dir.:

- Adm. Servs.
- Crim. Inv.
- Ident.
- Info. Mgmt.
- Insp.
- Intell.
- Lab.
- Legal Coun.
- Tech. Servs.
- Training
- Cong. Affs. O.
- Off. of EEO
- Off. Liaison &
- Int. Affs.
- Off. of Public
- Telephone Rm.
- Director's Of