

ENTRANCE BUTTON

# ENSURING ACCURACY & PRIVACY

epic 2005-2006

annual report

PRIMARY  
LEVER

1  
2  
3  
4  
5  
6  
7

## CONTENTS

- 1 mission & programs
- 2 voting technology:  
the design of privacy
- 4 epic program
- 7 epic publications
- 9 epic in congress
- 12 litigation
- 16 advocacy
- 20 internet public interest  
opportunities program
- 22 epic affiliated sites
- 24 finances
- 26 epic board & staff
- 27 epic supporters
- 28 support epic

**“The right of citizens of the United States to vote in any primary or other election for President or Vice President, for electors for President or Vice President, or for Senator or Representative in Congress, shall not be denied or abridged by the United States or any state by reason of failure to pay any poll tax or other tax.”** –CONSTITUTION OF THE UNITED STATES, 24TH AMENDMENT

## 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 two of the world’s most popular privacy sites—[epic.org](http://epic.org) and [privacy.org](http://privacy.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](http://privacyinternational.org)), the Internet Free Expression Alliance ([ifea.net](http://ifea.net)), the Global Internet Liberty Campaign ([gilc.org](http://gilc.org)), the Internet Democracy Project ([internetdemocracy.org](http://internetdemocracy.org)), and the Trans Atlantic Consumer Dialogue ([tacd.org](http://tacd.org)). EPIC maintains the Privacy Site ([privacy.org](http://privacy.org)) and coordinates the Public Voice coalition ([thepublicvoice.org](http://thepublicvoice.org)), the Privacy Coalition ([privacycoalition.org](http://privacycoalition.org)), and the In Defense of Freedom coalition ([indefenseoffreedom.org](http://indefenseoffreedom.org)). EPIC also established the National Committee on Voting Integrity ([votingintegrity.org](http://votingintegrity.org)).

"We are working to ensure that election systems preserve the secret ballot, accuracy, privacy, integrity, and the proper tabulation of the voter's intent regardless of his or her physical condition, language of origin, or literacy ability." – NATIONAL COMMITTEE FOR VOTING INTEGRITY'S



## Voting Technology:

## The Design of Privacy

This edition of the EPIC Annual Report explores the world of electronic voting. Many of EPIC's advisors have been pioneers in this field, which today has become a critical concern for election reform and voting rights activists across the country.

The design of modern voting technology seeks to reconcile two goals. First, there is the need to ensure the accuracy and integrity of the vote tabulation process. Votes should be counted as cast. Disputes should be resolved by means of a transparent system for auditing. All participants in an election should be satisfied that the outcome is correct.

Second, the secrecy of the ballot should be preserved. While the state has the right to ensure that only eligible voters cast votes, once that goal is fulfilled, the state has no right to inquire about for whom a vote was cast. The reason is obvious: many people go to the polls to choose new leaders and change their government. This is why the secret ballot is critical for democracy.

These two goals were not so difficult to achieve in an era of lever machines and paper ballots, at least in theory. But in a world of electronic voting systems, the challenges are enormous. Electronic recording of votes creates the risk that votes can be reconstructed and the identity of a voter might be linked to a vote that was cast. At the same time, the absence of meaningful procedures for auditing could raise questions about the reliability of vote tallies.

There is very important work being done in the field of cryptography—a critical component of electronic privacy and a core part of EPIC's history—that could achieve both accuracy and secrecy. But these methods are complex and voters may not trust them unless they are well understood.

*"I want to express my gratitude to all the individuals who help keep democracy and our constitutional rights protected. Without organizations such as EPIC, we would be in a dismal state of affairs." - J.K.*

Privacy issues also arise when states establish identification requirements and collect personal information from voters. ID requirements can operate as barriers to voter participation, much as poll taxes and literacy tests have in the past. It may be easy for a person with a drivers license to present a photo ID, but for a person who is poor or disabled and cannot afford a car or does not need one, the photo ID requirement may be the difference between voting and not voting.

Almost 15 years ago, a resident of Virginia challenged the state's practice of collecting and publishing the Social Security numbers of registered voters. He said the publication of his Social Security number was an unconstitutional burden on his right to vote. A federal appellate court agreed and the SSN was removed from the voter roles with no negative impact on the voting process.

Today as then we are confronting new challenges with the modernization of voting technology. Courts are being asked to ensure accuracy and preserve secrecy. Privacy is not simply a consideration in this process, it is a central requirement.

As with many of challenges to the right of privacy, EPIC continues to be on the front lines of emerging civil liberties issues.

In this issue of our annual report, we share with you both our work from the past year and encourage you to think about the future of voting technology.

**MARC ROTENBERG**

President

Electronic Privacy Information Center

**“Voting systems are particularly challenging from a security viewpoint because of the need to remove voter’s identities from their cast ballots, in order to prevent vote-buying and the coercion of voters.” – PROF. RONALD L. RIVEST**

# 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 online censorship. As a leading publisher of policy materials on the Internet, EPIC joined with other civil liberties and computer industry organizations and served as both co-counsel and co-plaintiff in that historic litigation. EPIC has continued to play a leading role in defense of free expression, including the right to receive and distribute information anonymously.

In 2005, following EPIC’s work on an important case concerning anonymity before the Supreme Court that challenged a state identification requirement, EPIC launched a project on Identification and Surveillance and began the monthly series, “Spotlight on Surveillance” ([epic.org/privacy/surveillance/spotlight/](http://epic.org/privacy/surveillance/spotlight/)) to scrutinize federal government programs that affect individual privacy and anonymity.

