ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
THE EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET

"Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites"
Docket E9-17756
E-mail: oira_submission@omb.eop.gov

August 10, 2009

Introduction

The Office of Management and Budget (OMB) requested comments on its current prohibitions on Web tracking technologies, such as persistent cookies.[1] The agency stated that the goal of the policy review is "to continue to protect the privacy of people who visit Federal Government Web sites while at the same time making these Web sites more user-friendly, providing better customer service, and allowing for enhanced Web analytics."[2]

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington D.C. Established in 1994 EPIC continues to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in the establishment and enforcement of strong federal privacy laws and government agency regulations that safeguard personal information from over collection, retention, abuse, and misuse by government agencies. We also have a well-established interest in the opaque use of Web tracking technologies in online commercial settings.

Comment on Rulemaking

At the outset, EPIC notes that the OMB notice (1) provided less than two weeks for public response, (2) was unusually vague for a federal register notice, and (3) fails to mention the obvious links to private sector vendors. These defects in the Federal Register are significant. First, without a meaningful opportunity for the public to comment on a proposed policy change, the likelihood that the agency will make a final decision without regard for public opinion necessarily increases.

[1] Federal Register Notice, Office of Management and Budget, Volume 74, Number 142, July 27, 2009, available at http://edocket.access.gpo.gov/2009/E9-17756.htm , July 27, 2009
[2] *Id.*

Second, the lack of clarity and detail in the OMB notice makes it difficult for the public to provide a meaningful assessment. In this instance, the agency proposes a multi-tier framework for the use of persistent cookies across the federal government but fails to provide any detail as to how such a framework might be applied. For example, would queries across one agency always operate at the same tier? How would users, i.e. citizens, be notified when government tracking techniques are being deployed? Given that such a multi-tiered framework would reverse previous agency policy, it is vital that the public have clarity on the scope and details of the proposal before it is asked to comment.

The OMB throws these questions back to the public without ever providing a clear statement as to what its own plans will be. This is an almost meaningless form of public rulemaking as the agency will be free to produce any policy it wishes and selectively choose comments to support its conclusions.

Finally, the agency rulemaking fails to explain the significant role that private sector vendors will play in many of the applications that are driving the effort to revise the federal government's policy on persistent identifiers. Without providing this information to the public, it is difficult to fully assess the impact that the proposed change will have, particularly on the ability of private firms to monitor the activities of US citizens who seek public information from government web sites.

Taken as a whole, the nature of this public comment procedure undermines government transparency, the Administrative Procedure Act, and the type of public engagement that the President urged in his January 2009 executive order.[3]

Background

On June 22, 2000, the Office of Management and Budget published *Privacy Policies and Data Collection on Federal Web Sites*. In September 2003, the agency issued guidance for implementing the Privacy Provisions of the E-Government Act of 2002. Both documents addressed the issue of federal agency use of Web tracking technologies and correctly rejected their broad adoption. In 2006, federal agencies violated these rules barring the use of web tracking technology by secretly placing cookies on the computers of visitors to their web sites.[4] Violators included the Department of Defense, Department of The Treasury, and the National Security Agency. All of these agencies used permanent cookies in violation of the OMB regulation. In some cases the cookies were managed through a private vendor

[3] Executive Order, President Obama, available at http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/, January 21, 2009

[4] "Government Web sites are keeping an eye on you," Declan McCullagh and Anne Braoche, CNET News, available at http://news.cnet.com/Government-Web-sites-are-keeping-an-eye-on-you/2100-1028_3-6018702.html, January 5, 2006

(WebTrends), while others were set using Adobe Web Development software (ColdFusion). Following media disclosure of these violations, agencies suspended the use of Web tracking technology.

