COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE DRUG ENFORCEMENT ADMINISTRATION of the

DEPARTMENT OF JUSTICE

[CPCLO Order No. 006-2012]

Proposed Rule: Privacy Act of 1974 Exemptions

May 18, 2012

By notice published on April 18, 2012, the Drug Enforcement Administration ("DEA") of the Department of Justice ("DOJ") has proposed to exempt the "Investigative Reporting and Filing System (IRFS), JUSTICE/DEA—008" ("IRFS") system of records from certain provisions of the Privacy Act of 1974.[1]

Pursuant to the notice in the Federal Register, the Electronic Privacy Information Center ("EPIC") submits these comments to address the substantial privacy issues raised by the proposed exemptions. Specifically, EPIC notes: (1) the proposed exemptions contravene the intent of the Privacy Act; (2) the DEA does not clearly articulate its legal authority to claim certain exemptions; (3**)** the DEA is required to collect only relevant and necessary information, and therefore, it should limit its information collection; (4) individuals within the IRFS system of records should have access to their information after criminal investigations are complete; and (5) individuals within the system should have a right to correct their information.

[1] Privacy Act of 1974: Proposed Rule; Drug Enforcement Administration, United States Department of Justice, 75 Fed. Reg. 23173 (proposed Apr. 18, 2012) (to be codified at 28 C.F.R. pt. 16.98 (i)(j)).

EPIC is a public interest research center in Washington, D.C., established in 1994 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 preserving privacy safeguards established by Congress, including the Privacy Act of 1974, and routinely comments in public rulemakings on agency proposals that would diminish the privacy rights and agency obligations set out in the federal Privacy Act.[2]

The Scope of the System of Records

The DEA proposes to exempt the IRFS system of records from the Privacy Act. This system of records notice was first published in its entirety on October 17, 1996.[3] On April 11, 2012, pursuant to a Federal Register notice, the DEA proposed to modify the IRFS, including the categories of individuals covered by IRFS, the categories of records

[2] *See, e.g.*, Letter from Marc Rotenberg, Khaliah Barnes, and Alan Butler, EPIC, to Senator Daniel Akaka, Chairman, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (May 14, 2012), *available at http://epic.org/privacy/1974act/EPIC-Supp-S1732-Priv-Act-Modernization.pdf;* Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC), Federal Aviation Administration, et al., v. Stanmore Cawthon Cooper (2011)(No. 10-1024), *available at* http://epic.org/amicus/cooper/Cooper-EPIC-Brief.pdf; Brief of *Amici Curiae* Electronic Privacy Information Center, et. al and 16 Legal Scholars and Technical Experts, Buck Doe v. Elaine Chao, Secretary of Labor, 540 U.S. 614 (2004), *available at* http://epic.org/privacy/chao/Doe_amicus.pdf*;* Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records, DHS-2011-0082 (Nov. 28, 2011), *available* at http://epic.org/privacy/1974act/EPIC-DHS-2011-0082.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records, DHS-2011-0030 (June 8, 2011), *available at* http://epic.org/privacy/EPIC%20E-Verify%20Comments%20Final%2006.08.11.pdf; Comments of the Electronic Privacy Information Center to the Office of the Director of National Intelligence, Notice of Privacy Act System of Records (May 12, 2010), *available at* http://epic.org/privacy/ODNI_Comments_2010-05-12.pdf; Comments of the Electronic Privacy Information Center to the Department of Homeland Security, Notice of Privacy Act System of Records: U.S. Customs and Border Protection, Automated Targeting System, System of Records and Notice of Proposed Rulemaking: Implementation of Exemptions; Automated Targeting System(Sept. 5, 2007), *available at* http://epic.org/privacy/travel/ats/epic_090507.pdf.