## Open Government

**“EPIC keeps tabs on those who are keeping close tabs on us, and on important legal issues.” – [SAN DIEGO UNION-TRIBUNE](#)**

EPIC’s award winning work applies Freedom of Information Act rules to make government records concerning domestic surveillance, data mining, government profiling, and networking available to the public.

In 2005, EPIC launched FOIA Notes ([epic.org/foia\\_notes/](http://epic.org/foia_notes/)), an online newsletter that gives subscribers fast access to important documents obtained by EPIC under the Freedom of Information Act. The publication provides images and information about the government’s latest disclosures, as well as links to other FOIA resources.



## Privacy

**“EPIC works “not in the heat of the moment or only in partisan arenas, but deliberately, neutrally, and thoughtfully,” and “EPIC’s efforts in [cyberspace law] have served us all well.” – AMERICAN BAR ASSOCIATION**

Passenger profiling. Data mining. RFID identity cards. Biometric identifiers. Electronic voting. 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. Congressional committees and government agencies to identify privacy risks and develop new approaches for privacy protection frequently call upon EPIC.

With the world’s most comprehensive archive of privacy resources, EPIC’s award-winning web site demonstrates the educational potential of the Internet. With many of the top-ranked web pages on key privacy topics, the EPIC site is the central resource for the ongoing debate about the future of privacy.

## Electronic Voting

**“Election Officials say their electronic voting system are the very best. But the truth is, gamblers are getting the best technology, and voters are being given [voting] systems that are cheap and untrustworthy by comparison.” – NEW YORK TIMES EDITORIAL**

The increased use of technology that facilitates the right of citizens to participate in public elections may threaten privacy. The use of technology in the online and offline voting process is growing in popularity around the world, while the science that would verify the efficacy and integrity of voting systems lacks vital support. EPIC’s efforts in election reform focus on transparency, privacy, and security of voting systems and processes.

**“Providing sufficient assurances for computerized election integrity is a very difficult problem. Serious risks will always remain, and some elections will be compromised. The alternative of counting paper ballots by hand is not promising. But we must question more forcefully whether computerized elections are really worth the risks, and if so, how to impose more meaningful constraints.” – DR. PETER NEUMANN**

**“Thank you for your stand on privacy as recently reflected on a C-SPAN program dealing with the NSA domestic spying issue.” – N.B.**

## 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.

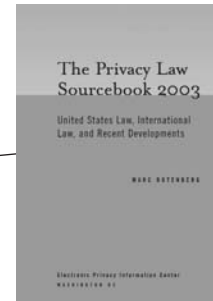
The Public Voice Project in cooperation with the OECD, UNESCO, and other international organizations works to bring civil society leaders face to face with government officials for constructive engagement about current policy issues. Public Voice events have been held in Buenos Aires, Dubai, Hong Kong, Honolulu, Ottawa, Paris, Washington, and Wroclaw.

In 2005, EPIC hosted several programs to promote the perspectives of civil society organization on issues concerning today’s emerging information society, including a symposium in Bogota, Colombia. EPIC also worked to gain greater acceptance for civil society groups at the World Summit on the Information Society.

**“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**





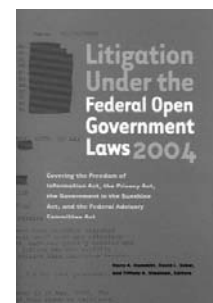
**EPIC's FOIA Manual — Deserves a place in the library of everyone who is involved in, or thinking about, litigation under the Freedom of Information Act.”**

— 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](http://bookstore.epic.org)) and also from the EPIC Bookshelf at Powell’s Books ([powells.com/features/epic/epic.html](http://powells.com/features/epic/epic.html)). Discounts are available for multiple copies to educational institutions.

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

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

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

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

**“Freedom of expression and participation without fear of retribution is the basis for democracy. Anonymity is the only known means to achieve it — that’s why anonymity is essential in voting.” – DR. DAVID CHAUM**

**“I appreciate your taking the time to respond – I know things are very busy in your camp.” – R.A.L.**

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

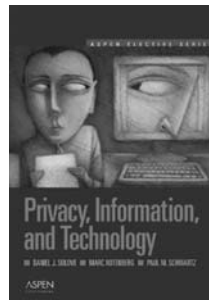
This annual survey, by EPIC and Privacy International, reviews the state of privacy in over sixty countries around the world. The survey examines a wide range of privacy issues including data protection, telephone tapping, genetic databases, e-voting, RFID, ID systems and freedom of information laws.

### **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.

**Solove, Rotenberg & Schwartz, INFORMATION PRIVACY LAW (Aspen Publishers) —  
“A Masterful Synthesis of the Field.”**

**Solove, Rotenberg & Schwartz, PRIVACY, INFORMATION, AND TECHNOLOGY  
(Aspen Publishers) — “A comprehensive, in-depth treatment of all important  
issues involving information privacy.”**



# 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](#)**

**“EPIC’s Bill Track is a good current resource for federal legislation concerning privacy, speech and cyber-liberties...” - [INTERNET LAW RESEARCHER](#)**

In 2005, 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 Internet telephony, DNA collection, RFID passports, and government watch lists.

## **AIRLINE PASSENGER SCREENING PROGRAM**

In November 2005, EPIC testified before the House Committee on Homeland Security and warned that the new plan for passenger screening was still flawed. EPIC pointed out that the problems with watch list errors had not been solved, that there are no legal safeguards to prevent misuse, and that “mission creep” is almost certain. EPIC recommended that the program not go forward until these problems are fixed.

