

STUDENT PRIVACY patriot act  
genetic genetic  
privacy genetic  
FOIA FOIA  
cybersecurity open  
government government  
EPIC v. NSA  
social network  
privacy privacy  
epic  
BIG DATA  
2013  
free speech  
privacy  
DRONES  
OVERSIGHT  
EPIC  
v. DHS  
biometrics  
brokers  
data  
scanners  
Constitution  
PUBLIC VOICE  
surveillance  
SMART GRID

# EPIC ANNUAL REPORT

2013

## CONTENTS

- EPIC 2013 – Snowden, NSA, Word of the Year
- In re EPIC and Related EPIC Cases
- Emerging Privacy Issue – Drone Surveillance
- EPIC in Congress
- EPIC Open Government Project
- EPIC Public Voice Project
- EPIC Appellate Program
- EPIC and Consumer Protection
- EPIC Student Privacy Project
- EPIC Publications
- EPIC Staff at Conferences
- EPIC in the News
- EPIC Online
- Planning for 2014
- EPIC Staff
- EPIC Board and Advisory Board
- EPIC Champions of Freedom
- EPIC Financial Statements
- EPIC 2013 Wrap Up – Ray Ozzie

The Electronic Privacy Information Center is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues, and to safeguard privacy, the First Amendment, and other Constitutional values.

**EPIC 2013 – Snowden, NSA, Word of the Year**



*Marc Rotenberg*

Not since news broke that President Nixon had spied on his political opponents has the American public been more engaged in the debate over electronic privacy. Whether or not you support Mr. Snowden’s actions, there can be no question that he has made possible a long overdue discussion about the scope of surveillance in the post 9-11 world

Because of Mr. Snowden, we have learned that the National Security Agency engaged in a far more aggressive collection of personal information than ever imagined. The NSA routinely collected the telephone records and Internet data of individuals all around the world. The NSA also worked to weaken basic standards that help ensure the security and stability of the Internet.

EPIC had long warned about the growing impact of the NSA on privacy and Internet security. And we specifically pointed to the risk of expanding the Foreign Intelligence Surveillance Act. Over the years, we have urged Congress to improve reporting requirements and increase transparency. At technical conferences, we explained the history of the “Clipper Chip” and the real risks to Internet security of weakened crypto standards. Well before Mr. Snowden, we proposed that the opinions of the Foreign Intelligence Surveillance Court be made available to the public and that more data be collected on the actual effectiveness of the various NSA programs.

At hearings in Congress and before the European Parliament, meetings at the White House, presentations before various panels, and a petition to the US Supreme Court, EPIC has recommended that the powers granted to the NSA under the Foreign

Intelligence Surveillance Act be significantly narrowed, that the bulk collection of domestic telephone data end, that Privacy Act safeguards be enforced, and that much greater transparency be established whenever the government engages in electronic surveillance of individuals suspected of no crime.

For a long time, this has seemed like a very lonely battle. But if the public became more aware of the extent of NSA surveillance this year, 2013 may have also marked a turning point in the public debate. As the end of the year approached, a federal judge in Washington ruled that the NSA data collection program violated the Constitution. “Almost Orwellian” is how Judge Leon described the routine collection by the NSA of all phone records of Americans.

And then an expert panel, named by the President, set out a dramatic proposal for reform of the NSA surveillance activities and establishment of new privacy safeguards. They recommended that the NSA get out of the business of domestic surveillance, called for more judicial oversight, and recommended the creation of a new privacy agency. Many of the panel’s recommendations included proposals that EPIC has long championed.

We know that there are still many debates, many cases, many hearings, and much work ahead. But if you have any doubt that this is important work, consider that Mr. Snowden finished second to the Pope as Time Person of the Year and that “privacy” is the Word of the Year, according to Dictionary.com.

It takes a talented staff, expert advisors, and dedicated supporters to accomplish what we have managed to achieve. Across a wide range of issues, from drone surveillance and biometric identification to consumer protection and new techniques for online privacy, EPIC has been on the front lines from the start, working to safeguard privacy and promote civil liberties.

Thank you for your interest in our work.

*Marc Rotenberg*  
EPIC President

**IN RE EPIC and RELATED EPIC CASES**

In early June 2013, a previously secret order of the Foreign Intelligence Surveillance Court was made public. The order revealed that the NSA was routinely collecting the telephone records of all phone customers in the United States. The government claimed that the records were “relevant” to an “authorized investigation.” It was an unbelievable legal claim.

EPIC developed a legal response. Working closely with experts in privacy and national security law, EPIC prepared a petition to the US Supreme Court, urging the Court to find that the order was unlawful. Dozens of legal scholars and former members of the Church Committee joined the EPIC petition. *In re EPIC* was widely discussed. Unfortunately, the Supreme Court chose not to take the case. But EPIC did not stop.