[3] Privacy Act of 1974; Modified System of Records, 61 Fed. Reg. 54219 (proposed Oct. 17, 1996).

within the system, the purposes of the system, and the system's routine uses for disclosure.[4] The modified categories of individuals covered by the system include

> Drug offenders; alleged drug offenders; persons suspected of conspiring to commit, aiding or abetting the commission of, or committing a drug offense; defendants and respondents; other individuals related to, or associated with, DEA's law enforcement investigations into and intelligence operations [concerning the aforementioned individuals], including witnesses, confidential sources, and victims of crimes; and system users in connection with audit log information.[5]

The categories of records in the system include

> law enforcement intelligence and investigative information in paper and/or electronic form, including information compiled for the purpose of identifying criminal, civil, and regulatory offenders; reports of investigations; identifying data and notations of arrest, the nature and disposition of allegations and charges, sentencing, confinement, release, and parole and probation status; intelligence information on individuals suspected to be violating laws and regulations; fingerprints and palmprints; laboratory reports of evidence analysis; photographs; records of electronic surveillance; seized property reports; polygraph examinations; and audit log information.[6]

The purpose of IRFS is "to enforce the Comprehensive Drug Abuse Prevention and Control Act of 1970, as amended, its implementing regulations, and related statutes."[7]

DEA proposed a staggering twenty-seven routine uses, which authorize the agency to disclose personally identifiable information outside of the DEA.[8] Pursuant to the routine uses, individuals within the IRFS system of records could have information

[4] Privacy Act of 1974; Modified System of Records, 77 Fed. Reg. 21808 (proposed Apr. 11, 2012).
[5] *Id.* at 21809.
[6] *Id.*
[7] *Id.*
[8] *Id.*

disclosed to various federal government agencies, law enforcement personnel, and numerous federal, state, local, territorial, tribal, foreign, and/or international entities.[9]

Although the agency intends to disclose troves of personally identifiable information to a seemingly endless list of recipients, DEA now proposes to deny individuals within the IRFS system of records the right to access, correct, and amend their information.

I. Exemption of the Investigative Reporting and Filing System Contravenes the Intent of the Privacy Act.

As noted above, the IRFS contains a vast amount of information about an array of individuals. It contains records on both convicted drug offenders individuals, as well presumptively innocent individuals, such as those simply suspected or alleged of drug offenses. The DEA, however, seeks to invoke broad exemptions from the Privacy Act that would allow its employees to use sensitive information with little accountability and deny individuals access to records containing information pertaining to them.

The DEA proposes exempting IRFS from all Privacy Act provisions guaranteeing citizens the right to access records containing information about them and provisions defining the government's obligation to allow citizens to challenge the accuracy of information contained in their records. The exemptions proposed are: "5 U.S.C. 552a(c)(3) and (4); (d)(1), (2), (3), and (4); (e)(1), (2), (3), (4)(G) (H) (I), (5), and (8); (f), and (h)" pursuant to 5 U.S.C. 552a(j)(2), (k)(1), or (k)(2)."[10] These provisions of the Privacy Act provide that:

- an agency must give individuals access to the accounting of disclosure of

[9] *Id*. at 21809-10.
[10] 75 Fed. Reg. 23175.

their records;[11]

- any agency or individual to whom the records are disclosed must also receive "any correction or notation of dispute";[12]

- individual may request access to records an agency maintains about him or her;[13]
- an agency must correct identified inaccuracies promptly;[14]

- an agency must make notes of requested amendments within the records;[15]

- an agency must ensure it only collects data "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President";[16]

- an agency must "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";[17]

- each individual must be informed whom the agency asks to supply information;[18]

- an agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access;[19]

- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records[20]; and,

- an individual may seek judicial review to enforce the statutory right of access provided by the Act.[21]

The broad exemptions that DEA proposes would allow the agency to create and use

[11] 5 U.S.C. § 552a(c)(3).
[12] 5 U.S.C. § 552a(c)(4).
[13] 5 U.S.C. § 552a(d)(1).
[14] 5 U.S.C. § 552a(d)(2)(B), (d)(3)
[15] 5 U.S.C. § 552a(d)(4).
[16] 5 U.S.C. § 552a(e)(1).
[17] 5 U.S.C. § 552a(e)(2).
[18] 5 U.S.C. § 552a(e)(3).
[19] 5 U.S.C. §§ 552a(e)(4(G),(e)(4)(H),(f).
[20] 5 U.S.C. § 552a(f)(4).
[21] 5 U.S.C. § 552a(g)(1).

this massive database with little accountability, which contravenes the Privacy Act's intent. 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.[22] 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."[23] Thus, Congress sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[24] As the Supreme Court recently explained:

> The Privacy Act of 1974, codified in part at 5 U. S. C. §552a, contains a comprehensive and detailed set of requirements for the management of confidential records held by Executive Branch agencies. If an agency fails to comply with those requirements "in such a way as to have an adverse effect on an individual," the Act authorizes the individual to bring a civil action against the agency. §552a(g)(1)(D).