**“Only 72 percent of eligible citizens were registered to vote in 2004, according to the Census Bureau. And the registration rate among 18- to 24-year-olds was a dismal 58 percent, which helps explain why voter turnout for this age group in the presidential election was far below the national average. That’s simply unacceptable.” – HON. JOHN ANDERSON**

#### **EMPLOYMENT VERIFICATION SCHEMES**

In May 2005, EPIC testified before the House Judiciary Committee on one of several proposals before Congress to impose new employment verification requirement on those wishing to work within the United States. The legislation would require all workers to obtain a Social Security Number card that would be machine-readable. The bill would also empower the Department of Homeland Security to determine employment eligibility of those seeking employment. EPIC opposed the creation of this new employment verification system because of the risks it poses to privacy and civil liberty.

#### **DATA PROTECTION**

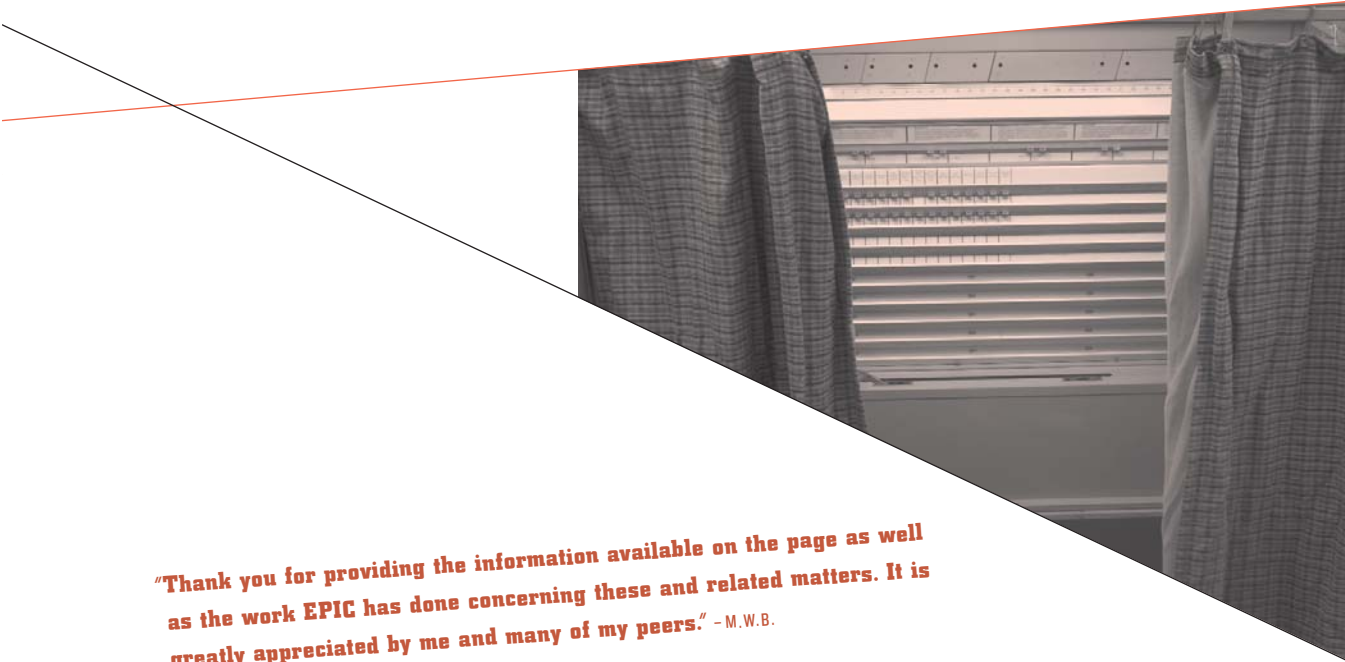
In July 2005, EPIC testified before the House Commerce Subcommittee on Consumer Protection. EPIC urged Congress to pass strong data security legislation that includes privacy protections for use of personal information. The hearing concerned bipartisan draft data security legislation that would require companies to give notice to consumers of security breaches.

#### **MEDICAL PRIVACY**

In October 2005, EPIC and Patient Privacy Rights launched a joint campaign to strengthen protections for patients’ medical information. In 2005, Congress began consideration of several bills that would establish a national Health Information Network that excluded protection of patient privacy rights.

#### **DATA BROKERS**

In May 2005, EPIC urged lawmakers to regulate Choicepoint and other data brokers in testimony before the House Commerce Subcommittee on Consumer Protection. EPIC testified that there is too much secrecy and too little accountability in the business dealings of data brokers, and that Choicepoint’s selling of customer information to identity thieves underscored the need for federal regulation of the information broker industry.



***"Thank you for providing the information available on the page as well as the work EPIC has done concerning these and related matters. It is greatly appreciated by me and many of my peers." - M.W.B.***

#### **CYBERCRIME CONVENTION**

In July 2005, EPIC testified before the Senate Committee on Foreign Relations in opposition to the ratification of the Council of Europe Convention on Cybercrime. EPIC urged the Senate to oppose ratification because of the convention's sweeping expansion of law enforcement authority, the lack of legal safeguards, and the impact on U.S. Constitutional rights.

