



February 20, 2015

VIA FACSIMILE and EMAIL

Freedom of Information & Privacy Act Unit (SARF)
 Drug Enforcement Administration
 8701 Morrisette Drive
 Springfield, VA 22152
 Fax: (202) 307-8556
 Email: DEA.FOIA@usdoj.gov

1718 Connecticut Ave NW
 Suite 200
 Washington DC 20009
 USA
 +1 202 483 1140 [tel]
 +1 202 483 1248 [fax]
 www.epic.org

RE: Freedom of Information Act Request

Dear FOIA Officer:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Drug Enforcement Administration ("DEA").

EPIC seeks all of the DEA's privacy assessments not already published online.

Background

The E-Government Act of 2002 requires agencies to perform Privacy Impact Assessments ("PIAs") under certain circumstances. For example, PIAs are required when "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form" or "initiating a new collection of information" that contains identifiable information.¹ Additionally, the PIAs are required to be made public if practicable.²

The Department of Justice ("DOJ") provides additional guidance to DOJ components on performing privacy assessments, including the PIAs required by the E-Government Act of 2002. Specifically, the DOJ's Office of Privacy and Civil Liberties ("OPCL") describes when to do an Initial Privacy Assessment ("IPA"), a precursor to the PIA, and provides guidance on doing a PIA if the initial assessment requires it. The IPA, which has replaced the Privacy Threshold Analysis ("PTA"), "is a tool used to facilitate the identification of potential privacy issues; assess whether additional privacy documentation is required; and ultimately, to ensure the Department's

¹ E-GOVERNMENT ACT OF 2002, PL 107-347, Dec. 17, 2002, 116 Stat. 2899 § 208(b)(1)(A)(i)-(ii); See also M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, available at http://www.whitehouse.gov/omb/memoranda_m03-22.

² *Id.* at § 208(b)(1)(B)(iii).

compliance with applicable privacy laws and policies."³ The IPA "identif[ies] privacy concerns that may necessitate changes to the system and [determines] whether additional privacy analysis and documentation are required, such as a system of records notice (SORN) or collection notice under the Privacy Act, or a Privacy Impact Assessment (PIA) under the E-Government Act."⁴ According to OPCL, the "IPA should be completed at the beginning of development of an information system, before commencement of any testing or piloting."⁵

The OPCL assesses all IPAs to determine if a PIA is needed. "Once OPCL provides a component with a determination that a PIA is required, a PIA should be conducted."⁶ According to the OPCL, the PIA should be conducted during development, "with sufficient lead time to permit final Departmental approval and public website posting on or before the commencement of any system operation (including before any testing or piloting)."⁷ PIAs are required for national security systems too. It is the DOJ's "policy that PIAs must also be conducted for national security systems and submitted to OPCL for review and approval by the CPCLO."⁸

As DOJ documentation notes, the PIA "helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions."⁹ PIAs provide an important means for the public to assess the government's efforts to protect its privacy and serve as a check against the encroachment on privacy by the government. Specifically, PIAs allow the public to see how new programs and technology the government implement affect their privacy and assess whether the government has done enough to mitigate the privacy risks.

The DEA currently has several programs that employ, or employed, information systems for which PTAs, IPAs or PIAs should have been conducted in accordance with DOJ guidance that of the writing of this FOIA request are not publicly available.

Some programs, such as the Hemisphere program, which since 2007 has enabled law enforcement direct access to an AT&T database of telephone call records, are already known and are actively being litigated.¹⁰ Indeed, on September 25, 2013, EPIC submitted, via certified mail, a FOIA request to the DEA seeking records regarding the Hemisphere program.¹¹ That FOIA

³ United States Department of Justice Office of Privacy and Civil Liberties (OPCL), Initial Privacy Assessment (IPA) Instructions & Template, 1 (Mar. 2010), *available at* <http://www.justice.gov/opcl/initial-privacy-assessment.pdf>.

⁴ *Id.*

⁵ *Id.*

⁶ Office of Privacy and Civil Liberties United States Department of Justice, Privacy Impact Assessments: Official Guidance, 4 (Mar. 2012), *available at* <http://www.justice.gov/opcl/docs/2012-doj-pia-manual.pdf>.