- EPIC organized a grassroots petition, urging the National Security Agency to comply with the requirements of the federal Privacy Act
- EPIC filed a lawsuit against to obtain the legal memorandum about the NSA’s PRISM program, which involves the collection of data of Internet users.
- EPIC discussed challenge to the NSA telephone record collection program at conferences across the country and events at the Aspen Institute, the Council on Foreign Relations, the National Press Club, Georgetown University Law Center, New York University Law School, Stanford Law School, and Yale Law School.



*In re EPIC*, the Petition to end the NSA Telephone Record Collection Program

## EMERGING PRIVACY ISSUE SPOTLIGHT – DRONE SURVEILLANCE

When the news broke that the White House intended to dramatically increase the number of aerial drones in the United States, EPIC looked closely at the privacy risks. To be sure, there are many good uses for drone technology – better news reporting, improved land management, and better crisis response. But the risks are also real. Drones falling from the sky will not be good for public safety. And intrusive camera surveillance will not be good for personal privacy. So, EPIC went to work:

- EPIC organized a public event at the National Press Club in January -- “Drones and Domestic Surveillance” -- with leading technical experts and legal scholars, representatives of the drone industry and Members of Congress.
- EPIC petitioned the Federal Aviation Administration to develop privacy regulations. In February, the Agency agreed to establish a privacy policy for drone test sites. EPIC has pressed the Agency to establish privacy safeguards for all domestic drones.
- EPIC testified before the United States Senate on legislation to establish new privacy safeguards for the use of drones in the United States
- EPIC pursued a Freedom of Information Act request which revealed that the aerial drones deployed by the Department of Homeland Security had the ability to conduct human identification on the ground.
- EPIC participated in rallies across the United States concerning drone surveillance and spoke with news organizations about the issue.



EPIC's Amie Stepanovich Testifies before  
The US Congress About Drone Surveillance

**EPIC IN CONGRESS**

EPIC continued to provide objective advice to Congressional committees, state legislatures, federal agencies and the White House about emerging civil liberties issues. For several years, EPIC had urged Congress to consider the impact of increased drone deployment in the United States. As with many new technologies, privacy consequences should be fully assessed, and where new risks are identified, solutions should be found and implemented.

- In March 2013 EPIC testified before the Senate Judiciary Committee hearing on “The Future of Drones in America” in support of new privacy safeguards prior to the deployment of drones in the United States.
- EPIC met with the President’s Intelligence Review panel in September 2013 and explained that the current NSA telephone record collection program was unlawful and presented a series of changes to reform the FISA.
- EPIC appeared before the Privacy and Civil Liberties Oversight Board to urge FISA reform and to recommend that the Board pursue a broad agenda that covers “fusion centers,” integrated surveillance, and Privacy Act compliance.
- EPIC staff also testified before state legislatures on several issues, including student privacy (Colorado), cell phone records and location privacy (Texas, Maryland), and drone surveillance (Oklahoma).



EPIC’s Marc Rotenberg speaks before the Privacy and Civil Liberties Oversight Board

## EPIC OPEN GOVERNMENT PROJECT

People are often surprised to learn that EPIC runs one of the leading Open Government programs in the United States. They shouldn't be. Promoting government transparency is the other side of protecting personal privacy. The aim on both fronts is to protect the rights of the individual and to hold government accountable.

All EPIC staff pursue open government complaints. Even our summer clerks help us draft and submit Freedom of Information Act requests. And EPIC in association with the Georgetown University Law Center, just finished another semester of the Open Government Litigation clinic to teach law students the elements of FOIA litigation

2013 marked one of EPIC's most successful years ever in open government efforts. Not only did EPIC uncover important public information in federal agencies and create favorable precedent in federal court, increasingly EPIC is able to obtain attorneys fees in cases against federal agencies. In 2013, EPIC obtained fees in FOIA cases against the CIA, the Department of Education, the Department of Homeland Security, the FBI, and the Office of the Director of National Intelligence. Other highlights from the past year include:

- A favorable determination that the Department of Homeland Security should explain when it intends to use the "Internet kill switch," a technical procedure that can shut down local WiFi networks and cell phone service (*EPIC v. DHS*, No. 12-260).
- EPIC obtained a copy of the Inspector General's report that confirmed the CIA's collaboration with the New York Police Department in domestic surveillance efforts. EPIC's findings were widely covered in the news media, including a front-page story in the *New York Times*. (*EPIC v. CIA*, No. 12-2053).
- As a result of a FOIA lawsuit against the Department of Homeland Security, EPIC obtained documents which reveal that the Department of Defense required companies to disclose information about Internet traffic on private networks. These documents contradict Homeland Security's assertions that companies participating in a the pilot project would not be required release user data to federal agencies. (*EPIC v. DHS*, No. 12-333).
- New FOIA procedures at the Privacy and Civil Liberties Oversight Board, based on extensive comments provided by EPIC, will make it easier for the public to learn about the activities of the oversight panel.



