epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Comments of

THE ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)

to

THE NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE,

DEPARTMENT OF DEFENSE

[Docket ID: DoD-2015-OS-0100]

GNSA 18, "Operations Records"
Privacy Act of 1974; System of Records

November 20, 2015

By notice published October 21, 2015, the National Security Agency ("NSA") proposes to alter its system of records notice GNSA 18, entitled "Operations Records."[1] Among other proposed changes, NSA seeks to (1) expand the categories of records collected and (2) define additional routine uses of the records in this system. Pursuant to the NSA notice, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by the proposed changes; to oppose further expansion of NSA's information collection activities; to oppose additional routine uses of these records; and to demand that NSA significantly narrow the Privacy Act exemptions for the system if the proposal goes forward.

[1] Privacy Act of 1974; System of Records, 80 Fed. Reg. 63,749 (Oct. 21, 2015) [hereinafter Operations Records SORN].

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]

EPIC has previously urged NSA to conduct information collection activities in compliance with the Privacy Act.[4] EPIC specifically petitioned the agency to "conduct a public rulemaking on the agency's monitoring and collection of communications traffic within the United States. 5 U.S.C. § 553(e)."[5] The agency responded:

> As a general matter, any NSA activities involving the collection of communications that may meet the description set forth in your letter, if any [sic], would not constitute Agency actions that are subject to the notice-and-comment requirements of the Administrative Procedures Act, such as the issuance, amendment or repeal of rules or regulations.[6]

EPIC has advised the Privacy and Civil Liberties Oversight Board ("PCLOB") about the need to minimize data collection and to limit the dissemination of collected information, as well as the critical need for transparency and oversight of surveillance activities, particularly under Executive Order 12333.[7]

---

[2] *About EPIC*, https://epic.org/epic/about.html (2015).
[3] *EPIC Advisory Board*, https://epic.org/epic/advisory_board.html (2015).
[4] EPIC Comments on Dept. of Def. Privacy Program (Oct. 21, 2013) https://epic.org/privacy/nsa/Coal-DoD-Priv-Program-Cmts.pdf; Petition from EPIC et al. to Keith B. Alexander, Director, Nat'l Sec. Agency & Chuck Hagel, Sec. of Defense (June 17, 2013), *available at* https://epic.org/NSApetition/.
[5] Petition from EPIC et al. to Keith B. Alexander, Director, Nat'l Sec. Agency & Chuck Hagel, Sec. of Defense (June 17, 2013), *available at* https://epic.org/NSApetition/.
[6] Letter to Marc Rotenberg, President, EPIC from David A. Sherman, Associate Director Policy and Records, National Security Agency (Aug. 26, 2013) ("Re: EPIC Petition for NSA to Conduct a Public Rulemaking"), *available at* https://epic.org/privacy/nsa/NSA-Petition-Reply-8-30-13.pdf.
[7] EPIC Comments to Privacy and Civil Liberties Oversight Bd. on Surveillance Activities Under E.O. 12333, https://www.epic.org/privacy/surveillance/12333/EPIC-12333-PCLOB-Comments-FINAL.pdf.

I. The Privacy Act Grants Individuals Judicially Enforceable Rights and Imposes Obligations on Federal Agencies

The Privacy Act of 1974 governs federal agency maintenance, collection, use, and dissemination of U.S. citizen and lawful permanent resident "records" contained in a "system of records."[8] The Act broadly defines "record" to include:

> any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph[.][9]

A "system of records" is

> a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual [.][10]

When it enacted the Privacy Act of 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required transparency in agency information practices.[11] Privacy Act legislative history reveals that the Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems data of the Federal Government [.]"[12] It is also intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right

[8] 5 U.S.C. § 552a.
[9] *Id*. § 552a(a)(4).
[10] *Id*. § 552a(a)(5).
[11] S. Rep. No. 93-1183 at 1 (1974).
[12] *Id*.

protected by the Constitution of the United States."[13] Congress thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[14] These rights, for example, guarantee that individuals:

- may request access to records an agency maintains about him or her, as well as have a copies made;[15]
- may amend a record about him or her;[16] and
- must be informed whom the agency asks to supply information;[17]

Importantly, the Privacy Act grants individuals a private right of action and individuals may sue a federal agency for violating the Privacy Act.[18] In addition to granting individual rights, the Privacy Act also imposes several obligations on federal agencies, including obligations that agencies must:

- at least 30 days prior to publication of each record routine, "publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency";[19]
- not maintain records "describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity";[20]
- give individuals access to the accounting of disclosure of their records;[21]
- make notes of requested amendments within the records;[22]

[13] Pub. L. No. 93-579 (1974).
[14] *Id.*
[15] 5 U.S.C. § 552a(d)(1).
[16] *Id*. § 552a(d)(2).
[17] *Id*. § 552a(e)(3).
[18] *Id*. § 552a(g).
[19] *Id*. § 552a(e)(11).
[20] *Id*. § 552a(e)(7).
[21] *Id*. § 552a(c)(3).
[22] *Id*. § 552a(d)(4).