#### **RECRUITING DATABASE**

In October 2005, EPIC led a campaign of more than 100 organizations that urged Secretary of Defense Rumsfeld to end the "Joint Advertising and Market Research Studies" Recruiting Database. The groups cited the broad exemptions to federal privacy laws that would allow the Defense Department to disclose personal information to others without an individual's consent or knowledge. The database would include name, date of birth, gender, address, telephone, e-mail address, Social Security Number, ethnicity, high school, education level, college, and intended field of study for more than 30 million Americans who are 16–25 years old.

“Because of the secrecy surrounding almost every aspect of e-voting along with a lack of public national incident reporting— independent computing technologists can provide only limited analyses of problems relating to hardware, software, testing, security, and human factors. Nonetheless, evidence of these problems is widespread and varied.” – DR. BARBARA SIMONS



# Litigation

“The search to obtain DNA raises privacy concerns more significant than the search of a vehicle, a house, or even a person’s pockets because DNA reveals the most intimate details about a person.” – EPIC AMICUS BRIEF IN KOHLER V. ENGLADE (2005)

## 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.

---

### **WHOIS PRIVACY — Peterson v. NTIA (Amicus)**

In April 2006, EPIC filed a friend of the court brief supporting the rights of domain name holders not to publish their personal information on the Internet. In 2005, the U.S. Department of Commerce, which administers the .us country code top-level domain, banned users who registered .us domains from using proxy services, which provide some privacy protection for Internet users who register domain names. EPIC's brief argues that the policy for .us diverges wildly from international policy and the policies of other countries' top-level domains. The case is currently pending before the Fourth Circuit.

### **FOIA LITIGATION — EPIC v. Department of Justice**

In a complaint filed in April 2005, EPIC asked a federal court to force the FBI to disclose information about its use of expanded investigative authority granted by sunset provisions of the USA PATRIOT Act. The agency agreed to quickly process EPIC's Freedom of Information Act request for the data, but did not comply with the timeline for even a standard FOIA request. The FBI released a small number of documents in October 2005, which included reports of intelligence misconduct from the FBI to an intelligence oversight board. In November 2005, Judge Gladys Kessler ordered the FBI to publicly release or account for 1,500 of pages responsive to the request every fifteen days.

### **PATRIOT ACT AUTHORITY — Gonzales v. Doe (Amicus)**

This lawsuit concerns the FBI's authority to issue national security letters to businesses for certain customer records without judicial approval. This investigative power, which is part of the Electronic Communications Privacy Act, also imposes a permanent nondisclosure order prohibiting the recipient from ever telling anyone he has received a national security letter.

In 2004, an anonymous Internet service provider and the ACLU challenged the constitutionality of this broad authority, arguing that it violates the First and Fourth Amendments because the law fails to provide adequate checks on the FBI's power to force companies to turn over sensitive customer information. They also argued that the "gag" provision violates the First Amendment because it completely and permanently forbids every recipient from disclosing the fact that he received a national security letter—regardless of whether such a sweeping ban is actually necessary. A federal court in New York found the power unconstitutional on First Amendment grounds in September 2004. The government challenged that ruling in the Second Circuit Court of Appeals.

**“The idea is counterintuitive, and for most of the long history of secret codes, it was ignored. But with the rise of computer-assisted cryptography in the past 50 years or so, there has been a sea change in the working assumptions of cryptographers. Now, you can’t get good cryptography by designing in secret.” – WHITFIELD DIFFIE**

EPIC co-authored an amicus brief with the National Security Archive arguing that the courts must provide meaningful oversight of the government’s investigative activity, and that the FBI’s national security letter power undermines government accountability. Other organizations supporting the brief include the Project on Government Secrecy of the Federation of American Scientists and the National Whistleblower Coalition.

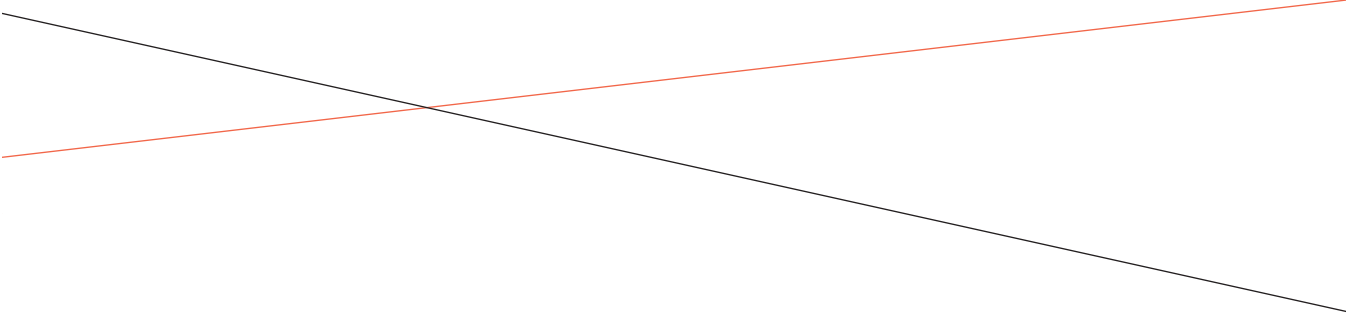
#### **CENSUS PRIVACY – EPIC v. Department of Commerce**

In July 2004, EPIC obtained heavily redacted documents through the FOIA revealing that the Census Bureau had provided the Department of Homeland Security’s Bureau of Customs and Border Protection with statistical data on people who identified themselves on the 2000 census as being of Arab ancestry. The redacted information was withheld at the insistence of Customs. EPIC appealed the withholdings to both the Commerce Department (the parent agency of the Census Bureau) and Customs. Neither agency responded within the time frame required by law. EPIC filed suit in September 2004 to compel the agencies to release the redacted information. Commerce responded to EPIC’s appeal, and EPIC dropped its suit against that agency. The case against Customs is pending.

