epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

OFFICE OF MANAGEMENT AND BUDGET

Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act

October 28, 2016

By notice published on October 7, 2016, the Office of Management and Budget ("OMB") solicited public comments on draft revisions to Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act ("A-108").[1]

Accordingly, the Electronic Privacy Information Center ("EPIC") submits these comments to the OMB regarding revisions to A-108. In summary, EPIC recommends that OMB increase its oversight and strengthen its guidance on federal agency implementation of the Privacy Act "routine use" exemption to remain true to legislative intent and provide important safeguards for individuals' personal privacy.

[1] Request for Comments on Proposed OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act, 81 Fed. Reg. 69,871 (Oct. 7, 2016); *see also Circular A-108*, https://www.whitehouse.gov/sites/default/files/omb/assets/omb/circulars/a108/draft_omb_circular_a_108_10_3_16_clean.pdf (last visited Oct. 28, 2016).

I. EPIC'S INTEREST

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving privacy safeguards, established by Congress, in the development of new information systems operated by the federal government.[2] EPIC has submitted extensive comments on numerous federal agency system of records notices,[3] and has advised Congress on modernizing and strengthening the Privacy Act.[4] EPIC also filed an amicus brief in the U.S. Supreme Court case *NASA v. Nelson*,[5] which considered the privacy rights of federal employees. EPIC's brief

[2] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket No. DHS-2016-0002, DHS-2016-0001 (Feb. 22, 2016), *available at* https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf; Comments of EPIC to the Department of Homeland Security, Notice of Privacy Act System of Records, Docket No. DHS-2011-0094 (Dec. 23, 2011), *available at* http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010), *available at* http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the United States Customs and Border Protection; Department of Homeland Security on the Establishment of Global Entry Program, Docket No. USCBP-2008-0097 (Jan. 19, 2010), *available at* http://epic.org/privacy/global_entry/EPIC-Comments-Global-Entry-2010.pdf.

[3] *See*, *e.g.,* Comments of EPIC to the Department of Homeland Security, Automated Targeting System Notice of Privacy Act System of Records and Proposed Rule: Privacy Act of 1974 Exemptions, DHS Docket Nos. 2012-0019 and 2012-0020 (June 21, 2012) https://epic.org/apa/comments/EPIC-ATS-Comments-2012.pdf; EPIC Comments to the Department of Justice, FBI Insider Threat Program Records (ITPR), JUSTICE/FBI-023 Notice of a New System of Records and Notice of Proposed Rulemaking, CPCLO Order Nos. 007–2016 and 008–2016 (Sept. 19, 2016), https://www.epic.org/apa/comments/EPIC-FBI-Insider-Threat-Comments.pdf

[4] *See, e.g.,* Letter from EPIC to U.S. House of Representatives Committee on the Judiciary (Sept. 16, 2015), https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf; Letter from EPIC to Senator Daniel Akaka, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (May 14, 2012), https://epic.org/privacy/1974act/EPIC-Supp-S1732-Priv-Act-Modernization.pdf; Letter from EPIC to Senator Daniel Akaka, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (Mar. 27, 2012), https://epic.org/privacy/1974act/EPIC-on-S-1732-Privacy-Act-Modernization.pdf.

[5] *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011).

highlighted problems the Privacy Act, including the "routine use" exception, security breaches, and the agency's authority to carve out its own exceptions to the Act.[6]

II. FEDERAL AGENCIES REGULARLY MISUSE THE "ROUTINE USE" EXCEPTION

The definition of "routine use" is precisely tailored, and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. However, federal agencies regularly rely on this exception to disclose information in a manner inconsistent with the purpose for which it was originally gathered. This practice exceeds statutory authority to disclose personally identifiable information without obtaining individual consent, circumvents Privacy Act Safeguards, and contravenes legislative intent.

The Privacy Act prohibits federal agencies from disclosing records they maintain "to any person, or to another agency" without the written request or consent of the "individual to whom the record pertains."[7] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[8] One of these exemptions is "routine use."[9] "Routine use" means "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[10]

The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping

[6] *Amicus Curiae* Brief of EPIC, *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134 (2011), https://epic.org/amicus/nasavnelson/EPIC_amicus_NASA_final.pdf.
[7] 5 U.S.C. § 552a(b).
[8] *Id*. §§ 552a(b)(1) – (12).
[9] *Id*. § 552a(b)(3).
[10] 5 U.S.C. § 552a(a)(7).

> measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[11]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act— interpreted the above Congressional explanation of routine use to mean that a "'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[12]

Subsequent Privacy Act case law interprets the Act's legislative history to limit routine use disclosure based upon a precisely defined system of records purpose. In *United States Postal Service v. National Association of Letter Carriers, AFL-CIO*, the Court of Appeals for the D.C. Circuit relied on the Privacy Act's legislative history to determine that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[13] The Court of Appeals went on to quote the Third Circuit as it agreed, "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[14]

A. Agencies Regularly Claim Routine Uses of Information Entirely Incompatible With Original Purpose of Collection

[11] *Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[12] *Id*.
[13] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[14] *Id*. at 145 (quoting *Britt v. Natal Investigative Serv*., 886 F.2d 544, 549-50 (3d. Cir. 1989). *See also Doe v. U.S. Dept. of Justice*, 660 F.Supp.2d 31, 48 (D.D.C. 2009) (DOJ's disclosure of former AUSA's termination letter to Unemployment Commission was compatible with routine use because the routine use for collecting the personnel file was to disclose to income administrative agencies); *Alexander v. F.B.I*, 691 F. Supp.2d 182, 191 (D.D.C. 2010) (FBI's routine use disclosure of background reports was compatible with the law enforcement purpose for which the reports were collected).

Despite the Privacy Act requirement that routine uses be compatible with the original purpose for which information was collected, federal agencies regularly claim broad routine uses that permit discloses for boundless purposes. For example, the Department of Defense claims a routine use of the records contained in Advertising and Marketing Research Recruiting Database that would allow disclose of information for law enforcement purposes.[15] This is entirely unrelated to advertising and marketing research and exceeds DoD's statutory authority. It also exemplifies the risk of such broad routine uses, which invites mission creep and other abuses by allowing agencies to do much more with Americans' personal information than originally intended.

More troubling, federal agencies have created databases for the stated purpose of maintaining records, and then claim a routine use of such databases is to provide and obtain records. For example, the stated purpose of the National Security Agency's Operations Records database is to "maintain records on foreign intelligence, counterintelligence, and information systems security matters relating to the mission of the National Security Agency."[16] NSA claims a routine use of this database is to disclose records "to provide, and in order to obtain, foreign intelligence, counterintelligence, information assurance/cybersecurity information, and other information, in accordance with applicable law and policy."[17] In other words, the purpose of this database is to collect information and it is regularly used to disclose and collect additional information. Such an overbroad purpose and use of government databases allows for virtually

[15] Notice to add a system of records; DHRA 04--Joint Advertising and Market Research Recruiting Database., 70 Fed. Reg. 29486. *See also*, Comments of EPIC to DOD, DHRA 04 Joint Advertising and Marketing Research Recruiting Database (June 22, 2005), https://epic.org/privacy/profiling/dodrecruiting.html.

[16] Privacy Act of 1974; System of Records, 80 Fed. Reg. 63,749 (Oct. 21, 2015). *See also*, Comments of EPIC to the National Security Agency, GNSA 18 Operations Records System of Records Notice, Docket ID: DoD-2015-OS-0100 (Nov. 20, 2015), https://www.epic.org/privacy/nsa/EPIC-NSA-SORN-Comments-2015.pdf.

[17] *Id*.

unlimited collection and disclosure of American citizens' personal information and must be curtailed.

B. Agencies Frequently Claim "Public Relations" Routine Uses of Information That Prioritize Agency Reputation Over Individual Right to Privacy

Numerous systems of records contain a "Public Relations" exemption to the Privacy Act that would permit the agency to release personal information if – incredibly – such disclosure would "preserve confidence" in the agency or "demonstrate accountability."[18] For example, the Department of Homeland Security Insider Threat database includes the following routine use that permits the agency to disclose information:

> To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS' officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.[19]

The phrase "when disclosure is necessary to preserve confidence in the integrity of DHS" is discordant with the Privacy Act because it gratuitously puts the face of the agency above an individual's right to privacy. The term "necessary" is ambiguous; the agency could take advantage of this criterion to unduly influence its image. Similar "public relations" routine uses are found in systems of records maintained by the Coast Guard,[20] DHS's Automated Identification Management System,[21] and the FBI's Insider Threat Database.[22] OMB should revise A-108 to explicitly prohibit "public relations" routine uses.