- collect records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President";[23]

- "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs";[24]

- assure that all records used by the agency in making determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness;[25]

- make a reasonable effort to notify an individual when a record about him or her is made available to another individual when it is a matter of public record;[26]

- promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual", instituting disclosure procedures for medical and psychological records, create procedures, review amendment requests, as well as determining the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record;[27]

In addition to assessing "reasonable attorney fees and other litigation costs," for noncompliant agencies, courts may order agencies to amend individuals records, as well as "enjoin the agency from withholding records."[28] The Act also imposes criminal penalties for officers and agency employees who willfully disclose agency records in violation of the Privacy Act or Privacy Act regulations.[29]

[23] *Id.* § 552a(e)(1).
[24] *Id*. § 552a(e)(2).
[25] *Id*. § 552a(e)(5).
[26] *Id*. § 552a(e)(8).
[27] *Id*. § 552a(f)(1), (2), (3), (4), (5).
[28] *Id*. § 552a(g)(2)(B); *id*. § 552a(g)(3)(A).
[29] *Id*. § 552a(i).

II. NSA's Broad Claims of Privacy Act Exemptions Remove any Meaningful Privacy Safeguards for this Vast Database

The NSA is an "agency" subject to the Privacy Act.[30] However, the NSA claims numerous Privacy Act exemptions for the Operations Records database. The NSA claims exemption for some or all of the records maintained in its "Operations Records" system from §§ 552a(c)(3); (d); (e)(1); (e)(4)(G), (H), and (I); and (f) pursuant to § 552a(k)(1), (2), and (5).[31] These provisions of the Privacy Act ensure that:

- an agency must give individuals access to the accounting of disclosure of their records;[32]
- allowing individuals to request access and amendments to records the agencies maintains about them;[33]
- agencies must "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President";[34]
- an agency must publish the establishment or revision of the notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access, contest content, and learn the categories of sources or records in the system;[35]
- the agency shall promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual", instituting disclosure procedures for medical and psychological records, create procedures, review amendment requests, as well as determining the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record.[36]

Several of NSA's claimed exemptions would further exacerbate the impact of its proposed expansions to the categories of records and routine uses in this system of records. NSA exempts itself from § 552a(e)(1), which requires agencies to maintain only those records relevant

[30] *Id*. § 552a(a)(1).
[31] 32 CFR § 322.7(p).
[32] 5 U.S.C. § 552a(c)(3).
[33] *Id*. § 552(a)(d).
[34] *Id*. § 552a(e)(1).
[35] *Id*. § 552a(e)(4)(G), (H), (I).
[36] *Id*. § 552a(f).

to the agency's statutory mission. The agency exempts itself from § 552a(e)(4)(I), which requires agencies to disclose the categories of sources of records in the system. And the agency exempts itself from its Privacy Act duties under to § 552a(e)(4)(G) and (H) to allow individuals to access and correct information in its records system. In other words, the NSA claims the authority to collect any information it wants without disclosing where it came from or accounting for its accuracy or acknowledging its existence. The net result of these exemptions, coupled with the NSA's proposal to collect and retain "any type of information,"[37] would be to diminish the legal accountability of the agency's information collection activities.

It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to maintain a database on U.S. citizens containing so much personal information and simultaneously be granted broad exemptions from Privacy Act obligations. It is as if the agency has placed itself beyond the reach of the American legal system on the issue of greatest concerns to the American public – the protection of personal privacy. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of the data used in a system that now contains the records of millions of American citizens.

III. NSA Proposes to Significantly Expand the Categories of Records in the System

The NSA currently collects and retains extensive personal, sensitive information within its "Operations Records" database:

> Records include individual's name, Social Security Number (SSN); employee identification number; administrative information; biographic information; intelligence requirements, *analysis and reporting*; *information systems security analysis and reporting*; operational records; articles; public-source data; and other published information on individuals and events of interest to NSA/CSS; actual or purported

[37] Operations Records SORN at 63,749.

> compromises of classified intelligence; countermeasures in connection therewith; and identification of classified source documents and distribution thereof.[38]

The agency's stated purpose of the 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.[39]

The NSA now seeks to vastly expand the categories of records collected in this system to include:

> any type of information acquired or maintained about an individual as NSA pursues its lawfully authorized missions, including but not limited to: An individual's name; Social Security Number (SSN); employee identification number; administrative information; biographic information when associated with an individual, such as phone number and email address; intelligence requirements; foreign intelligence, counterintelligence, and information assurance/cybersecurity analysis and reporting; operational records; articles, public-source data, and other published information on individuals and events of interest to NSA/CSS; actual or purported compromises of classified intelligence; countermeasures in connection therewith; and identification of classified source documents and distribution thereof.[40]

The language NSA proposes to add to the categories of records in the system would significantly expand the types of information collected in this database. In light of the extremely broad routine uses NSA claims for these records, as well as the broad exemptions NSA claims from Privacy Act safeguards, this proposed change to the System of Record Notice ("SORN") should not be permitted.