The use of Web tracking by private sector developers and adopters has not disclosed the technology's full range of capabilities, nor have government oversight authorities had the capacity to independently investigate the extent of these capabilities. What is known about Web tracking technologies has come from intense independent investigations by researchers and advocacy organizations. These investigations reveal a not so pleasant view of the erosion of online privacy rights.[5] Web tracking capabilities can now include all logged information, such as search queries, IP-address information, browser, traffic information, and usage based on date and time.[6]

Comments on Register Notice on Revision of Policy Regarding Federal Agency Use of Web Tracking Technologies

a) "Under a framework that we are considering, any Federal agency using Web tracking technologies on a Federal Government Web site would be subject to basic principles governing the use of such technologies and would be required to: Adhere to all existing laws and policies (including those designed to protect privacy) governing the collection, use, retention, and safeguarding of any data gathered from users;"

EPIC agrees with this premise but notes that federal agencies routinely exempt themselves from Privacy Act obligations. They also try to blunt the force of the Privacy Act by adopting "privacy principles" or contract out data management to third parties. Hence, the policy goal will only be meaningful if agencies are neither able to "opt-out" of privacy obligations nor enter into contractual arrangements where the intent of the Privacy Act is written out of enforcement.

Based on a series of documents recently obtained by EPIC from the General Services Administration under a Freedom of Information Act request, it is clear that the federal government has negotiated contracts with the private sector that fail to comply with existing statutory privacy rights. For example, a contract obtained from

[5] Privacy? Proposed Google/DoubleClick Merger, EPIC, available at http://epic.org/privacy/ftc/google/

[6] FTC Complaint and Request for Injunction in the Matter of Google, Inc. and DoubleClick, EPIC, available at http://epic.org/privacy/ftc/google/epic_complaint.pdf; and Supplemental Complaint, available at http://epic.org/privacy/ftc/google/supp_060607.pdf; and "Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices, Center for Digital Democracy, available at http://www.democraticmedia.org/current_projects/privacy/analysis/mobile_marketing#ftn6

GSA regarding Google's provision of a video player service for the government states:

> Provider acknowledges that, except as expressly set forth in this Agreement, Google uses persistent cookies in connection with the YouTube Video Player. To the extent any rules or guidelines exist prohibiting the use of persistent cookies in connection with Provider Content applies to Google, Provider expressly waives those rules or guidelines as they may apply to Google."[7]

b) "Post clear and conspicuous notice on the Web site of the use of Web tracking technologies;"

This is, in many respects, an incongruous proposal because it gives citizens an unreasonable choice—either accept an announced infringement of privacy or choose to not receive valuable information. For much of the information covered by this rulemaking, the federal government is the only source that citizens may go to for reliable information. As was the case of the H1N1 flu virus outbreak, rumors abounded, while agencies worked very hard to get the facts out the American public. What does it mean if the federal government provides a privacy warning sign on its web sites for citizens seeking access to public information? In most instances, there are no meaningful alternatives to receive the information. Making access to taxpayer funded sources of government information conditioned upon giving up Constitutionally protected privacy rights would neither be in the best interest of government nor the people it serves. The government should move aggressively to end agency use of Web blocking technology that prevents the archiving of government agency Web sites by services like the Internet Archive.

There is no sense in which "notice and choice" provides any meaningful privacy protection for a government web site. The use of a privacy notice in this way is truly Orwellian.

c) "Provide a clear and understandable means for a user to opt-out of being tracked;"

Visitors to government sponsored or hosted Web sites should not have to opt-out of the collection of personal information related to their visit. The point of privacy protection is to constrain the ability of information collectors to exploit the vulnerability of those seeking information. Requiring federal agency Web site visitors to accept opt-out cookies as a means to protect privacy places an unreasonable burden on the consumer. The practical impact of this approach to

[7] Content Hosting Agreement For Federal Entities [Contract between the General Services Administration and Google/YouTube], Effective 2009-02-19 (on file with EPIC).

privacy protection is to require a user to retain a cookie for every agency Web site for which he or she does not wish to be tracked.

A privacy approach to cookies allows users the option of not accepting a cookie. Under no circumstances should not accepting a government agency cookie lead to any other form of tracking technology being applied for any purpose once the user declines cookies from an agency sponsored or hosted site. There are techniques available that would enable government agencies to provide anonymous browsing without requiring users to accept cookies.

d) "Not discriminate against those users who decide to opt-out, in terms of their access to information;"

The worst form of privacy discrimination is to make access to information conditional upon the relinquishment of personal information. The mention of non-discrimination in the context of access to government information raises questions about what the Administration may know about past agency conduct as it relates to the use of Web tracking technology.