- As a result of a FOIA lawsuit against the FBI, EPIC has also received documents about the agency's development of a biometric identification system that will include fingerprints, iris scans, DNA profiles, voice identification profiles, and palm prints. The documents EPIC has obtained will help the public respond to this biometric data collection. (*EPIC v. FBI*, No. 13-442).
- EPIC won a contested fee dispute with the Department of Homeland Security. In that case, EPIC obtained documents which revealed that the DHS was monitoring news organizations and twitter feeds. The court described EPIC's work in the case as "the sort of public benefit that FOIA was designed to promote." (*EPIC v. DHS*, No. 11-2261).
- EPIC is currently pursuing more than a dozen FOIA law suits, including cases concerning the FBI's interception of cell phone location data, the NSA's warrantless collection of internet user emails, the State Department's access to anonymous online activism information, and the Justice Department's legal authority to collect bulk internet and email metadata.
- EPIC is also pursuing many FOIA requests, including requests for information regarding Hemisphere, the largest telephone record collection program reported to date; Presidential Directive 21, a cybersecurity directive that authorizes DHS to monitor cyber network traffic in real time; and BitCoin, the digital currency that can protect user anonymity.

NGI shall return the correct candidate a minimum of 85% of the time, when it exists in the searched repository, as a result of a facial recognition search in support of photo investigation services.

NGI shall return an incorrect candidate a maximum of 20% of the time, as a result of facial recognition search in support of photo investigation services.

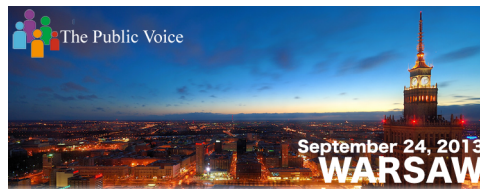
In *EPIC v. FBI*, EPIC obtained a document which revealed that the FBI will rely on a facial recognition search techniques that are wrong 20% of the time.

*For more information about EPIC's FOIA work, visit [www.epic.org/foia](http://www.epic.org/foia)*

## EPIC PUBLIC VOICE PROJECT

EPIC has long worked with civil society organizations in the United States and around the world on issues of common concern. Our aim is to provide constructive dialogue between civil society leaders and government decisionmakers. In Washington, DC, the Privacy Coalition provides an opportunity for consumer privacy organizations to meet with public officials away from special interests, to discuss issues of genuine concern to Internet users and consumers. The Public Voice coalition was established to bring civil society to key meetings with officials around the world. Over the long history of the Public Voice project, EPIC has organized conferences in more than a dozen countries on topics ranging from privacy and data protection, to freedom of expression, open government, Internet governance, cyber security, encryption policy, and consumer protection.

- In September, 2013, the Public Voice project organized an international conference in Warsaw in conjunction with the annual meeting of the Privacy and Data Protection Commissioners. “Our Data, Our Lives” explored a wide range of challenges facing those in the field of data protection and continued the dialogue on the Madrid Declaration, first adopted at a Public Voice conference held in Madrid in 2009.
- The Public Voice project supported the participation of civil society organizations at the OECD, specifically on Internet policy issues.
- In 2013, the Privacy Coalition organized meetings in Washington, DC for consumer privacy organizations with FTC Commissioner Maureen Olhausen, PCLOB Chair David Medine, the FTC Director of Consumer Protection Jessica Rich, FTC Chair Edith Ramirez, and others.



“Our Data, Our Lives”  
2013 Public Voice conference held in Warsaw

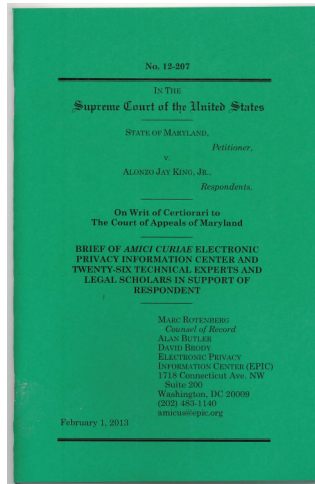
*Learn more about the Public Voice project at [www.thepublicvoice.org](http://www.thepublicvoice.org)*

EPIC routinely files “friend of the court” briefs in matters concerning new technologies and privacy law. EPIC does not simply argue that privacy is important or echo the arguments made by one of the parties in a case. Following the tradition of the “Brandeis brief,” EPIC amicus briefs are carefully researched reports on current government and business practices that impact personal privacy. Members of the EPIC Advisory Board, distinguished leaders in their areas of expertise, review and endorse the amicus briefs filed by EPIC. The importance of ongoing participation in privacy cases is clear. In 2013, many of the key decisions by the Supreme Court, both favorable and not, were marked by 5-4 majorities.