⁷ *Id.*

⁸ *Id.*

⁹ *Id.* at 3.

¹⁰ See EPIC: EPIC v. DEA - Hemisphere, <https://epic.org/foia/dea/hemisphere/>.

¹¹ Freedom of Information Act Documents: EPIC's FOIA Request to the DEA (Sep. 25, 2013), *available at* <http://epic.org/foia/dea/EPIC-FOIA-DEA-09-25-13.pdf>.

request is currently the subject of litigation before the U.S. District Court for the District of Columbia.¹²

However, other programs are less known, or entirely unknown, but are no less subject to privacy concerns necessitating the analysis of a PTA, IPA, or PIA. The following is meant to serve as a non-exclusive selection of DEA programs for which no PTA, IPA or PIA is publicly available.

On May 21, 2012, the U.S. House of Representatives Subcommittee on Border and Maritime Security held a field hearing on “Stopping The Flow Of Illicit Drugs In Arizona By Leveraging State, Local And Federal Information Sharing”.¹³ At that hearing, Douglas W. Coleman, Special Agent in Charge, Phoenix Field Division of the DEA, was one of the witnesses. In his statement for the record, Mr. Coleman indicated that “[i]n December 2008, DEA launched a National License Plate Reader (LPR) Initiative in direct response to the smuggling of illicit drug monies out of the United States, primarily via the U.S.- Mexico border.”¹⁴ According to Mr. Coleman’s statement for the record, the DEA’s LPR program monitors and targets vehicles, uses existing database technology, and promotes information sharing.¹⁵

The DEA’s LPR program has recently been the subject of reports by U.S. news media, including the Wall Street Journal.¹⁶ On January 28, 2015, Chairman Charles E. Grassley and Ranking Member Patrick Leahy of the Senate Judiciary Committee sent a letter to Attorney General Eric Holder regarding privacy concerns related to the government’s use of LPRs. The Senators stated, “we remain concerned that government programs that track citizens’ movements, see inside homes, and collect data from the phones of innocent Americans raise serious privacy concerns.”¹⁷ Despite these privacy concerns no PTA, IPA, or PIA for the DEA’s LPR program is publicly available.

During the same field hearing, again in his statement for the record, Mr. Coleman identified another program entitled the DEA Internet Connectivity Endeavor (“DICE”) that “... enables any participating federal, state, local and tribal law enforcement agency to de-conflict investigative information, such as phone numbers, email addresses, bank accounts, plane tail numbers and license plates, to identify investigative overlaps.”¹⁸ DICE provides access to

¹² Complaint, Electronic Privacy Information Center v. Drug Enforcement Administration, No. 14-cv-317 (D.D.C. Feb. 26, 2014).

¹³ <http://homeland.house.gov/hearing/subcommittee-field-hearing-stopping-flow-illicit-drugs-arizona-leveraging-state-local-and>.

¹⁴ *Stopping The Flow Of Illicit Drugs In Arizona By Leveraging State, Local And Federal Information Sharing: Hearing Before the Subcomm. on Border and Maritime Security of the House Comm. on Homeland Security*, 112th Cong. 3 (2012) (statement of Douglas W. Coleman, Special Agent in Charge, DEA).

¹⁵ *Id.*

¹⁶ Devlin Barrett, *U.S. Spies on Millions of Drivers*, WALL ST. J. (Jan. 26, 2015), <http://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779>.

¹⁷ Letter from Senators Patrick Leahy and Charles Grassley to Attorney General Eric Holder on DEA License Plate Reader Privacy Concerns (Jan. 28, 2015), *available at* <http://www.leahy.senate.gov/download/012815-leahy-grassley-to-holder-re-dea-lpr>.