EPIC would appreciate clarification on what is meant by discrimination. For example: How would users report incidents of suspected discrimination? Would they be able to make reports anonymously? How would users be protected from agency adverse reactions to being reported? How will incidents of suspected discrimination be investigated and by whom? Would there be civil and criminal consequences for engaging in discriminatory behavior? Will there be transparency of an agency's discriminatory history through the imposition of annual reporting requirements or other requirements?

e) "OMB is currently considering the application of a three-tiered approach to the use of Web tracking technologies on Federal Government Web sites. A set of tiers that we are considering would be: 1st Single-session technologies--which track users over a single session and do not maintain tracking data over multiple sessions or visits;"

This statement leaves many questions unanswered regarding what the Administration has in mind. Without a detailed description of the "set of tiers" under consideration, how they are intended to work, and which agencies would be assigned to which tier a cogent reply to this section of the proposal is not possible. The Administration must also address how a change of Web tracking policy would mesh with ongoing cyber-security measures, which the public has been assured would involve no tracking or monitoring of non-government Web communications.

One of these programs is Einstein, which is operated by the Department of Homeland Security. Einstein's Privacy Impact Assessment described the program as

an effort to collect information on Web site traffic within government agency Web sites. [8] The information collected includes IP addresses, which can accurately be used to identify visitors to government agency hosted pages. However, with Web tracking technology visitor identification will be even easier since it can be used to continue tracking visitors once they leave government agency Web sites. In addition, the Einstein program's focus on suspicious behavior raises questions about what would raise suspicion and thereby justify tracking – solely activity related to visits of government hosted sites or activity that occurred once the user left those sites?

Prior to the adoption of a "set of tiers," EPIC requests that a full description and intended purpose of the proposal be set out in a Federal Register Notice published 60 days prior to this proposal going into effect. This includes an opportunity for public comment.

Privacy

The right of privacy is a personal and fundamental right in the United States. The privacy of an individual is linked to the collection, use, and dissemination of personal information. The opportunities to secure employment, insurance, and credit, to obtain medical services, the rights of due process, free speech, and dissent, are threatened by the misuse of personal information.[9]

The Privacy Act of 1974 was passed in response to concerns about how the creation and use of computerized databases might affect individuals' privacy rights. However, its scope was limited to federal government agencies. It safeguards privacy of federal government-held records through the creation of four procedural and substantive rights in personal data. First, the Privacy Act requires government agencies to show an individual any records kept on him or her. Second, it requires agencies to follow certain principles, called "fair information practices," when gathering and handling personal data. Third, it places restrictions on how agencies

[8]Einstein 2 Privacy Impact Accessment, Department of Homeland Security, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein2.pdf; and Cybersecurity Plan to Involve NSA, Telecoms, Ellen Nakashima, Washington Post, available at http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771.html, July 3, 2009

[9] "Town Requires Job Seekers to Reveal Social Media Passwords," Molly McDonough, ABA Journal, available at http://www.abajournal.com/news/town_requires_job_seekers_to_reveal_social_media_passwords/, June 19, 2009; Associate Press, 'Las Vegas Review-Journal' Served Federal Subpoena' available at http://www.editorandpublisher.com/eandp/news/article_display.jsp?vnu_content_id=1003984860, June 16, 2009; "Documents show state police monitored peace and anti-death penalty groups," Nick Madigan, Baltimore Sun, available at http://www.baltimoresun.com/news/maryland/bal-te.md.spy18jul18,0,5659230.story, July 18, 2008

can share an individual's data with other people and agencies. Fourth and finally, it allows individuals to sue the government for violating the provisions of the Act.[10]

Federal law enforcement, domestic security, and foreign intelligence agencies have routinely exempted themselves or ignored key provisions of the privacy act and/or Federal laws as they relate to the collection sharing, and use of personal information.[11]

Web tracking technology coupled with federal agency negotiated agreements with social networking sites Facebook, MySpace, Google (YouTube), SlideShare, VIMEO, AddThis, Blip Networks, Blist, and Flickr create a powerful new ability to collect information on online users. EPIC notes that Twitter is not included in the list of social networking companies known to have agreements with federal government agencies.