- In *Maracich v. Spears*, the Supreme Court considered a challenge to a key provision of the Drivers Privacy Protection Act. EPIC's amicus brief detailed the staggering amount of personal information in driver's records, particularly as a consequence of the REAL ID regulations. In June 2013, the Supreme Court upheld the law 5-4.
- In *Maryland v. King*, EPIC argued to the Supreme Court that DNA profiling reveals sensitive personal information about arrestees and their families, and that the indefinite retention of DNA samples risks further exposure from future expansions of DNA profiling. The EPIC amicus, joined by technical experts and legal scholars, detailed the extensive DNA collection practices across the criminal justice system. The Supreme Court upheld the Maryland DNA Collection Act 5-4.
- In *Clapper v. Amnesty Int'l*, EPIC filed an *amicus* brief, joined by experts in surveillance and privacy law, discussing the NSA's intelligence collection capabilities and emphasizing the need for judicial oversight and transparency. The Supreme Court issued a 5-4 opinion, holding that the claims that the NSA had engaged in unlawful surveillance were “too speculative.” Justice Breyer, writing in dissent, cited EPIC's amicus brief concerning NSA's surveillance capabilities and the likelihood that unlawful surveillance had occurred.
- In *Florida v. Harris*, the Supreme Court considered whether the use of a drug-detection dog was sufficient to establish probable cause to search an automobile. EPIC filed an *amicus* brief in *Harris*, highlighting a recent report by the National Academy of Sciences that detailed the lack of reliable standards for forensic investigatory techniques. The Court overturned the lower court

decision, holding that the dog’s reliability was properly established under the “totality of the circumstances” test.

- EPIC also filed an *amicus* brief in *Jennings v Broome*, joined by nineteen privacy, civil liberties, and consumer organizations, arguing that the it is critically important to clarify the application of federal privacy law to stored e-mail messages. The Supreme Court denied the petition in April 2013.
- In *Joffe v. Google*, a federal appeals court considered whether Google could lawfully gather private communications from residential Wi-Fi networks. EPIC’s *amicus* brief traced the development of consumer Wi-Fi products and explained that private networks are not “readily accessible” to the general public. The court ruled that Google had violated the federal wiretap act.
- In *State v. Earls*, EPIC filed two *amicus* briefs and argued in court that cell phone technology enables tracking of individuals with increasing precision, and can reveal private details about activities within constitutionally protected spaces. The Court held unanimously that individuals have a reasonable expectation of privacy in their cell phone location information under the New Jersey Constitution.



EPIC Amicus brief in *Maryland v. King*, concerning the collection of DNA samples

Learn more about EPIC Amicus Briefs at <http://epic.org/amicus/>

## EPIC AND CONSUMER PROTECTION

From its early days, EPIC has worked to ensure that the Federal Trade Commission, the Federal Communications Commission, and other agencies help protect the privacy of consumer and Internet users. In a series of high-profile complaints brought in 2009 and 2010, with the support of other consumer privacy organizations, EPIC helped the FTC establish comprehensive privacy programs for Google and Facebook.

In 2013, EPIC pursued several high profile complaints to the FTC and the FCC, as well as working closely with State Attorneys General across the country.

- Following an announcement from Facebook that it planned to modify its privacy policy so that it could use the images of minors for commercial endorsement without their consent, EPIC alerted the Federal Trade Commission that the change would violate the consent order with the FTC.
- EPIC asked the FTC to determine whether Jay-Z's new app for "Magna Carta" violated consumer protection law by collecting so much data from users without their knowledge or consent. EPIC's complaint put the app privacy issue squarely before the music industry.
- EPIC also asked the FTC to examine Snapchat, a popular photo sharing service, that tell users that it will instantly delete photos. Research by EPIC revealed that the photos on Snapchat could be retrieved.
- EPIC asked a key financial agency in Washington to consider the privacy risks created by the use of social media by financial institutions.
- EPIC spoke at the annual conference of the National Association of Attorneys General in Washington DC and worked with NAAG staff throughout the year on efforts to strengthen privacy for students.
- In November 2013, EPIC staff spoke at the FTC workshop on "The Internet of Things: Privacy and Security in a Connected World."