IV. The NSA's Proposed Routine Uses Remove Privacy Act Safeguards and Permit the Disclosure of Records for Virtually Unlimited Purposes to Private and Foreign Entities That Are Not Subject to the Privacy Act

A routine use, as defined in the Privacy Act, 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

[38] 75 Fed. Reg. 74,019.
[39] 75 Fed. Reg. 74019.
[40] Operations Records SORN at 63,749.

was collected."[41] The NSA has failed to establish that the proposed routine uses are compatible with the purpose for which the data was collected, as required by law.[42]

The NSA currently claims broad routine uses for the Operation Records database. The NSA states that the DoD "Blanket Routine Uses" apply to this records system, which enumerate the following sixteen broad routine uses:

> 01. Law Enforcement Routine Use; 02. Disclosure When Requesting Information Routine Use; 03. Disclosure of Requested Information Routine Use; 04. Congressional Inquiries Disclosure Routine Use; 05. Private Relief Legislation Routine Use; 06. Disclosure Required by International Agreements Routine Use; 07. Disclosure to State and Local Taxing Authorities Routine Use; 08. Disclosure to the Office of Personnel Management Routine Use; 09. Disclosure to the Department of Justice for Litigation Routine Use; 10. Disclosure to Military Banking Facilities Overseas Routine Use; 11. Disclosure of Information to the Federal Services Administration Routine Use; 12. Disclosure of Information to the National Archives and Records Administration Routine Use; 13. Disclosure to the Merit Systems Protection Board Routine Use; 14. Counterintelligence Purpose Routine Use; 15. Data Breach Remediation Purposes Routine Use; and 16. Information Sharing Environment Routine Use.[43]

The "Law Enforcement Routine Use, " for example, would permit disclosure of information otherwise subject to the Privacy Act that "indicates a violation or potential violation of law."[44] This is a potentially very broad use.

The NSA now seeks to significantly expand its routine use of the information contained in this vast database. Current NSA routine uses are:

> To U.S. Government agencies, and in some instances foreign government agencies or their representatives, to provide foreign intelligence, counterintelligence, information systems security information, and other information.
>
> To U.S. Government officials regarding compromises of classified information including the document(s) apparently compromised, implications of disclosure of intelligence

[41] 5 U.S.C. § 552a(a)(7).
[42] *Id*.
[43] *Systems of Records Notices (SORNS)*, Defense Privacy and Civil Liberties Division, U.S. Dep't of Defense, http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.
[44] *Id*.

sources and methods, investigative data on compromises, and statistical and substantive analysis of the data.

To any U.S. Government organization in order to facilitate any security, employment, detail, liaison, or contractual decision by any U.S. Government organization.

Records may further be disclosed to agencies involved in the protection of intelligence sources and methods to facilitate such protection and to support intelligence analysis and reporting.

The DoD 'Blanket Routine Uses' published at the beginning of the NSA/CSS' compilation of systems of records notices apply to this system.[45]

The proposal would add the following routine uses of the records maintained in the Operation Records system:

- To U.S. Government agencies, including state and local agencies, and in some circumstances, foreign government agencies or their representatives, and private entities to provide, and in order to obtain, foreign intelligence, counterintelligence, information assurance/cybersecurity information, and other information, in accordance with applicable law and policy. The National Security Agency does not collect or provide such records to afford a competitive advantage to U.S. companies or U.S. business sectors commercially.

- To any U.S. Government or foreign government organization in order to facilitate any security, employment, detail, liaison, or contractual decision by any U.S. Government organization.

- To the President's Foreign Intelligence Advisory Board, the Intelligence Oversight Board, and the Privacy and Civil Liberties Oversight Board, and any successor organizations, when requested by those entities, or when NSA/CSS determines that disclosure will assist in oversight functions.[46]

The proposed revisions that would permit the NSA to disclose records, subject to the Privacy Act, to private entities and to foreign organizations should be removed. The Privacy Act only applies to records maintained by United States government agencies.[47] Releasing

[45] 75 Fed. Reg. 74,019.
[46] Operations Records SORN at 63,749.
[47] 5 U.S.C. § 552a(b).

information to private and foreign entities does not protect individuals covered by this records system from Privacy Act violations.

The proposed additions to the first routine use would allow NSA to disclose any information "to provide, and in order to obtain, foreign intelligence, counterintelligence, information assurance/cybersecurity information, and other information, in accordance with applicable law and policy."[48]

V. Conclusion/Recommendations

NSA currently conducts information collection activities that are overbroad and unlawful. Now, the NSA seeks to add new categories of personal information to the Operations Records system of records, permit routine disclosure of this information to foreign governments and private contractors, and reduce compliance with legal obligations establish by the Privacy Act. The NSA should withdraw this System of Records Notice, and start over.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associate Director and Administrative Law Counsel

Claire Gartland
EPIC Consumer Protection Fellow

Aimee Thomson
EPIC Appellate Advocacy Fellow

[48] Operations Records SORN at 63,749.