#### **DRIVERS PRIVACY – Kehoe v. Fidelity Bank (Amicus)**

In August 2005, the 11th Circuit Court of Appeals held that individuals suing to recover for violations under the Drivers Privacy Protection Act do not need to demonstrate actual harm in order to recover monetary damages. In the case, a Florida man sued Fidelity Bank for obtaining the personal information of 565,000 individuals from the State’s motor vehicle databases for junk mail purposes. EPIC’s brief in the case argued that monetary damages were necessary in order to deter unaccountable data brokers from obtaining personal information from government coffers.





*"I visited the EPIC web site today for some of my privacy research, and its contents reminded me yet again of the extraordinary value of your work and that of your colleagues at EPIC. This is a simple note of my appreciation for what you and your colleagues do." - E.O.*

**ONLINE PRIVACY – United States v. Councilman (Amicus)**

In August 2005, a federal appeals court held that the interception of e-mail in temporary storage violated the federal wiretap act. The decision reverses an earlier opinion. EPIC joined with other civil liberties groups to support the reversal and assisted technical experts who submitted a brief favoring an interpretation of privacy laws that will protect the confidentiality of electronic communications.

**COERCED DNA SAMPLE – Kohler v. Engle (Amicus)**

In October 2005, EPIC filed an amicus brief in support of a person who challenged a DNA dragnet search in Baton Rouge, Louisiana. At least 15 men including Kohler declined to provide a DNA sample to police. The Baton Rouge Police Department obtained a seizure warrant to force Mr. Kohler to submit his DNA sample for the investigation. Kohler was later cleared of any connection with the crime and challenged the seizure of his DNA. When a district court dismissed Kohler's claim, Kohler appealed to the Fifth Circuit Court of Appeals. In supporting Kohler's petition, EPIC presented an extensive survey of DNA dragnets which demonstrated that it is not an effective investigative technique. EPIC also argued that DNA dragnet searches implicated Fourth Amendment interests, and that if the court were to permit such searches to occur, there should be clear rules to protect Fourth Amendment values. The case is currently before the Fifth Circuit.

“The alarm call could not be clearer. A state should not be permitted to condition exercise of the electoral franchise on a voter’s skills with technology, her luck, or her county of residence.” – PROF. PAUL SCHWARTZ

# ADVOCACY

In 2005, 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 Internet telephony, DNA collection, RFID passports, and government watch lists.

## **Parent Locator Databases**

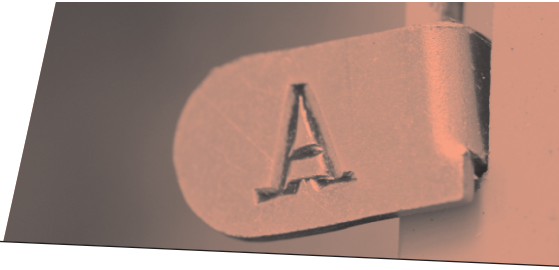
EPIC submitted comments to the Department of Health and Human Services on the need to improve accuracy for government access to “parent locator services.” These services, which were first implemented to locate “deadbeat dads,” have expanded to include an incredible array of personal information. The comments explain the need for audit logs and for the ability for individuals to correct information in the database.

## **Detail Calling Record Privacy**

In August 2005, EPIC petitioned the Federal Communications Commission on the behalf of consumers requesting that the agency initiate a rulemaking to enhance security safeguards for individuals’ calling records. The petition follows an EPIC complaint made earlier in the year concerning the illegal sale of personal information obtained from telephone carriers through a deceptive practice called “pretexting”.

## **Internet Telephony**

On November 2005, EPIC filed comments with the Federal Communication Commission opposing the expansion of a telephone wiretap law into voice over Internet Protocol (IP) communications. The Commission’s expansion of the Communications Assistance for Law Enforcement Act would require developers to build security backdoors for government wiretapping into a wide range of devices and applications, putting privacy and security at risk.



### **DOD Recruitment Database**

In June 2005, EPIC submitted comments to the Department of Defense objecting to the creation of a massive database for military recruitment purposes. The database is reported to contain data files on all those individuals 16–25 years of age who are residing in the United States. EPIC challenged the establishment of the database, which failed to comply with the federal Privacy Act.

### **DNA Collection and Retention**

In June 2005, EPIC submitted comments urging the Justice Department to identify and ensure compliance with existing privacy protections when preserving biological evidence during the investigation of a federal crime for which an individual is in prison. EPIC argued that the agency should limit access to DNA material that must be preserved under law to government agencies that will use the material to further this legislative purpose.

### **Medical Privacy**

In October 2005, EPIC urged the Food and Drug Administration to examine medical marketing databases. Medical marketers sell the personal information of people with cancer and other serious diseases. These databases can be used to target vulnerable groups, and privacy law does not cover all of the information collected.

### **Children's Online Privacy**

In June 2005, EPIC filed comments to the Federal Trade Commission, which were requested as part of the agency's review of the Children's Online Privacy Protection Act (COPPA). EPIC argued that COPPA has improved children's privacy online, but there is a need to continue to clarify COPPA through its enforcement. The comments also argued for more research into the cutting-edge techniques being used to direct web sites at children. EPIC warned that further action is still needed to address the privacy concerns raised in the offline market for children's personal information.

