epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER
to the
DEPARTMENT OF HOMELAND SECURITY

Privacy Act of 1974; Department of Homeland Security/United States Coast Guard-029 Notice of Arrival and Departure System of Records

Notice of Privacy Act System of Records and Notice of Proposed Rulemaking

[Docket Nos. DHS-2015-0078,79]

December 28, 2015

By notice published on November 27, 2015, the Department of Homeland Security ("DHS") Privacy Office solicited public comments on DHS's proposal to revise a DHS system of records titled, ''029 Notice of Arrival and Departure System of Records.''[1] The System of Records Notice ("SORN") describes a database that will allow the agency to collect, retain, and disseminate personal information of individuals, including United States citizens, that travel to and from the U.S. by sea.[2] On the same date, DHS proposed Privacy Act exemptions that would prevent individuals from knowing who else has access to their personal information and would prohibit individuals from suing DHS if the agency misuses their personal information.[3]

The Electronic Privacy Information Center ("EPIC") submits these comments to: (1) address the substantial privacy issues raised by the database, (2) urge DHS to significantly

[1] Notice of Privacy Act System of Records, 80 Fed. Reg. 74,116 (Nov. 27, 2015) [hereinafter "Sea Arrival/Departure SORN"].
[2] *Id*. at 74, 117-19.
[3] Notice of Proposed Rulemaking, 80 Fed. Reg. 74,018 (Nov. 27, 2015) [hereinafter "Sea Arrival/Departure NPRM"].

narrow the Privacy Act exemptions for the Sea Arrival/Departure Database, and (3) recommend that DHS remove unlawful and unnecessary routine use disclosures.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, freedom of expression, and democratic values.[4] EPIC has a particular interest in preserving privacy safeguards established in the Privacy Act of 1974.[1] EPIC has made numerous recommendations to Congress and federal agencies on the need to strengthen Privacy Act protections.[2]

EPIC recently filed a Freedom of Information Act lawsuit against the DHS and U.S. Coast Guard to uncover records on the Nationwide Automatic Identification System ("NAIS"), a controversial boater tracking program.[5] EPIC wrote that NAIS, "exceeds the stated purpose of marine safety and constitutes an ongoing risk to the privacy and civil liberties of mariners across the United States."[6] The boating community is equally alarmed. Ralph Naranjo, a widely regarded mariner, author, and former Vanderstar Chair at the U.S. Naval Academy, expressed dismay that "a sailor's Good Samaritan effort to share location data will automatically enroll them in a data bank that tracks all of their movements."[7] And in comments to the USCG regarding the agency's dissemination of NAIS data, BoatU.S., "the nation's largest organization of recreational boaters," said that NAIS "raises questions as to who might wish to use [the] data and to what end," and urged the agency to "narrowly confine the use of [the] data for safety and homeland security purposes."[8] According to documents EPIC has obtained in the lawsuit, DHS believes that boaters have "no expectation of privacy with regard to any information transmitted" on the Automated Identification System.[9] The documents also reveal that DHS combines AIS data with other government data to craft detailed boater profiles.[10]

---

[4] EPIC, *About EPIC* (2015), https://epic.org/epic/about.html.
[5] *See EPIC v. U.S. Coast Guard et al.*, No. 15-1527 (D.D.C. *filed* Sept. 18, 2015).
[6] Complaint at 2, *EPIC v. U.S. Coast Guard et al.*, No. 15-1527.
[7] Ralph Naranjo, *Big Brother on the Water: The Coast Guard's Maritime Domain Awareness Program Chips Away at our Boating Freedoms*, Practical Sailor, Feb. 2011, at 28, available at http://www.practical-sailor.com/issues/37_2/features/Is_AIS_Chipping_Away_at_Our_Freedoms_10135-1.html.
[8] BoatU.S., *Comment on Interim Policy for the Sharing of Information Collected by the Coast Guard Nationwide Automatic Identification System* (Feb. 18, 2010), http://www.regulations.gov/contentStreamer?documentId=USCG-2009-0701-0009&attachmentNumber=1&disposition=attachment&contentType=pdf.
[9] U.S. Coast Guard, U.S. Department of Homeland Security, Policy for the Sharing of Automatic Identification System Information that is Collected by the Coast Guard Nationwide Automatic Identification System (NAIS), 2 (Dec. 16, 2011), *available at http://epic.org/foia/dhs/uscg/nais/EPIC-15-05-29-USCG-FOIA-20151030-Production-1.pdf#page=2.*
[10] EPIC, *EPIC v. USCG – Nationwide Automatic Identification System*, https://epic.org/foia/dhs/uscg/nais/.