## **EPIC COMMENTS TO THE FEDERAL AGENCIES**

Since its founding, EPIC has submitted more than 100 comments to federal agencies, urging compliance with the federal Privacy Act, better rules for transparency, and more government accountability.

In the past several years, EPIC turned its attention to the TSA's ill-conceived plan to deploy backscatter x-ray devices in US airports. After extensive review, EPIC determined that there were significant privacy risks, and that the value of the devices had been greatly overstated. Medical experts also expressed concern about the machines' health impacts. EPIC launched a campaign to force the removal that began with a Spotlight on Surveillance report, and continued with petitions to the DHS Secretary, eventually winning a court-ordered federal rulemaking. Early in 2013, all backscatter x-ray devices were removed from US airports. No longer will government officials look at the naked images of air travelers.

In 2013, EPIC provided several important comments to federal agencies.

- EPIC submitted extensive comments opposing TSA's decision to deploy body scanners in US airports. EPIC also led a successful campaign encouraging the public to comment on the rulemaking. The public submitted more than 5,000 comments largely opposing TSA's body scanner program. The agency has since removed the x-ray devices from airports.
- In comments to the Privacy and Civil Liberties Oversight Board, EPIC urged the agency not to adopt proposals that would weaken the Freedom of Information Act and Sunshine Act. The Board adopted nearly all of EPIC's recommendations.
- EPIC, joined by a coalition of privacy, consumer rights, and civil rights organizations, and members of the public, pushed the National Highway Traffic Safety Administration to protect driver privacy and establish privacy safeguards for car black boxes.
- EPIC led a coalition of privacy and civil rights advocates in pressing the Department of Defense to require the National Security Agency to comply with the Privacy Act.

**EPIC STUDENT PRIVACY PROJECT**

EPIC has a longstanding interest in the protection of information of young people. EPIC contributed to the development of the Children's Online Privacy Protection Act, as well as the new COPPA regulations adopted by the Federal Trade Commission. EPIC has also filed briefs and comments in support of "FERPA," the federal law designed to protect the privacy of educational records. EPIC's activities in 2013 included:

- Publishing an article on the growing risks to student privacy resulting from the change in the FERPA rule. (EDUCAUSE January 2013)
- Participating in workshops on Student Privacy and Cloud Computing organized by the Berkman Center for Internet & Society.
- Pursuing a case against the US Department of Education concerning changes to FERPA that reduce safeguards for student data. The court dismissed the case on procedural grounds.
- Pursuing a Freedom of Information Act case against the Department of Education, in which EPIC obtained documents revealing that many private debt collection agencies maintain incomplete and insufficient quality control reports. (EPIC v. Dept. of Ed., No.13-345).
- Filing an extensive complaint with Federal Trade Commission concerning Scholarships.com's sale of sensitive student data.
- Testifying before the Colorado State Board of Education regarding private companies' acquisition of sensitive student information.
- Leading webinar presentations on student privacy trends.
- Urging Congress to restore privacy protections for student data and investigate the impact of the revised FERPA rules.

## EPIC PUBLICATIONS

Throughout the year, EPIC staff published articles and letters in academic journals and mainstream publications

"Amassing Student Data and Dissipating Privacy Rights", EDUCAUSE (January 2013), Marc Rotenberg & Khaliah Barnes

"Are Vehicle Black Boxes a Good Idea?" Costco Connect (April 2013), by Marc Rotenberg

"Protecting Privacy: The Role of the Courts and Congress," ABA Human Rights Magazine (March 2013), Marc Rotenberg and David Brody

"Updating the Law of Information Privacy: The New Framework of the European Union," Harvard Journal of Law and Public Policy (Spring 2013), Marc Rotenberg and David Jacobs

"Can you hear me now? The surveillance state must be reined in," The Washington Times, June 10, 2013, Amie Stepanovich

"Supreme Court must protect our privacy from the government," Special to CNN (July 17, 2013), by Marc Rotenberg

"Better Privacy Laws: Priority for America and Germany," The New York Times (September 3, 2013), Marc Rotenberg

"Protecting Data Privacy," The New York Times (November 5, 2013), Marc Rotenberg

"Square Peg, Round Hole - How the FISC has misapplied FISA to Allow for Bulk Metadata Collection," Just Security (December 2, 2013), Alan Butler and Amie Stepanovich

"When Cyberweapons End Up on Private Networks: Third Amendment Implications for Cybersecurity Policy," American University Law Review (2013), Alan Butler



**EPIC IN THE NEWS**

EPIC's mission is to focus public attention on emerging privacy and civil liberties issues. Toward that goal, EPIC maintains a strong media presence. EPIC staff are routinely interviewed about EPIC's work.

