



ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to the
OFFICE OF MANAGEMENT AND BUDGET (OMB)

Circular No. A-130, Managing Information as a Strategic Resource

December 4, 2015

By notice published on October 22, 2015, the Office of Management and Budget (“OMB”) solicited public comments on draft revisions to Circular No. A-130, Managing Information as a Strategic Resource (“A-130”).¹

Accordingly, the Electronic Privacy Information Center (“EPIC”) submits these comments to the OMB regarding revisions to A-130. In summary, EPIC recommends that: (1) each federal agency publish on its website the agency’s authorizing statute(s), regulations, adjudications, guidance, and interpretive rules, as well all court documents from cases involving the agency; (2) the National Archives and Records Administration ensure all federal legislation, statutes, and regulations are publically accessible in a centralized location; and (3) agency websites refrain from tracking government website visitors.

I. EPIC’s Interests

EPIC is a non-profit research and educational organization established in 1994 to focus public attention on emerging human rights issues, and to defend privacy, freedom of expression, and democratic values.² The EPIC Advisory Board is comprised of experts in law, technology and public policy.³

¹ Request for Comments on Circular No. A-130, Managing Information as a Strategic Resource, 80 Fed. Reg. 64,002, 64,002 (Oct. 22, 2015); *see also* Circular A-130, <https://a130.cio.gov/> (last visited Nov. 30, 2015).

² EPIC, *About EPIC* (2015), <https://epic.org/epic/about.html>.

³ EPIC, *EPIC Advisory Board* (2015), https://epic.org/epic/advisory_board.html.

EPIC regularly submits comments to state, federal, and international agencies in support of stronger privacy protections, enhanced protections for consumers, and increased government transparency.⁴ EPIC has previously urged state and federal courts to provide greater public access to public court records while simultaneously protecting sensitive personal information often contained in public records.⁵

EPIC has also advised OMB against lifting its ban on the use of cookies and other tracking technologies on government websites,⁶ and advocated against tracking visitors to government websites.⁷ In 2009, EPIC filed a Freedom of Information Act request for contracts between the federal government and social networking and cloud computing services.⁸ Many of the contracts EPIC obtained failed to require web 2.0 companies to protect the privacy of government website visitors, and some even permitted companies to collect visitor data and track users for advertising purposes.⁹ EPIC concurrently submitted comments addressing the privacy risks and the best practices of government use of social media.¹⁰ Despite EPIC's comments and opposition from other civil society groups,¹¹ OMB reversed its longstanding ban on the use of cookies and tracking technologies on federal government websites in 2010.¹² As discussed

⁴ EPIC, *EPIC Administrative Procedure Act (APA) Comments* (2015), <https://epic.org/apa/comments/>

⁵ See, e.g., EPIC, *Comments on Privacy, Access and Court Records / Report and Recommendations of the Committee on Privacy and Court Records / Group Two, Florida Supreme Court* (Feb. 28, 2006), *available at* <https://epic.org/privacy/publicrecords/flgp222806.html>; EPIC, *Comments on Privacy and Access to Court Records, Administrative Office of Pennsylvania Courts* (Nov. 9, 2005), *available at* <https://epic.org/privacy/publicrecords/paecfcomments.html>; EPIC, *Comment on Privacy and Public Access to Electronic Case Files, Administrative Office of the United States Courts* (Jan. 26, 2001), *available at* https://epic.org/open_gov/ecfcomments.html#1.

⁶ EPIC, *Comments on the Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites, Docket No. E9-17756* (Aug. 10, 2009), *available at* <https://epic.org/privacy/cookies/comnts-to-OMB-cookie.pdf>.

⁷ EPIC, *Comments to the Open Government Dialogue, White House Office of Sci. & Tech.* (2009), *available at* <http://opengov.ideascale.com/a/pmd/6537-4049>.

⁸ EPIC, *Privacy and Government Contracts with Social Media Companies* (2015), <https://epic.org/privacy/socialnet/gsa/>.

⁹ *Id.*

¹⁰ EPIC, *Comments on the Government 2.0 Workshop: Privacy and Best Practices, Docket No. DHS-2009-0020* (June 1, 2009), *available at* https://epic.org/privacy/socialnet/dhs_socialnetworking-6-09.pdf.

¹¹ Miguel Helft, *Privacy Plan for Federal Web Sites Gets Mixed Reviews*, N.Y. Times Bits Blog (Aug. 11, 2009), http://bits.blogs.nytimes.com/2009/08/11/privacy-plan-for-federal-web-sites-gets-mixed-reviews/?_r=0.