FAA v. Cooper, 566 U.S ___ (2012) (slip opinion).

II. The DEA Does Not Have Clear Statutory Authority to Claim the Proposed Privacy Act Exemptions.

As an initial matter, we note that the DEA has invoked 5 U.S.C. § 552a(k)(2) as authority for its exemption of specific Privacy Act requirements. Subsection (k)(2) is applicable only where the system of records is "investigatory material compiled for law enforcement purposes."[25] The subsection provides, however, that

[22] S. Rep. No. 93-1183 at 1 (1974).
[23] Pub. L. No. 93-579 (1974).
[24] *Id.*
[25] 5 U.S.C. § 552a(k)(2).

> if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.[26]

Given that the DEA seeks to exempt the IRFS system of records from the Privacy Act's access provisions, as we discuss below, it is unclear whether subsection (k)(2) authorizes the DEA's action. As such, we urge the DEA to explain how (k)(2) gives the agency authority to exempt the system of records from the Privacy Act provision that it cites.

We also question whether the DEA's invocation of exemptions is procedurally and substantively sound. The legislative history of the Privacy Act suggests it is not:

> Once the agency head determines that he has information legitimately in one of his information systems which falls within these definitions [of exempted categories] then he must, via the rulemaking process, determine that application of the challenge, access and disclosure provisions would "seriously damage or impede the purpose for which the information is maintained." The Committee intends that this public rulemaking process would involve candid discussion of the general type of information that the agency maintains which it feels falls within these definitions and the reasons why access, challenge or disclosure would "seriously damage" the purpose of the maintenance of the information. The Committee hastens to point out that even if the agency head can legitimately make such a finding he can only exempt the information itself or classes of such information . . . and not a whole filing system simply because intelligence or investigative information is commingled with information and files which should be legitimately subject to the access, challenge and disclosure provisions.[27]

[26] *Id*.
[27] S. Rep. No. 93-3418, at 75 (1974).

Although the DEA provides purported justifications for the proposed exemptions, the application of the claimed exemptions to the entire system of records is clearly inappropriate, as it will obviously contain information "which should be legitimately subject to the access, challenge and disclosure provisions."[28]

Additionally, the DEA states that "[w]here compliance would not interfere with or adversely affect the law enforcement or counterterrorism purposes of this system, or the overall law enforcement process, the applicable exemption *may* be waived by the DEA in its sole discretion."[29] The Privacy Act, however, *requires* that if the system of records is not explicitly exempt, agencies cannot claim exemptions, and therefore *must* waive exemptions. Contrary to the DEA's statement, it is not within the agency's sole discretion to waive an exemption if the exemption does not apply.

The DEA must cure these defects before collecting personal data for inclusion in the Investigation Reporting and Filing system of records.

III. The Privacy Act Requires DEA to Collect Only Relevant and Necessary Information. Therefore, the DEA Should Narrowly Tailor its Collection of Records.

The Privacy Act's "relevant and necessary" requirement is a fundamental and necessary part of the Privacy Act's protections, as it is designed to assure observance of basic principles of privacy and due process by requiring that where an agency delves into an area of personal privacy in the course of meeting government's needs, its actions may not be arbitrary.[30]

---

[28] *See also*, Office of Management and Budget, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28948, 28972 (July 9, 1975) ("OMB Guidelines") ("agencies should, wherever practicable, segregate those portions of systems for which an exemption is considered necessary so as to hold to the minimum the amount of material which is exempted").
[29] 75 Fed. Reg. 23175 (emphasis added).
[30] S. Rep. No. 93-3418, at 47 (1974).

Part of the Privacy Act's purpose was to stave off the risk that government databases might become dossiers cataloging the various details of individuals' lives. By limiting the data kept by an agency to that which is necessary and relevant to the agency's purpose, the Privacy Act limits the extent to which a system of records may invade privacy. Limiting the data to that which is necessary and relevant also reduces the risk of "mission creep," in which a system is pressed into unintended uses. Such mission creep presents additional opportunity for errors, as has been seen in other DOJ component agency databases.[31]