EPIC has opposed other DHS passenger profiling programs like NAIS,[11] and called for an independent audit to determine whether the Transportation Security Administration ("TSA") airport screeners engage in racial profiling.[12] EPIC highlighted the problems inherent in passenger profiling systems such as Secure Flight in previous testimony and comments. In testimony before the 9/11 Commission, EPIC President Marc Rotenberg explained, "there are specific problems with information technologies for monitoring, tracking, and profiling. The techniques are imprecise, they are subject to abuse, and they are invariably applied to purposes other than those originally intended."[13]

I. The Arrival/Departure Database Contains Sensitive, Personal Information on Americans Travelling by Sea

According to DHS, the Sea Arrival/Departure Database allows the United States Coast Guard ("Coast Guard") to monitor the "entry and departure of vessels into and from the United States, and assist with assigning priorities for complying with maritime safety and security regulations."[14]

Specifically, DHS proposes to include the following categories of individuals in the Sea Arrival/Departure Database:

- Crew members who arrive or depart the United States by sea; and
- Other individuals or organizations associated with a vessel and whose information is submitted as part of a notice of arrival or notice of departure, such as vessel owners, operators, charterers, reporting parties, 24-hour contacts, company security officers, and passengers who arrive and depart the United States by sea.[15]

---

[11] *See, e.g.*, EPIC, *Comments on TSA PreCheck Application Program System of Records*, Docket Nos. DHS-2013-0040, 0041 (Oct. 10, 2013), *available at* https://epic.org/apa/comments/EPIC-TSAPreCheck-Comments.pdf; EPIC et al., *Comments on the Terrorist Screening Database System of Records, Notice of Privacy Act System of Records and Notice of Proposed rulemaking, Docket Nos. DHS 2011-0060 and DHS 2011-0061* (Aug. 5, 2011), *available at* http://epic.org/privacy/airtravel/Comments_on_DHS-2011-0060_and_0061FINAL.pdf; EPIC, *Comments on Secure Flight, Docket Nos. TSA-2007-28972, 2007-28572* (Sept. 24, 2007), *available at* http://epic.org/privacy/airtravel/sf_092407.pdf; EPIC, *Secure Flights Should Remain Grounded Until Security and Privacy Problems are Resolved, Spotlight on Surveillance Series* (August 2007), *available at* http://epic.org/privacy/surveillance/spotlight/0807/default.html; EPIC, *Passenger Profiling* (2015), http://epic.org/privacy/airtravel/profiling.html; EPIC, *Secure Flight* (2015), http://epic.org/privacy/airtravel/secureflight.html; EPIC, *Air Travel Privacy* (2015), http://epic.org/privacy/airtravel/.

[12] Letter from EPIC et al., to Secretary Janet Napolitano and Honorable Charles K. Edwards, Department of Homeland Security (Dec. 1, 2011), *available at* http://epic.org/privacy/airtravel/12-01-11-Coalition-Racial-Profiling-Audit-DHS-Letter.pdf.

[13] Marc Rotenberg, President, EPIC, *Prepared Testimony and Statement for the Record of a Hearing on Security & Liberty: Protecting Privacy, Preventing Terrorism Before the National Commission on Terrorist Attacks Upon the United States* (Dec. 8, 2003), *available at* http://www.epic.org/privacy/terrorism/911commtest.pdf.

[14] Sea Arrival/Departure SORN, 80 Fed. Reg. at 74,116.

[15] *Id*. at 74,117.

DHS also proposes to include the following categories of records:

- Records on vessels including: Name of vessel; name of registered owner; country of registry; call sign; International Maritime Organization (IMO) number or, if a vessel does not have an IMO number the official number; name of the operator; name of charterer; and name of classification society;
- Records on arrival information pertaining to the voyage
- Records about crewmembers;
- Records about ''other individuals associated with a vessel and whose information is submitted as part of a notice of arrival or notice of departure'' (e.g., passenger information) including: Full name; date of birth; nationality; identification type (e.g., passport, U.S. Alien Registration Card, government- issued picture ID); identification number, issuing country, issue date, expiration date; U.S. address information; and location where the individual embarked (list port or place and country);
- Records related to cargo onboard the vessel; and
- Records regarding the operational condition of equipment.[16]