¹² Office of Mgmt. & Budget, Exec. Office of the President, M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies* (2010), *available at*

below, OMB's change in policy infringes on personal privacy and OMB should prohibit agencies from tracking website visitors.

II. OMB should revise A-130 to provide open access to law.

The First Amendment guarantees the public a right of access to courts, including access to court records and proceedings.¹³ This right is so fundamental that even prison inmates have a constitutional right to law libraries and legal assistance.¹⁴ The Supreme Court has also recognized a common law right to access, observing that “the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents.”¹⁵

The public's constitutional and common law rights of access to the law are fundamental to a society governed by the rule of law. A myriad of rules, regulations, codes, ordinances, statutes, and common law decisions governs all aspects of American life. The ability of citizens to comply with law and to bring grievances in court require citizens to have easy and free access to what the laws actually permit and restrict.

The right to access also enables the public to monitor government agencies and inquire into the operation of the government.¹⁶ EPIC supports the right of public access to law in all forms. The public must have free and meaningful access to statutes, legislation, rules, regulations, adjudications, ordinances, codes, and case law at the local, state, tribal, and federal levels. Greater public access into the workings of the court system gives citizens tools to evaluate the court system, fosters greater confidence in government and the courts, and offers

https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf; see EPIC, Comments on the Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites, *supra* note 6; see generally EPIC, *Cookies* (2015), <https://epic.org/privacy/internet/cookies/default.html>.

¹³ *E.g.*, *Globe Newsp. Co. v. Super. Ct. for Norfolk County*, 457 U.S. 596, 604 (1982); *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 575–76 (1980); *NBC Subsidiary (KNBC-TV), Inc. v. Superior Court*, 980 P.2d 337, 358 (Cal. 1999) (“Indeed, every lower court opinion of which we are aware that has addressed the issue of First Amendment access to civil trials and proceedings has reached the conclusion that the constitutional right of access applies to civil as well as to criminal trials.”).

¹⁴ *Bounds v. Smith*, 430 U.S. 817, 828 (1977) (“We hold, therefore, that the fundamental constitutional right of access to the courts requires prison authorities to assist inmates in the preparation and filing of meaningful legal papers by providing prisoners with adequate law libraries or adequate assistance from persons trained in the law.”).

¹⁵ *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 597 (1978).

¹⁶ *Id.* at 598.

opportunities for scholars, journalists, and researchers to provide insight into the nature of government.

Unfortunately, much of American law is currently outside the reach of average citizens. Binding codes and legal decisions are often not online in a text-searchable or indexed format. Many states “rely on commercial services to post court briefs and decisions,” which then require a paid subscription.¹⁷ Centralized commercial databases of local, state, and federal law also require subscriptions that cost thousands or millions of dollars a year.¹⁸ And PACER—the federal judiciary’s centralized database of federal court records and documents—provides limited functionality but charges what can easily become prohibitively high fees.¹⁹

Through A-130 revisions, federal agencies can adopt several simple policies that would provide the public with meaningful access case law, federal statutes, regulations, administrative decisions, and other documents that impact agency authority. EPIC recommends the following line edits:

(1) After line 700 (in the “Information Management and Access” subsection, in the sub-subsection stating, “Agencies shall ensure that the public can appropriately use disseminated information by:”²⁰), add:

g) Making available and accessible to the public on the agency’s website:

- (1) the agency’s authorizing statutes (current and former);
- (2) the agency’s rules and regulations issued pursuant to the Administrative Procedure Act (APA) (current and former);
- (3) the agency’s adjudications made pursuant to the APA (current and former);
- (4) the agency’s guidance and interpretive rules, issued pursuant to the APA (current and former); and
- (5) documents from all court cases involving the agency (pending and concluded).

¹⁷ Erik Eckholm, *Harvard Law Library Readies Trove of Decisions for Digital Age*, N.Y. Times (Oct. 28, 2015), http://www.nytimes.com/2015/10/29/us/harvard-law-library-sacrifices-a-trove-for-the-sake-of-a-free-database.html?_r=0.

¹⁸ *Id.*

¹⁹ See, e.g., Carl Malamud, *In re: The PACER System*, <https://yo.yourhonor.org/> (last visited Dec. 1, 2015).

²⁰ A-130(5)(h)(4).