**“Some argue that the application of technology will be the medicine that will cure the body politic of flawed elections. Others argue that the solution is found in the people who perform election administration. The truth is found in both views with two additional elements — transparency and oversight.” – LILLIE CONEY**

### **Electronic Voting**

In August 2005, EPIC testified before the Election Assistance Commission on the development of new Voluntary Voting System Guidelines. The new standards are intended to improve the quality of voting systems available for public elections. This guidance to states would follow the expending of over \$3 billion in federal funds to replace older voting systems.

### **Traveler Privacy**

In April 2005, EPIC submitted comments to the Department of Homeland Security urging the agency to abandon a flawed proposal to embed radio frequency identification (RFID) tags in travel documents. EPIC opposed the plan because it lacked basic privacy and security safeguards.

### **Government Watch List**

In September 2005, EPIC submitted comments to the FBI urging the agency to stop expanding the Terrorist Screening Center’s watch list record system until the Bureau resolves significant privacy issues. EPIC objected to the FBI’s proposal to exempt the watch list from legal requirements that ensure record accuracy. EPIC has uncovered significant problems with watch list errors through Freedom of Information Act activities.

### **Government Surveillance Database**

In May 2005, EPIC led a national coalition of organizations to oppose the creation of the “Homeland Security Operations Center Database,” a massive government database. The agency planned to exempt the vast database from legal requirements that protect privacy and promote government accountability.

### **Voter ID Requirements**

In July 2005, EPIC opposed Georgia’s petition to the Department of Justice for a government-issued photo identification document to vote in all state or federal elections. Georgia is required by the Voting Rights Act of 1965 to submit all changes to voting law for pre-approval by the Department of Justice. Although the Justice Department approved the change, it was subsequently found unconstitutional by two federal courts.



*"Thank you for providing the information available on the page as well as the work EPIC has done concerning these and related matters. It is greatly appreciated by me and many of my peers,..." - M.W.B.*

#### **Radio Frequency Identification Devices (RFID)**

In April 2005, EPIC submitted comments to urge the State Department to scrap its plans to require RFID enabled passports for all American travelers. EPIC said the proposal was flawed because the Department lacked legal authority to require RFID travel documents, and had failed to show the benefits of the e-passports. EPIC also led a public education campaign to engage consumer advocacy groups on this issue. Later the State Department revised the passport requirements and strengthened their security.

#### **Biometric Identification**

In March 2005, EPIC filed comments with the Transportation Security Administration and requested a delay in the agency's plan to test biometric technology for transportation workers until it conducted a comprehensive Privacy Impact Assessment. EPIC argued that the assessment should allow the agency "to ensure protection of the privacy rights of program members." EPIC said that the program must comply with the federal Privacy Act and noted that there are unique problems associated with biometric technologies, including the varying degrees of error, the risk of circumvention, and the likelihood of mission creep.

**“Even if we get the technology right, we still won’t be done. If the goal of a voting system is to accurately translate voter intent into a final tally, the voting machine is only one part of the overall system.” –BRUCE SCHNEIER**

## **Internet Public Interest Opportunities Program**

**“I would highly recommend your program to law students looking to work for a leading public interest group in D.C. I would recommend the cutting edge research on privacy law as well as the high level of clerk involvement on each project...I found the process of researching and commenting on a proposed rulemaking to be very interesting and a great learning experience.... I also liked the variety of projects and the fact that they were focused on a mission, which gave me the feeling that I was actually participating in something that mattered.” –2005 IPIOP CLERKS**

A grant from the Glushko-Samuelson Foundation established the Internet Public Interest Opportunities Program (IPIOP). IPIOP is an intensive, paid legal internship conducted during the summer, fall, and spring terms. There are summer and school semester internships available for outstanding law students with a strong interest in civil liberties relating to the Internet, particularly free speech, privacy, open government, and democratic governance. The EPIC IPIOP program gives law students the opportunity to 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, 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 intersection between Internet law and public policy.



### LEGISLATION

The legislative process is the critical opportunity for public interest organizations to make their 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 process by researching and drafting memoranda on issues before Congress, and by attending hearings.

### GOVERNMENT OVERSIGHT

The Freedom of Information Act (FOIA) is a powerful tool for public interest organizations to learn about otherwise inscrutable government 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 government 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 Equal Justice Works ([equaljusticeworks.org](http://equaljusticeworks.org)).

### APPLICATIONS

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

# Epic Affiliated Sites

“This consumer group provides a wealth of information at its web site.”

- GOVERNING MAGAZINE

**In 2005, EPIC introduced a new web resource, “Spotlight on Surveillance,” ([epic.org/privacy/surveillance/spotlight](http://epic.org/privacy/surveillance/spotlight)). The site features in-depth analysis of federal government programs that impact individual privacy.**

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

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

## **GLOBAL INTERNET LIBERTY CAMPAIGN (GILC)** [gilc.org](http://gilc.org)

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

## **IN DEFENSE OF FREEDOM (IDOF)** [indefenseoffreedom.org](http://indefenseoffreedom.org)

The IDOF coalition was established after September 11, 2001, 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 10-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](http://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](http://privacyinternational.org)

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

**THE PRIVACY SITE** [privacy.org](http://privacy.org)

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

**THE PUBLIC VOICE** [thepublicvoice.org](http://thepublicvoice.org)

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

***"The Electronic Privacy Information Center advocates for 'the right to be left alone' in this digital age. It's a tough fight, but somebody has to keep it going." - KNIGHT/RIDDER TRIBUNE NEWS SERVICE***