Incredibly, DHS proposes to exempt this database containing detailed, sensitive personal information from well-established Privacy Act safeguards. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of the data used in government databases.[17]

II. DHS Proposes Broad Exemptions for the Sea Arrival/Departure Database, Contravening the Intent of the Privacy Act of 1974

DHS proposes broad Privacy Act exemptions for the Sea Arrival/Departure Database, thus contravening the intent of the Privacy Act of 1974. DHS asserts these claims for "law enforcement or national security purposes."[18] DHS claims it "will not assert any exemption with respect to information maintained in the system that is collected from a person at the time of arrival or departure, if that person, or his or her agent, seeks access or amendment of such information."[19] But DHS further states that "exemptions applicable to" records "ingested from other systems" will continue to apply.[20]

Furthermore, DHS proposes to claim Privacy Act exemptions to:

> preclude subjects of these activities from frustrating the investigative process; to avoid disclosure of investigative techniques; protect the identities and physical safety of confidential informants and of law enforcement personnel; ensure DHS's and other federal agencies' ability to obtain information from third parties and other

[16] *Id.*
[17] The Privacy Act of 1974, Pub. L. 93–579, § 2, 88 Stat. 1896 (Dec. 31, 1974).
[18] Sea Arrival/Departure NPRM, 80 Fed. Reg. at 74,019.
[19] *Id.*
[20] *Id.*

sources; protect the privacy of third parties; and safeguard sensitive information. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.[21]

Specifically, pursuant to 5 U.S.C. §§ 552a(j)(2), DHS proposes to exempt the Sea Arrival/Departure Database from sections (c)(3), (e)(8), and (g) of the Privacy Act. These provisions of the Privacy Act ensure that:

- an agency must give individuals access to the accounting of disclosure of their records;[22]
- an agency must "make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record";[23]
- an individual may obtain civil remedies when an agency fails to adhere to Privacy Act requirements.[24]

DHS's attempts to circumvent the intent of the Privacy Act will create a massive government database of detailed personal information that lacks accountability. DHS's proposed exemptions from 5 U.S.C. § 552a(c)(3), (e)(8), and (g) only serve to increase the secrecy of the database and erode agency accountability. DHS claims that accounting for disclosures, granting individuals access to their records, and implementing notification regulations may put entities on notice that they are being investigated, thereby hindering their investigative efforts.[25]

While EPIC recognizes the need to withhold notice during the period of the investigation, individuals should be able to know, after an investigation is completed or made public, the information stored about them in the system. Access to records of a completed investigation, with appropriate redactions to protect the identities of witnesses and informants, would provide individuals and entities with the right to address potential inaccuracies. And because the investigations have already been completed, DHS's law enforcement purposes would not be undermined and DHS could still protect individual privacy rights.

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that Federal agencies were able to collect, and furthermore, required agencies to be transparent in their information practices.[26] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that: "in order to protect the privacy of individuals identified in information

[21] *Id*.
[22] 5 U.S.C. § 552a(c)(3).
[23] § 552a(e)(8).
[24] § 552a(g).
[25] Sea Arrival/Departure NPRM, 80 Fed. Reg. at 74,020.
[26] S. Rep. No. 93-1183 at 1 (1974).

systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." [27]

The Privacy Act is intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion and to establish accountability for the collection and use of personal information. By asserting an exemption that allows the agency to encroach on an individual's right to know about disclosures of their personal information held by the agency, DHS violates the central purpose of the Privacy Act.

III. DHS's Proposed Routine Uses Contravene the Intent of the Privacy Act and Exceed the Authority of the Agency

The Privacy Act's 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. The Sea Arrival/Departure Database contains a broad category of personally identifiable information. By disclosing information in a manner inconsistent with the purpose for which the information was originally gathered, DHS exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[28] 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 protected by the Constitution of the United States."[29]

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."[30] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[31] One of these exemptions is "routine use."[32] The Arrival/Departure system of records notice states that "all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3)."[33] "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."[34]

[27] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[28] S. Rep. No. 93-1183 at 1 (1974).
[29] Pub. L. No. 93-579 (1974).
[30] 5 U.S.C. § 552a(b).
[31] *Id*. §§ 552a(b)(1) – (12).
[32] *Id*. § 552a(b)(3).
[33] Sea Arrival/Departure SORN, 80 Fed. Reg. at 74,118.
[34] 5 U.S.C. § 552a(a)(7).