(2) After line 820 (in the “Government-wide Responsibilities” subsection, in the sub-subsection addressing the “National Archives and Records Administration”²¹), add:

- 5) Make available and accessible to the public online in a centralized website all:
 - (1) federal congressional legislation (pending and enacted);
 - (2) federal statutes (current and former)
 - (3) federal agency regulations (current and former).

III. OMB should revise A-130 to prohibit government agencies from tracking website visitors.

Internet tracking poses serious risks to individual privacy—risks that increase exponentially when the federal government is doing the tracking. IP addresses, MAC addresses, cookies, and other methods allow websites to collect personally identifiable information about site visitors and track them across the Internet.²² As EPIC explained in 2009, these tracking tools enable the “secret collection of information about an individual’s interests, actions, habits, and traits in both the offline and online worlds”—otherwise known as “behavioral targeting.”²³ EPIC warned that allowing the federal government to engage in behavior targeting poses “an ominous threat to privacy, civil liberties, and constitutional rights.”²⁴

Because the Privacy Act of 1974 does not cover “the collection, retention, sharing, and use of personal information by private entities,”²⁵ access by private social media and cloud computing services to government website visitor data is especially alarming.²⁶ As EPIC’s 2009 FOIA request revealed, government contracts with Internet companies such as Google, Yahoo,

²¹ A-130(6)(d).

²² See, e.g., EPIC, Search Engine Privacy (2015), https://epic.org/privacy/search_engine/; EPIC, Comments on the Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites, *supra* note 6, at 6–10; Joanna Geary, *Tracking the trackers: What are cookies? An introduction to web tracking*, The Guardian (Apr. 23, 2012), <http://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro>; Peter Eckersley, *How Unique Is Your Web Browser?*, Elec. Frontier Found. <https://panopticklick.eff.org/browser-uniqueness.pdf> (last visited Dec. 1, 2015).

²³ EPIC, Comments on the Proposed Revision of the Policy on Web Tracking Technologies for Federal Web Sites, *supra* note 6, at 8.

²⁴ *Id.*

²⁵ *Id.* at 7.

²⁶ Marc Rotenberg, *Letter to the Editor: Protecting Privacy Online*, N.Y. Times (Aug. 30, 2009), http://www.nytimes.com/2009/08/31/opinion/l31privacy.html?_r=0.

Facebook, and Vimeo failed to address the privacy obligations of these third parties.²⁷ Google even “obtained a waiver of all privacy regulations so that it could track users visiting certain government Web sites.”²⁸

OMB’s repeal of its longstanding ban on the use of cookies and tracking technologies on federal government websites has led to federal agencies using cookies and other web analytics to monitor website visitors.²⁹ Agencies are, however, ostensibly prohibited from collecting personally identifiable information, tracking “user individual-level activity” on non-governmental websites, disclosing data to other departments or agencies, or cross-referencing collected data against already-retained PII.³⁰ But as recently as 2014, government websites, including whitehouse.gov, were using a new and “extremely persistent” form of online tracking.³¹ And as of early 2015, analytics.usa.gov, a government website run in conjunction with Google Analytics, provides detailed tracking and analytical information about visitors to federal government websites.

To ensure that website visitors can access the public information contained on government websites without being tracked or otherwise monitored, EPIC recommends the following line edit:

(1) After line 584 (in the “Privacy and Information Security” subsection, in the sub-subsection addressing “Privacy”³²), add:

i) Ensure that agency websites do not collect and retain website visitors’ PII (including IP addresses, MAC addresses, web cookies, and browser fingerprints), and ensure that agency websites do not track website visitors.

²⁷ EPIC, *Privacy and Government Contracts with Social Media Companies*, *supra* note 8.

²⁸ Rotenberg, *supra* note 26.

²⁹ See Guidance for Online Use of Web Measurement and Customization Technologies, *supra* note 12.

³⁰ *Id.* at 4.

³¹ Julia Angwin, *Meet the Online Tracking Device That is Virtually Impossible to Block*, ProPublica (July 21, 2014), <http://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block>.

³² A-130(5)(e)(1).

IV. Conclusion

Circular A-130 provides valuable guidance to executive branch agencies on organizing and implementing information systems. OMB should incorporate the revisions and recommendations above to ensure that federal agencies fulfill their obligations to provide open access to law and protect individual privacy.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associate Director and Administrative Law
Counsel

Aimee Thomson
EPIC Appellate Advocacy Fellow