**NATIONAL COMMITTEE FOR VOTING INTEGRITY** [votingintegrity.org](http://votingintegrity.org)

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

**PRIVACY COALITION** [privacycoalition.org](http://privacycoalition.org)

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

# Finances

## EPIC

### STATEMENT OF ACTIVITIES

2002, 2003, 2004 AND 2005

	2002	2003	2004	2005
<b>Support and Revenue</b>				
Contributions	\$ 251,250	\$ 183,376	\$ 380,205	\$ 78,473
Grants	862,167	840,323	840,473	606,250
Publications	16,956	22,232	20,319	13,624
Interest Income	36,134	40,160	45,768	49,833
Other	(53,398)	39,602	(5,171)	(17,165)
<b>Total Support and Revenue</b>	<b>\$ 1,110,454</b>	<b>\$ 1,125,693</b>	<b>\$ 1,332,044</b>	<b>\$731,065</b>
<b>Expenses</b>				
Program	\$ 772,578	\$ 813,456	\$ 933,864	\$ 897,076
Administration	47,141	47,003	66,831	58,511
Fundraising	46,903	57,278	25,461	46,493
<b>Total Expenses</b>	<b>\$ 866,622</b>	<b>917,737</b>	<b>1,025,976</b>	<b>1,002,080</b>
<b>Change in Net Assets</b>	<b>\$ 243,832</b>	<b>\$ 207,956</b>	<b>\$ 306,068</b>	<b>(271,015)</b>
<b>Net Assets, Jan 1</b>	<b>\$ 1,132,595</b>	<b>\$1,376,427</b>	<b>\$ 1,584,383</b>	<b>1,890,451</b>
<b>Net Assets, Dec 31</b>	<b>\$ 1,376,427</b>	<b>\$1,584,383</b>	<b>\$ 1,890,451</b>	<b>1,619,436</b>

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](http://www.guidestar.org)

**EPIC**  
**STATEMENT OF FINANCIAL POSITION**  
**DECEMBER 31, 2005**

**Assets**

Current Assets	\$ 1,068,768
Fixed Assets	17,978
EPIC Trust	552,504

---

<b>Total Assets</b>	<b>\$1,639,250</b>
---------------------	--------------------

---

**Liabilities**

Accounts payable	\$ 19,814
------------------	-----------

---

<b>Total</b>	<b>\$ 19,814</b>
--------------	------------------

---

**Net Assets**

General	\$ 680,240
Projects	386,692
EPIC Trust	552,504

---

<b>Total</b>	<b>\$ 1,619,436</b>
--------------	---------------------

---

<b>Total Liabilities and Net Assets</b>	<b>\$1,639,250</b>
---	--------------------

---

The EPIC Trust was established in memory of Paul Simons.

# Epic Board & Staff 2005–2006

## 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*

Sherwin Siy  
*Staff Counsel*

Melissa Ngo  
*Staff Counsel*

Marcia Hofmann  
*Staff Counsel*

Katitza Rodríguez Pereda  
*International Policy Fellow*

R. P. Ruiz  
*Technology Fellow*

Harry Hammitt  
*Senior Fellow*

Kate Rears  
*Administrative Director*

Daniel Burger  
*Administrative Coordinator*

## EPIC ADVISORY BOARD

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

Steve Aftergood

Prof. Phil Agre

Hon. John Anderson

James Bamford

Prof. Ann Bartow  
*IPIOP Advisory Committee*

Prof. Francesca Bignami  
*Board Member*

Prof. Christine Borgman

Prof. James Boyle  
*IPIOP Advisory Committee*

David Burnham

Prof. Anita Allen-Castellitto  
*Board Member*

Vinton G. Cerf

David Chaum

Prof. Julie E. Cohen  
*IPIOP Advisory Committee*

Simon Davies

Whitfield Diffie  
*Board Member*

Prof. David Farber

Hon. David Flaherty

Philip Friedman  
*Board Member*

Prof. Oscar Gandy  
*Board Member*

Austin Hill

Deborah Hurley  
*Chair*

Prof. Jerry Kang  
*Secretary*

Judy Krug  
*IPIOP Advisory Committee*

Chris Larsen

Prof. Gary Marx

Mary Minow

Dr. Denise M. Nagel

Peter G. Neumann  
*Treasurer*

Prof. Eli Noam

Prof. Anita Ramasastry  
*IPIOP Advisory Committee*

Prof. Ron Rivest

Prof. Pamela Samuelson  
*IPIOP Advisory Committee*

Bruce Schneier  
*Board Member*

Prof. Paul M. Schwartz  
*IPIOP Advisory Committee*

Barbara Simons  
*Board Member*

Robert Ellis Smith

Prof. Daniel J. Solove  
*IPIOP Advisory Committee*

Prof. Frank Tuerkheimer  
*IPIOP Advisory Committee*

Edward G. Viltz  
*Board Member*

Willis Ware

Paul Wolfson

David Stern  
*IPIOP Advisory Committee*

# EPIC SUPPORTERS

*"Finally, I read your annual report. Sincerely, thank you for all the good work your organization does. We work in a place where money talks and Congress is fixated on what's good for business and law enforcement – and yet somehow your views get aired and considered." -T.T.*