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 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.[35]

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."[36]

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."[37] 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."[38]

DHS proposes to disclose traveler information for purposes that do not relate to maritime security and screening. DHS states that it may disclose information within the Sea Arrival/Departure Database with "other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions and missions."[39] These proposed disclosures transform the Sea Arrival/Departure Database from a narrowly defined maritime security system of records to a

---

[35] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[36] *Id*.
[37] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[38] *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).
[39] Sea Arrival/Departure SORN, 80 Fed. Reg. at 74,117.

general law enforcement repository. With its proposal, DHS fashions the Sea Arrival/Departure Database as a virtual line up that law enforcement agencies may access for purposes other than maritime security. The agency therefore exceeds its authority with this purpose and should not adopt it.

IV. Proposed Routine Uses G, H, J, I, and M Remove Privacy Act Safeguards by Disclosing Records to Foreign Entities Not Subject to the Privacy Act

The agency proposes a surprisingly broad list of exemptions that would permit the transfer of personal information on U.S. citizens, held by a U.S. federal agency, to foreign police and intelligence organizations that fall entirely outside the authority of US privacy law and the jurisdiction of U.S. federal courts. This is entirely inconsistent with the purposes of the Act and is contrary to case law.

Proposed Routine Use G would permit DHS to disclose information:

> To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.[40]

Proposed Routine Use H would permit DHS to disclose information:

> To federal and foreign government intelligence or counterterrorism agencies or components if USCG becomes aware of an indication of a threat or potential threat to national or international security, or if such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.[41]

Proposed Routine Use I would permit DHS to disclose information:

> To an organization or individual in either the public or private sector, foreign or domestic, if there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life, property, or other vital interests of a data subject and disclosure is proper and consistent with the official duties of the person making the disclosure.[42]

[40] *Id.* at 74,118.
[41] *Id.*
[42] *Id.*

Proposed Routine Use J would permit DHS to disclose information:

> To appropriate federal, state, local, tribal, territorial, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, USCG will provide appropriate notice of any identified health threat or risk to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantined disease or for combating other significant public health threats.[43]

Proposed Routine Use M would permit DHS to disclose information:

> To appropriate federal, state, local, tribal, territorial, or foreign governmental agencies or multilateral governmental organizations if USCG is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance border security or identify other violations of law, provided disclosure is appropriate in the proper performance of the official duties of the person making the disclosure.[44]

The proposed provisions in these Routine Uses permitting DHS to disclose information to foreign agencies and international agencies must be removed. The Privacy Act only applies to records maintained by United States government agencies.[45] Releasing information to foreign entities does not protect individuals included in the Sea Arrival/Departure Database from Privacy Act violations. DHS does not have jurisdiction over foreign agents. Therefore, the provisions in these Routine Uses that would permit DHS to disclose information to foreign or multilateral entities must be removed.

V. DHS's Proposed Routine Use N Contravenes the Legislative Intent of the Privacy Act

The DHS also proposes to create 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."[46]

Proposed Routine Use N would permit 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's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific

[43] *Id.*
[44] *Id.*
[45] 5 U.S.C. § 552a(b).
[46] Sea Arrival/Departure SORN, 80 Fed. Reg. at 74,118.

information in the context of a particular case would constitute an unwarranted invasion of personal privacy.[47]

The limitations on disclosure in proposed Routine Use N is too broad to have any substantive effect, creates opportunities for violations of statutory rights, and goes against the legislative intent of the Privacy Act. As it stands, Routine Use N directly contradicts Congressman William Moorhead's testimony that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[48]

The phrase "when disclosure is necessary to preserve confidence in the integrity of DHS"[49] in Routine Use N 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; DHS could take advantage of this criterion to unduly influence its image. DHS should remove this phrase from the proposed Routine Use because creating a category that is too broad can easily lead to the abuse of privacy rights of individuals whose data has been gathered and stored by DHS.

Conclusion

For the foregoing reasons, the proposed Sea Arrival/Departure Database is contrary to the core purpose of the federal Privacy Act. Accordingly, DHS must narrow the scope of its proposed Privacy Act exemptions and not adopt its proposed unlawful routine use disclosures.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associate Director and
Administrative Law Counsel

John Tran
EPIC FOIA Counsel and
Open Government Coordinator

[47] *Id.*
[48] Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy, 1031 (1976).
[49] Sea Arrival/Departure SORN, 80 Fed. Reg. at 74,118.