The tools of the national information infrastructure that are now at the disposal of federal government agencies can include the use of developer level platform applications. For example, Facebook supports a set of application programming interfaces and tools to facilitate external applications to access Facebook content. The company promotes developer driven tools as follows:

> You can build rich applications that run on Facebook and let users interact with each other. Or, with Facebook Connect, you can bring the social power of the Web to your own website.[12]

The questions about government use of application development and hosting are not limited to whether an agency is engaged in this activity, but whether they have contractors providing this service on their behalf. The Federal Privacy Act does not cover the collection, retention, sharing, and use of personal information by private entities. In addition, aside from Section 7, the Privacy Act does not cover state and local governments, though individual states may have their own laws regarding record keeping on individuals.

---

[10] Privacy Act of 1974, EPIC, available at http://epic.org/privacy/1974act/ (Accessed August 8, 2009)

[11] FOIA Work on National Security Agency's Warrantless Surveillance Program, EPIC, available at http://epic.org/privacy/nsa/foia/; Information Fusion Centers, EPIC, available at http://epic.org/privacy/fusion; DOD Recruitment Database, EPIC, available at http://epic.org/privacy/student/doddatabase.html; also see Domestic Surveillance Privacy Articles, http://privacy.org/cgibin/mt/mt-search.cgi?IncludeBlogs=2&search=domestic+spying , (Accessed August 8, 2009)

[12] Main Page, Facebook Developer Wiki, available at http://wiki.developers.facebook.com/index.php/Main_Page (Accessed August 8, 2009)

The excessive collection of personal data in the United States, coupled with inadequate legal and technological protections, has led to a dramatic increase in identity theft.[13] Data breaches are not limited to private sector firms, but have also extended to federal government agencies and designated programs.[14]

Web Tracking Technology and Privacy

Behavioral Targeting

Behavioral targeting is a technique used by advertisers that involves the secret collection of information about an individual's interests, actions, habits, and traits in both the offline and online worlds.[15] Theoretically, this improves the effectiveness of advertising by tailoring messages for individual consumers. The practice raises troubling privacy concerns and influences consumers through subconscious manipulation. Expanding behavioral targeting to include federal government agencies incurs an ominous threat to privacy, civil liberties, and constitutional rights.[16] The Department of Defense actively engages in something it calls "perception management" which attempts to influence public opinion.

Systems to deliver broadband Internet, digital television, and mobile services serve the needs of marketers. Advertisers have been in the forefront of plans to ensure that new communications technologies target individuals with sophisticated pitches, collecting lots of information about users in the process (consumer profiles).[17] These technologies have the capability to incessantly track the activity of users as they surf the Internet or watch television as well as the capability to use that information to tailor advertising for the greatest effect.

Long established ad industry metrics are now applied to our digital lives. "Web analytics" describes a software tool that is used to track users' navigation on individual websites and on the Web as a whole. The software analyzes how users relate to the content, and whether it is working effectively to connect users to the ad

---

[13] Fed. Trade Comm'n, Consumer Fraud and Identity Theft Compliant Data: January – December 2006 (Feb. 7, 2007), available at http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf (for the seventh year in a row, identity theft is the No. 1 concern of U.S. consumers).

[14] A Chronology of Data Breaches, Privacy Rights Clearinghouse, available at http://www.privacyrights.org/ar/ChronDataBreaches.htm, (Accessed August 8, 2009)

[15] Privacy and Human Rights: An International Survey of Privacy Laws and Developments, EPIC in association with Privacy International, available at http://epic.org/phr06/

[16] 'The Man Who Sold the War:' Marketing of Iraq, National Public Radio, available at http://www.cleveland.com/nation/index.ssf/2009/02/the_information_war_pentagon_s.html; and The information war: Pentagon surges spending on influencing public opinion at home, abroad, Chris Tomlinson, Associated Press, available at http://www.cleveland.com/nation/index.ssf/2009/02/the_information_war_pentagon_s.html, February 5, 2009

[17] Jeff Chester, Digital Destiny: New Media and the Future of Democracy (The New Press 2007).

by collecting "real-time" information on Internet behaviors. These behaviors include how a user got to a particular site and where they went afterward, how long they visited a site, and which content resulted in interest or interaction.