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

Arca Foundation	W.K. Kellogg Foundation	Rockefeller Family Fund
Bauman Foundation	Irving Kohn Foundation	Rose Foundation
Carnegie Corporation	Albert List Foundation	Glushko-Samuelson Foundation
Counterpane Systems	Lutz Foundation Trust	Scherman Foundation
Nathan Cummings Foundation	Markle Foundation	Simons Foundation
Earthlink	Metromail Cy Pres Fund	Sun Hill Foundation
Ford Foundation	Norman Foundation	Sun Microsystems
Fund for Constitutional Government	Omidyar Network	Trio Foundation of St. Louis
HKH Foundation	Quixote Foundation	Working Assets
	Red Hat Center	Zero Knowledge Systems

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

**“Everyone has the right to take part in the government of his country, directly or through freely chosen representatives. Everyone has the right to equal access to public service in his country. The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret or by equivalent free voting procedures.” –DECLARATION OF HUMAN RIGHTS, ARTICLE 21**

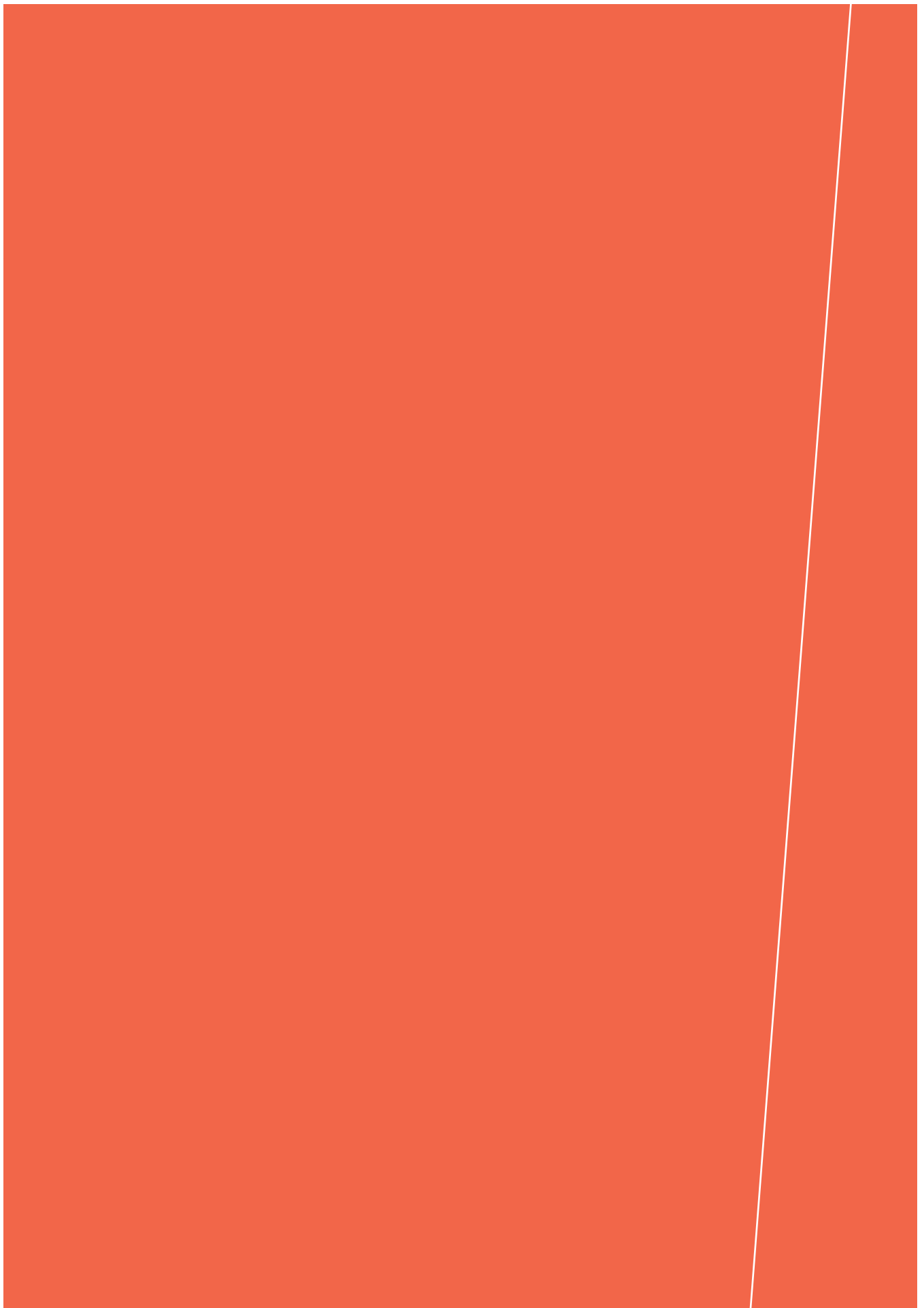
## SUPPORT EPIC

***“I just wanted to praise the EPIC website and the valuable info you make available to the public.... At the end of the year, me and others plan on contributing a few dollars to your organization.” – ANON.***

***“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 does wonderful work. I admire their efforts to protect the privacy of Americans. Particularly at this moment when there is growing concern about unlawful surveillance within the United States, I urge you to support the work of EPIC.” – JAMES BAMFORD, AUTHOR, [THE PUZZLE PALACE](#), [BODY OF SECRETS](#), AND [A PRETEXT FOR WAR](#)***

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, D.C. 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.





**ENTRANCE BUTTON**

**ELECTRONIC PRIVACY INFORMATION CENTER**

1718 Connecticut Avenue NW Suite 200  
Washington DC 20009 USA

[T] +1-202-483-1140 [F] +1-202-483-1248

**epic.org**

**PRIMARY  
LEVER**

1  
2  
3  
4  
5  
6  
7