The DEA claims that, as a system of investigatory records, the Investigative Reporting and Filing System must gather data whose relevance may not be known at the time. The DEA also notes that relevance and necessity are questions of judgment and timing. An investigation will likely begin with a broader scope than it ends with, and information at first gathered may later become irrelevant and unnecessary. However, the mere fact that relevance and necessity may change should not be a reason for the DEA to completely absolve itself of its Privacy Act obligations. A blanket exemption from §§ 552a(e)(1) and (e)(5) requirements would allow the records to contain wholly and blatantly irrelevant and unnecessary information unrelated to any purpose of the DEA. Furthermore, in assessing the necessity and relevance of records kept in a system, the nature of the system would be taken into account. Any facts in the system that might be helpful to the DEA in a particular investigation would hopefully be relevant and necessary to the investigation at some stage, and thus in compliance with the Privacy Act. As investigations proceed to a close, information can be added or removed from the

[31] Eric Lichtblau, *Justice Dept. Finds Flaws in F.B.I. Terror List*, THE NEW YORK TIMES, May 6, 2009, at A22, *available at* http://www.nytimes.com/2009/05/07/us/07terror.html.

system as it becomes more or less relevant and necessary. Therefore, the DEA should not exempt its IRFS system of records from the relevance and necessity requirements, as doing so would eliminate a vital privacy safeguard while failing to add any flexibility benefits not already provided by the Act.

IV. After an Investigation is Complete or Made Public, Individuals Should Have Access To Their Records.

EPIC also urges the DEA to limit its exemptions from the Privacy Act's provisions requiring disclosure to individuals of records kept about them and requiring notification of the systems of records and how to access them. [32] The DEA also claims exemption from Privacy Act Subsection (e)(8). This subsection mandates that the agency "makes 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."[33] If the process is a "matter of public record," it is unknown what value would be gained by exempting the agency from its Privacy Act obligation to make reasonable efforts to serve notice on an affected individual. This broad exception only serves to increase the secrecy of the database.

The DEA claims that these notification and access provisions, if implemented, may put entities on notice that they are being investigated. While EPIC recognizes the need to withhold notice during the period of the investigation, entities should be able to know, after an investigation is completed or made public, the information stored about them in the system. Since the DEA depends, at least in part, upon informants to initiate investigations, individuals within the DEA's purview may find themselves investigated

[32] 5 U.S.C. § 552a(c)(3).
[33] 5 U.S.C. § 552(a)(e)(8).

due to malicious misinformation spread by bad actors. Access to records of a completed investigation, with appropriate redactions to protect the identities of confidential informants, would provide individuals and entities with the right to address potential inaccuracies an completed investigations would not undermine the DEA's law enforcement purposes, while protecting the privacy rights of entities and their individual members. For the foregoing reasons, EPIC urges the DEA not to exempt itself from the relevance and necessity requirements of the Privacy Act, and to limit the scope of its exemptions from the notice and access provisions, by allowing entities to access files kept on them, insofar as the investigations have been completed.

V. Individuals Should have the Right to Correct Misinformation Contained Within DEA's System of Records.

The rights of access and correction are central to what Congress sought to achieve through the Privacy Act:

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[34]

The DEA proposes to deny individuals the critical right of record correction because, according to the agency, it would "interfere with ongoing investigations," and would impose" an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised. . ."[35] The agency, however, gives no consideration to the burdens placed on individuals that arise from government

[34] H.R. Rep. No. 93-1416 at 15 (1974).
[35] 75 Fed. Reg. 23175.

agency misinformation. Individuals erroneously listed in the IRFS system of records can be subject to investigations by federal and local law enforcement agencies. Therefore, individuals should be permitted to correct agency misinformation within the IRFS.

Additionally, the agency proposes to exempt itself from subsection (g) of the Privacy Act. Subsection (g) specifies the civil remedies that an individual has against an agency for failure to comply with its obligations under the Privacy Act. Exempting IRFS from subsection (g) of the Privacy Act means that individuals will have no judicially enforceable rights of access to their records or correction of erroneous information in such records.

Conclusion

For the foregoing reasons, EPIC believes that the DEA must revise its Privacy Act notice for the Investigative Reporting and Filing System to: (1) clearly establish its authority to claim certain Privacy Act exemptions; (2) limit the collection of information to only that which is necessary and relevant; (3) provide individuals enforceable rights of access and correction; and (4) uphold the Privacy Act's civil remedies provision. Finally, the agency should not acquire personal information, until it has revised its Privacy Act notice as suggested above.

Respectfully submitted

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Open Government Fellow