Commercial use of Web tracking focuses on developing analytics that will perfect micro-targeting applications intended to market more effectively to online customers. A Mobile Advertising Alliance white paper on the topic describes its goals for "Operator Analytics:"

> The Operator has exclusive access to detailed information on subscriber [behavior] and characteristics, including spending patterns, location, availability, interests (through browsing habits), social status (implied from device) as well as demographic data (at least for post-paid subscribers). This information is available across a range of disparate systems, but should be consolidated by an effective mobile advertising platform. [18]

The sentinels for Web analytics are cookies. Cookies are a general mechanism which server-side connections (such as CGI scripts) can use to both store and retrieve information on the client side of the connection. The addition of a simple, persistent, client-side state significantly extends the capabilities of Web-based client/server applications. To put it more plainly, a cookie is a mechanism that allows a web site to record your comings and goings, usually without your knowledge or consent.

Cookies

Cookies can make sure that returning visitors do not have to retype (or recall) such things as user names and passwords. But cookies are also linked to extensive profiling information that informs both the website and the online ad network about users' interests, shopping habits, and behavior. Users' IP addresses are another important piece of information, which allows advertisers to engage in marketing is "Advanced Geo-Targeting," a technique used to serve ads, based on income levels, ethnicity, and personal interest. Should the federal government engage in this level of engagement, the only piece of information it may lack are the personal interests of users of government online information services.

In a decade, Web tracking cookie technology has evolved to become more privacy invasive, while at the same time less transparent to users. The claim that Web tracking is an accepted practice begs for the qualification—in particular, that it is accepted by online service providers and marketers. Consumers are rejecting the

[18] "Implementing Multi-Channel Mobile Advertising Platform," Mobile Advertising Alliance, February 2008, http://www.mobileadvertisingalliance.com/downloads/MAA%20White%20Paper.pdf (Accessed August 8, 2009)

placement of cookies on their computers. According to a Jupiter Research study, 58% of online users have deleted cookies from their computer and 39% of users do so on a monthly basis.[19] This regular "cookie tossing" caused direct marketers to seek more invasive methods to track individuals. One of those methods is to set a "Local Shared Object," also known as a "Flash cookie" to track individuals.[20]

Flash Cookies

Simply put, the idea behind this tracking is to set two cookies on the user's machine--a standard cookie that the consumer may erase, and a second Flash cookie that the user probably will keep, because the existence of Flash cookies is not well known. Flash cookies are set through a mechanism in Macromedia's Flash MX player. According to Macromedia, 98% of computers have some version of Flash on them.

The administration needs to ask itself how far government should be allowed to encroach into the personal lives of online users. The government has the data wealth that online service providers might be willing to trade just about anything to have access to, while the service providers are collecting a massive amounts of detailed and continuously refreshed data on online users. EPIC makes the following recommendations in response to the Administration's request for comments.

Recommendations

The greatest protection of privacy is a state that disallows the collection of personal information under any circumstance. For this reason, the Administration should maintain the current ban on Cookie use. However, if the administration moves forward with changing federal agency policy regarding the use of cookies, EPIC makes the following recommendations:

- Do not track users once they depart cookie hosted government sponsored web sites or information portals.[21]
- Prohibit commercialization of information on users who visit government sponsored social media resources. [22]

---

[19] Press Release, Accurate Web Site Visitor Measurement Crippled by Cookie Blocking and Deletion, Jupiterresearc Finds, Press Release, available at http://www.webmediabrands.com/corporate/releases/05.03.14-newjupresearch.html

[20] Local Shared Objects -- "Flash Cookies," EPIC,, available at http://epic.org/privacy/cookies/flash.html (Accessed August 7, 2009)

[21] "Users Are Not Tracked on Government Sites," EPIC's Open Government Comments to the Obama Administration, *available at* http://opengov.ideascale.com/akira/dtd/3544-4049

[22] "Stopping Commercialization of Personal Data," EPIC's Open Government Comments to the Obama Administration, *available at* http://opengov.ideascale.com/akira/dtd/3538-4049, (accessed August 10, 2009).