- In 2013, EPIC staff participated in more than 300 media interviews, speaking with every major media organization in the United States including The Boston Globe, The Economist, The Los Angeles Times, The New York Times, USA Today, The Wall Street Journal, and The Washington Post, as well as the The Atlantic, Ars Technica, The Associated Press, CNET, The Financial Times, Forbes, Legal Times, Mediapost, Politico, Reason, Reuters, Rolling Stone, Slate, Salon, TechDirt, Techworld, The Washington Post, and Wired.
- In 2013, EPIC staff was interviewed by Bloomberg, ABC News, Al Jazeera America, BBC, CBS News, CNN, C-Span, Fox News, Huffington Post Live, MSNBC, NBC News, NPR, On the Media, and many local radio and television stations.
- And EPIC's legal work was cited by Courthouse News, Constitution Daily, FindLaw, Justia, JustSecurity, Law360, Lawfare, Legal Times, ScotusBlog.



EPIC's Marc Rotenberg discusses NSA Surveillance with Charlie Rose



EPIC's Khaliah Barnes discusses tracking of shoppers on CBS

Learn more about EPIC in the News at [http://epic.org/news/epic\\_in\\_news.html](http://epic.org/news/epic_in_news.html)

## EPIC STAFF AT CONFERENCES

In 2013, EPIC staff spoke at more than 100 events in the United States and around the world. Here is a sample:

"Bridging the EU-US Privacy Divide," CPDP 2013 Brussels, Belgium, January 2013

"The New Frontier: Policy & Politics in the Age of the Internet," Georgetown Public Policy Institute, US Congress, Washington, DC, February 2013

"Drones.edu: Hands on the Future in the Classroom," SXSW, Austin, March 2013

"Travel Surveillance, Traveler Intrusion," CATO Institute, Washington, DC, March 2013

"Cellular phones and mobile privacy: Direct government surveillance (Stingrays)" Yale Law School, New Haven, CT, March 2013

"Online Privacy: Consenting to Your Future," European Commission, Malta, March 2013

"Privacy in the Digital Age," National Association of Attorneys General, National Harbor, MD, April 2013

"Privacy and Government Surveillance," Florida State University College of Law Tallahassee, FL, April 2013

"ASAP 6th Annual National Training Conference," Arlington, VA, May 2013

"All Eyes on Privacy: Transparency in the New Economy," The National Journal / The Atlantic, Newseum, Washington DC June 2013

"Twitter Activism: What the Success of #PrivChat Can Teach You," Computers, Freedom, and Privacy, Washington, D.C., June 2013

"The Snitch In Your Pocket," Chautauqua Institution, Chautauqua, July 2013

"NSA Surveillance and Foreign Affairs," Yale Law School, Information Society Project, New Haven, September 2013

"Terms and Conditions May Apply," Camden International Film Festival, Camden, ME, September 2013

"The Foreign Intelligence Surveillance Act - What's Working and What Needs Fixing?" Federal Communications Bar Association, Washington, DC, February 2013

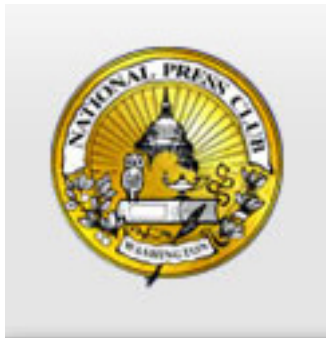
"Surveillance conference," Northwestern University School of Law, Chicago, IL, October 2013

"Does the U.S. have the balance between American civil liberties and its surveillance practices correct?" Council on Foreign Relations, New York city, November 2013

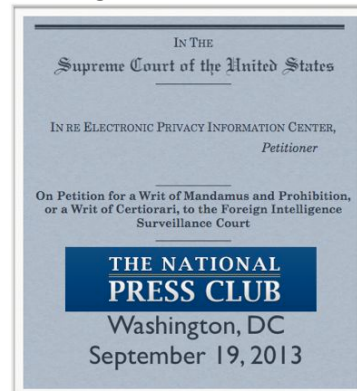
"The Year in Government Information: NSA Surveillance, Bin Laden Photos, White House Logs and More," ABA Administrative Law Conference, Washington, DC, November 2013

"When Worlds Collide: Technology, Privacy, and Security," Appellate Judges Education Institute, San Diego, CA, November 2013

"Student Privacy and Cloud Computing Working Meeting," Berkman Center, Harvard Law School, Cambridge, MA, November 2013



"Drones and Domestic Surveillance"  
National Press Club  
January 23, 2013



"In re EPIC"  
National Press Club  
September 19, 2013

Learn more about EPIC events at <http://epic.org/events/>

## EPIC ONLINE

EPIC began in 1994 with the Internet's first online petition, the effort to shut down the government's ill-conceived Clipper Chip encryption scheme. Since that time, EPIC has continued to pursue innovative online techniques to educate the public, provide information, and promote debate on emerging privacy and civil liberties issues.