---

[18] *See, e.g.*, https://epic.org/apa/comments/EPIC-DHS-Boating-Passenger-Cmts.pdf
[19] Notice of Privacy Act System of Records, 81 Fed. Reg. 9871, 9875 (Feb. 26, 2016).
[20] Privacy Act of 1974; Department of Homeland Security/United States Coast Guard-029 Notice of Arrival and Departure System of Records, Fed. Reg., 74,116, 74,118 (Nov. 27, 2015).
[21] Notice of Privacy Act System of Records, 70 Fed. Reg. 38,699, 38,700 (July 5, 2005).
[22] Notice of a new system of records, 81 Fed. Reg. 64198, 64,200 (Sep. 19, 2016).

C. Agencies Frequently Claim Routine Uses to Disclose Information to Foreign and Private Entities Not Subject to the Privacy Act

Numerous system of records notices claim routine uses that permit the transfer of personal information on U.S. citizens, held by a U.S. federal agency, to foreign and international governments and entities that fall entirely outside the authority of U.S. privacy law and the jurisdiction of U.S. federal courts.[23] Agencies also claim routine uses to disclose information to private entities not subject to the Privacy Act.[24] This is entirely inconsistent with the purposes of the Privacy Act and poses substantial risk to the privacy and security of American citizens.

Where agencies cannot fill their statutory obligations without disclosing information to third parties not subject to the Privacy Act, such routine uses should include the following language: "Entities and/or individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees."

III. OMB SHOULD REVISE A-108 LANGUAGE TO CLARIFY PERMISSIBLE SCOPE OF ROUTINE USES

The language OMB proposes to include in Circular A-108 regarding routine uses is consistent with the Privacy Act and legislative intent. However, it is clear that federal agencies continue to disregard the statutory limits on routine use exemptions and misuse this provision to

[23] *See, e.g.*, Privacy Act of 1974; Department of Homeland Security/United States Coast Guard-029 Notice of Arrival and Departure System of Records, Fed. Reg., 74,116, 74,118 (Nov. 27, 2015) (Routine Uses G, H, J, M); Privacy Act of 1974; Department of Homeland Security/United States Secret Service—003 Non-Criminal Investigation Information System of Records, 76 Fed. Reg. 66,937, 66,939 (Oct. 28, 2011) (Routine Use L); Notice of Privacy Act System of Records, DHS Automated Targeting System, 77 Fed. Reg. 30297, 30302 (May 22, 2012)

[24] *See, e.g.*, Privacy Act of 1974; Department of Homeland Security/United States Coast Guard-029 Notice of Arrival and Departure System of Records, Fed. Reg., 74,116, 74,118 (Nov. 27, 2015) (Routine Use I); Privacy Act of 1974; Department of Homeland Security/United States Secret Service—003 Non-Criminal Investigation Information System of Records, 76 Fed. Reg. 66,937, 66,939 (Oct. 28, 2011) (Routine Use I); Privacy Act of 1974; Department of Homeland Security/ALL—017 General Legal Records System of Records, 76 Fed. Reg. 72,428, 72,430 (Nov. 23, 2011) (Routine Uses O and S); Notice of Privacy Act System of Records, DHS Automated Targeting System, 77 Fed. Reg. 30297, 30302 (May 22, 2012).

circumvent Privacy Act safeguards. EPIC recommends that OMB strengthen its guidance on the routine use exemption accordingly.

Circular A-108 proposes the following language:

> Routine uses shall be narrowly tailored to address a specific and appropriate use of the records. Agencies shall describe each routine use with sufficient clarity and specificity to ensure that members of the public who are unfamiliar with the system or the agency's program can understand the uses to which the records will be subject. Overly broad or ambiguous language would undermine the purpose of the routine use notice requirement and shall be avoided.[25]

EPIC proposes the following additional language:

> Routine uses shall be narrowly tailored to address a specific and appropriate use of the records. Agencies shall describe each routine use with sufficient clarity and specificity to ensure that members of the public who are unfamiliar with the system or the agency's program can understand the uses to which the records will be subject. Overly broad or ambiguous language would undermine the purpose of the routine use notice requirement and shall be avoided. Under this provision, routine uses with the stated purpose to "disclose" or "obtain" records are insufficient. Routine uses that involve disclosing information to "preserve confidence" in the agency, "demonstrate accountability," or to further other public relations goals are prohibited.

Clarifying OMB guidance in this manner would aid in preventing unwarranted disclosure of individual records, and is true to the Privacy Act's legislative intent.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Claire Gartland
Claire Gartland
Director, EPIC Consumer Privacy Project

[25] A-108 at 11 (internal citations omitted).