- Apply meaningful rules for public participation in official comment across all platforms. [23]
- Promote open government and protect privacy. [24]
- Prohibit the use of technology that prevents digital archiving of government Web sites.[25]
- Federal agency sponsored cookie data should be available to users.
- User browser privacy and security settings should be respected (blocking and removal of government sponsored cookies)
- Prohibit Web analytics, but if it is not--each agency should publish the algorithms on the Web analytics it uses in the federal register no later than 60 days before they are deployed.
- Web applications, advertisements, and cookies should clearly indicate that they are sponsored by a federal government agency: i.e. dod_gov, ssa_gov, dept_ed_gov, etc. or some other defined signature to identify the federal hosting agency.
- The OMB should publish an annual survey outlining each federal government agency's use of Web tracking technology that should reflect all: URSs, Cookies, Web Tracking technologies and processes adopted and their intended purpose.
- Web cookies or applications must be related to a statutorily authorized program.
- Placing of Tracking technology for law enforcement, fusion center, national intelligence must conform to court oversight, and be subject to an annual reporting requirement to the appropriate Congressional Oversight Committees.
- Federal agencies must conduct themselves in accordance with federal and state laws that protect privacy.
- Prohibit agency use of data collected through Web tracking technology for any other purpose than those stated in a federal register notice that should be published at a minimum of 60 days prior to deployment.
- OMB should establish an ombudsman to manage complaints regarding violation of privacy, civil liberties, or constitutional rights due to agency over-collection, retention or use of personal information.
- The Department of Justice Inspector General should have the power to investigate complaints brought to its attention from federal government agencies, whistleblowers, private citizens, companies, and advocacy organizations.

---

[23] "Allowing Meaningful Public Participation," EPIC's Open Government Comments to the Obama Administration, *available at* http://opengov.ideascale.com/akira/dtd/3536-4049, (accessed August 10, 2009).
[24] "Promoting Open Government," EPIC's Open Government Comments to the Obama Administration, *available at* http://opengov.ideascale.com/akira/dtd/3533-4049, (accessed August 10, 2009).
[25] Homepage, Internet Archive, available at http://www.archive.org/index.php

Conclusion

Government support of privacy protections for developing technologies has a checkered past. In August 1945, at the end of World War II, the National Security Agency (NSA) approached heads of telecommunication companies to conduct intercepts of communications. Within weeks, "despite the fear of prosecution and the warnings of their legal advisers," the NSA had agreements with Western Union, RCA, Global, ITT World Communications to intercept and collect telegraph traffic. [26] Initially Western Union limited access to communications from only one country and insisted that its employees "operate the [microfilm] camera and to the actual handling of the messages." RCA, Global, and ITT World Communications also "gave the NSA access to the "great bulk" of their telegrams. [27]

During the social and political transformative period of the 1960s government agencies engaged in wiretapping and surveillance of civil rights leaders, cultural leaders, and youth leaders who engaged in activity protected by the first amendment. Between 1956 and 1971 the FBI conducted the domestic Counter Intelligence Program known as CONINTELPRO.[28] The objective was to investigate and disrupt dissident US political organizations.

The 2008 amendment of the Foreign Intelligence Surveillance Act (FISA)[29] specifically awarded retroactive immunity to telecommunication companies from prosecution for involvement in warrantless domestic wire-tapping operations.[30] This demonstrates a questionably close connection between communications providers and the government, which provides protection to companies when the government violates the privacy of consumers of telecommunications.

For the foregoing reasons, the Electronic Privacy Information Center respectfully reminds the Administration that Presidents come and go, but federal agencies remain. Given the long term effects that any new policy could have, we appreciate the invitation by the Obama Administration to submit comments as they evaluate the future of federal government policy regarding the collection and use of user online activity.

Sincerely,

Lillie Coney

---

[26] James Bamford, The Puzzle Palace, page 304-305 (Penguin Books 1983) (1982).
[27] Whitfield Diffie & Susan Landau, Privacy on the Line, page 158 (MIT Press 2007)
[28] CONINTELPRO, Answers, available at http://www.answers.com/topic/cointelpro
[29] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1871 (2004), available at http://uscode.house.gov/download/pls/50C36.txt.
[30] James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. TIMES, Dec. 16, 2005 available at http://www.nytimes.com/2005/12/16/politics/16program.html.

Associate Director
EPIC

Marc Rotenberg
Executive Director
EPIC

Anirban Sen
Fellow
EPIC

Christopher Suarez
Clerk
EPIC

Electronic Privacy Information Center
1718 Connecticut Avenue, NW
Suite 200
Washington, DC 20009
http://epic.org/