¹⁸ Coleman, *supra* note 11.

information collected through the LPR program (amongst other information), and allows the accessibility of such data through the Internet.¹⁹ Reuters previously reported that DICE contains approximately 1 Billion records, including phone log data.²⁰

Additionally, in an effort to promote information sharing amongst the DEA and over 20 different participating agencies, the DEA has also created the Special Operations Division (“SOD”). The SOD is “... a DEA led, multi-agency, operational coordination center whose mission is to establish seamless law enforcement strategies and operations aimed at dismantling national and international trafficking organizations by attacking their command and control communications.”²¹ In Mr. Coleman’s oral testimony at the same May 21, 2012 hearing, he spoke generally about information sharing and indicated that there is virtually no piece of information that the DEA has (aside from classified information) that state, local, or tribal law enforcement agencies cannot access.²² There is no PTA, IPA, or PIA for the DEA’s DICE program or the SOD that is publicly available.

On January 15, 2015, in a declaration filed with the U.S. District Court for the District of Columbia under Order of the Court, Assistant Special Agent in Charge of the Drug Enforcement Agency, Robert Patterson, referred to a law enforcement database, which is no longer in use and the name of which has been redacted.²³ Mr. Patterson stated that “[t]his database consisted of telecommunications metadata obtained from United States telecommunications service providers pursuant to administrative subpoenas ...”²⁴ Mr. Patterson further indicated that the database could be used to query telephone numbers by federal law enforcement officials who have a reasonable articulable suspicion that the telephone number being queried was related to a current criminal investigation.²⁵ No PTA, IPA, or PIA for the DEA’s unnamed program is publicly available.

The scope of the collection of personally identifiable information by DEA programs, along with the obvious privacy implications are positive indications that PTAs, IPAs, or PIAs for these programs should exist. Yet, no privacy assessments for these DEA programs are publicly available.

¹⁹ *Id.*

²⁰ John Shiffman, *How DEA program differs from recent NSA revelations*, REUTERS (Aug. 5, 2013, 5:16 AM), <http://www.reuters.com/article/2013/08/05/us-dea-sod-nsa-idUSBRE9740AI20130805>.

²¹ Coleman, *supra* note 11.

²² Committee on Homeland Security, *Subcommittee Field Hearing: Stopping The Flow Of Illicit Drugs In Arizona By Leveraging State, Local And Federal Information Sharing* 1:06:06 http://mfile3.akamai.com/65736/wmv/sos1469-1.streamos.download.akamai.com/65740/chs_112th/05-21-12-BMS-Field.asx.

²³ Although the name of the database is unknown, it is possible that this database is related to the above referenced programs Hemisphere and/or DICE.

²⁴ Declaration of Robert Patterson at 2, *United States v. Shantia Hassanshahi*, 989 F. Supp. 2d 110 (D.D.C. 2013) (No. 1:13-cr-00274-RC).

²⁵ *Id.*

Documents Requested

1. All Privacy Impact Assessments the DEA has conducted that are not publicly available at <http://www.dea.gov/FOIA/PIA.shtml>.²⁶
2. All Privacy Threshold Analysis documents and Initial Privacy Assessments the DEA has conducted since 2007 to present.

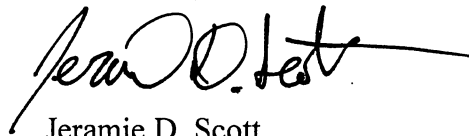
Request for “News Media” Fee Status

EPIC is a “representative of the news media” for fee waiver purposes.²⁷ As such, EPIC is entitled to receive the requested record for the cost of duplication only. Because disclosing this information will “contribute significantly to public understanding of the operations or activities of the government,” any duplication fees should be waived.²⁸

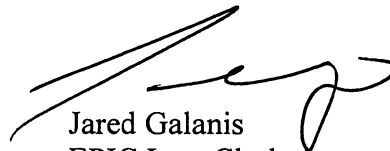
Conclusion

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(a)(6)(E)(ii)(I), we will anticipate your response within 20 business days. Should you require additional information, please contact Jeramie Scott at 202-483-1140 x108 or foia@epic.org.

Respectfully Submitted,



Jeramie D. Scott
EPIC National Security Counsel



Jared Galanis
EPIC Law Clerk

²⁶ See Attachment 1.

²⁷ *EPIC v. Dep’t of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).

²⁸ 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).