- EPIC maintains several of the leading privacy websites in the world, including [www.epic.org](http://www.epic.org) and [www.privacy.org](http://www.privacy.org)
- EPIC hosts the Privacy Coalition at [www.privacycoalition.org](http://www.privacycoalition.org)
- Throughout the year EPIC hosted #privchat, a weekly meeting for Internet activists concerned about online privacy
- EPIC is on Twitter at @EPICprivacy. Follow us!
- EPIC is on Facebook. Facebook.com/epicprivacy. Like us!
- EPIC updated its popular web page Practical Privacy Tools. [epic.org/privacy/tools.html](http://epic.org/privacy/tools.html)
- EPIC updated and expanded its online donation form, giving using contributors new ways to support EPIC while protecting privacy and always reserving the opportunity for anonymous donations. [www.epic.org/support](http://www.epic.org/support).



EPIC remains focused on emerging privacy and civil liberties issues. Here are a few of the issues we will be tracking in 2014:

Protection of Student Data. The increased testing of American students coupled with the commercialization of educational data is putting at risk future opportunities for a generation of Americans. EPIC will be pursuing a multi-faceted campaign in 2014 to restore privacy rights for students.

FBI Biometric Database. With all of the focus on the NSA this past year, few have noticed the development of the world's largest biometric database. EPIC will push for greater oversight of the FBI's new identification program.

Facial Recognition. As technology for facial recognition improves so too do the risks to privacy. Simply stated this is a technology that allows strangers to obtain your actual identity. We think further study is necessary before there is widespread use by the government and the private sector.

FTC Enforcement. The Federal Trade Commission has been reluctant to enforce important settlements with Facebook and Google or to mandate the Consumer Privacy Bill of Rights. EPIC will be stepping up efforts in 2014 to ensure that the FTC does more to safeguard Internet privacy.

Privacy Rights of the Press. Reporters in the United States are increasingly under scrutiny by the government because of the stories they write and the people they know. EPIC will be working more closely with press association to help safeguard the rights of reporters.

Promoting the Public Voice. EPIC will continue to work with civil society groups around the world to protect fundamental human rights.

"Privacy is Fundamental." Our theme for 2014. Think about it.

In 2014, EPIC will also celebrate its 20<sup>th</sup> anniversary. Join us to celebrate 20 years of privacy advocacy. More information at [www.epic.org/epic20th/](http://www.epic.org/epic20th/)

## EPIC BOARD AND EPIC ADVISORY BOARD

The EPIC Advisory Board is composed of distinguished experts in law, technology, and public policy.

Alessandro Acquisti	Charles M. Firestone *	Craig Newmark
Steven Aftergood	Addison Fischer *	Helen Nissenbaum
Phil Agre	David Flaherty	Eli Noam
Anita Allen	Philip Friedman	Ray Ozzie *
John Anderson	Michael Froomkin	Frank Pasquale
Ross Anderson	Urs Gasser	Harriet Pearson
Jack Balkin	Pamela Jones Harbour *	Deborah Peel *
James Bamford	Austin Hill	Stephanie Perrin
David Banisar	Aziz Huq	Chip Pitts
Grayson Barber *	Deborah Hurley *	Anita Ramasastry
Ann Bartow	Kristina Irion	Ronald L. Rivest
Colin Bennett	Joi Ito *	Jeffrey Rosen
Francesca Bignami	Jeff Jonas	Pam Samuelson
Christine Borgman *	Brewster Kahle	Bruce Schneier
danah boyd	Jerry Kang	Barbara Simons
Stefan Brands	Sheila Kaplan	Paul M. Smith
David Burnham	Pamela S. Karlan **	Robert Ellis Smith
Ryan Calo	Ian Kerr	Eugene Spafford
David Chaum	Orin Kerr	Latanya Sweeney **
Julie Cohen	Pradeep K. Khosla	Frank Tuerkheimer
Bill Coleman	Michael Kirby	Sherry Turkle
Susan Crawford	Chris Larsen	Ed Viltz
Simon Davies	Rebecca Mackinnon	Willis Ware
Whitfield Diffie	Gary Marx	Chris Wolf
Laura Donohue	Mary Minow	Paul Wolfson
Cynthia Dwork	Pablo G. Molina *	Tim Wu
David Farber *	Peter Neumann *	

\*: EPIC Board of Directors members

\*\* : On leave from EPIC Advisory Board, 2014-2015

### EPIC Board Officers

Deborah Hurley, Chair  
Marc Rotenberg, President  
Pablo Molina, Treasurer

Grayson Barber, Secretary



**Marc Rotenberg**  
EPIC President and  
Executive Director



**Julia Horwitz**  
EPIC FOIA Counsel and Coordinator,  
EPIC Open Government Project



**Khaliah Barnes**  
EPIC Administrative  
Law Counsel and Director,  
EPIC Student Privacy Project



**David Jacobs**  
EPIC Consumer Protection Counsel



**Alan Butler**  
EPIC Appellate Advocacy Counsel



**Jeramie Scott**  
EPIC National Security Counsel, and  
Coordinator, Privacy Coalition



**Amie Stepanovich**, Director  
EPIC Domestic Surveillance Project  
and Coordinator EPIC Clerks Program



**Caitriona Fitzgerald**  
EPIC Technology Fellow



**Gerald Tan**  
EPIC Administrative Director



**Beth Rosenberg**  
EPIC Alert Editor



**David Husband**  
EPIC Appellate Advocacy Fellow

For their work and help in 2013,  
thanks also to

Lillie Coney  
Ginger McCall  
Tom Moore

**Adam Marshall**  
EPIC Internet Activist

#### **EPIC 2013 Law Clerks**

Christopher Boone, Duke  
Elizabeth Hempowicz, American  
Eric Holmes, New York University  
Natalie Kim, Harvard  
Alexander Lopez, New York University  
Adam Marshall, George Washington  
Sarah McSweeney, College, Cork  
Heather Nodler, Georgetown  
Daniel Rockoff, New York University  
Aimee Thomson, New York University  
John Tran, Georgetown



**EPIC Champions of Freedom**

Sen. Patrick Leahy (2004)  
D.J. Caruso (2009)  
Rep. Ed Markey (2009)  
Paul Smith (2009)  
Prof. Pam Samuelson (2009)  
Rep. Joe Barton (2010)  
Addison Fischer (2010)  
Pamela Jones Harbor (2010)  
The Rose Foundation (2010)

Rep. Jason Chaffetz (2011)  
The Wall Street Journal (2011)  
Rep. Rush Holt (2011)  
Sen. Al Franken (2012)  
Judge Alex Kozinski (2012)  
Dana Priest (2012)  
Martha Mendoza (2013)  
Sen. Rand Paul (2013)  
Sen. Ron Wyden (2013)

**EPIC US Privacy Champions**

Beth Givens (2010)  
Jeff Chester (2011)  
Christopher Soghoin (2012)  
Susan Grant (2013)

**EPIC International Champions of Freedom**

Prof. Stefano Rodota, Italy (2009)  
Hon. Michael Kirby, Australia (2010)  
MEP Sophie In't Veld, Holland (2011)  
Jennifer Stoddart, Canada (2012)  
Max Schrems, Austria (2013)

**EPIC Lifetime Achievement**

Whitfield Diffie (2012)  
Wilis Ware (2012)  
David Flaherty (2013)

The 2014 EPIC Champion of Freedom Awards will be presented in Washington, DC on June 2, 2014.

## EPIC FINANCIAL STATEMENTS

(EPIC 2013 End of Year Financial Statements will be available late January 2014.  
EPIC's 2012 Financial Statements and 2012 Form 990 are available at the EPIC website.)

*What a year it's been.*

*A Supreme Court petition was filed by EPIC to stop NSA's telephone record collection program. Highly visible, it catalyzed tremendous discussion.*

*EPIC developed a privacy framework as it pertains to drone surveillance in the US. This is so important given where drones are headed.*

*EPIC kept pressure on commercial organizations to genuinely respect the ongoing privacy interests of their customers. EPIC also pursued numerous requests aimed at making the government more accountable, and won FOIA lawsuits against the CIA, the DHS, the FBI, the ODNI, and the Department of Education. We all hope and want to believe our gov't will be transparent and accountable. But in reality, hope's not sufficient. EPIC acts.*

*And of course, EPIC repeatedly brought together political leaders, agency heads, privacy advocates and tech experts toward advancing the development of new approaches to protect our online privacy. Not just reactive, EPIC's acting for our future.*

*Thanks to the entire staff of EPIC, for continuing to lead, continuing to take action, and continuing to catalyze dialog that's so necessary in this world that – for better and with risks – has fully embraced the pervasive sensing, recording and analysis of most everything we do.*

*Ray Ozzie  
EPIC Board Member,*

**Electronic Privacy Information Center (EPIC)**

1718 Connecticut Ave., NW Suite 200  
Washington, DC 20009

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

@EPICprivacy