UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. FEDERAL BUREAU OF INVESTIGATION, Defendant.	)	Civil Action No. 14-1311 (APM)

PLAINTIFF'S STATEMENT OF MATERIAL FACTS NOT IN DISPUTE AND RESPONSE TO DEFENDANT'S STATEMENT OF FACTS NOT IN DISPUTE

Pursuant to Local Rule 7(h) of the Rules of the United States District Court for the District of Columbia, Plaintiff Electronic Privacy Information Center ("EPIC") hereby submits the following statement of material facts as to which EPIC contends there is no genuine issue in connection with its cross-motion for partial summary judgment, and EPIC's response to Defendant's statement of material facts.

1. EPIC agrees that the matters set forth in ¶¶ 1–17 of Defendant's statement of material facts are not in dispute.
2. EPIC disputes ¶¶ 18–22 of Defendant's statement of material facts to the extent they are inconsistent with the statements set forth in the Declaration of David M. Hardy. EPIC respectfully refers the Court to the Hardy Declaration (ECF No. 26-2).
3. EPIC submits that ¶ 23 of Defendant's statement of material facts is not material because the FBI has not established that the agency conducted an adequate search

for responsive records. To the extent the paragraph contains any material facts, EPIC disputes them.

4. EPIC agrees that ¶¶ 24–25 of Defendant's statement of material facts are not in dispute.
5. EPIC submits that ¶ 26 of Defendant's statement of material facts is a legal conclusion in dispute in this case as it pertains to Exemption 7(E). To the extent the paragraph pertains to Exemption 5, EPIC submits it is not material.
6. EPIC submits that ¶¶ 27–32 of Defendant's statement of material facts are not material as they relate to Defendant's Exemption 5 claim, which is no longer in dispute in this case.
7. EPIC disputes ¶ 33 of Defendant's statement of material facts and submits that they are not material because the Privacy Impact Assessments and Privacy Threshold Analysis were compiled to facilitate agency compliance with privacy and transparency laws.
8. EPIC submits that ¶¶ 34–35 of Defendant's statement of material facts are legal conclusions and in dispute in this case.
9. EPIC submits that ¶¶ 36–38 of Defendant's statement of material facts are not material because the disputed records are not compiled for law enforcement purposes.
10. EPIC submits that ¶¶ 39–41 of Defendant's statement of material facts are conclusions of law in dispute in this case.
11. EPIC submits that ¶ 42 of Defendant's statement of material facts is not material in so far as it pertains to Exemption 5 and 7(D), which are no longer in dispute.

With respect to EPIC's challenges to the sufficiency of FBI's search, the FBI's segregability analysis, and the FBI's withholdings pursuant to Exemption 7(E), EPIC states that these challenges apply beyond the sample set.

12. The FBI is required to conduct privacy assessments whenever they "develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form." DOJ, *E-Government Act of 2002* (June 18, 2014);[1] *see* E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921–23 (codified at 44 U.S.C. § 3501 note).

13. The purpose of the E-Government Act is "to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government." E-Government Act at § 208(a).

14. A PIA is "an analysis of how information in identifiable form is collected, stored, protected, shared, and managed in an Information Technology (IT) system or online collection." Hardy Decl. ¶ 6.

15. A PTA, in turn, determines whether the agency is required to prepare a PIA. *Id.* ¶ 7.[2]

[1] https://www.justice.gov/opcl/e-government-act-2002.

[2] The Department of Justice uses the term "Initial Privacy Assessment ('IPA')" to describe this process whereas the FBI uses the term PTA. Hardy Decl. ¶ 7 n.3. An IPA "is the first step in a process developed by [Office of Privacy and Civil Liberties] to assist DOJ components in the development and use of information systems." DOJ, Office of Privacy & Civil Liberties, *Initial Privacy Assessment (IPA) Instructions & Template* (May 2015), https://www.justice.gov/opcl/file/629231/download.

16. PTAs and IPAs are "used to facilitate the identification of potential privacy issues; assess whether additional privacy documentation is required; and ultimately, to ensure the Department's compliance with applicable privacy laws and policies." DOJ, Office of Privacy & Civil Liberties, *Initial Privacy Assessment (IPA) Instructions & Template* (May 2015)[3] [hereinafter DOJ IPA Guidance].
17. A PIA is required to ensure that privacy is considered "from the beginning stages of a system's development and throughout the system's life cycle," and to ensure "that privacy protections are built into the system from the start—not after the fact." DOJ, Office of Privacy & Civil Liberties, *Privacy Impact Assessments Official Guidance* 3 (July 2015)[4] [hereinafter DOJ PIA Guidance].
18. A PIA is also intended to insure that "system developers and owners have made technology choices that reflect the incorporation of privacy into the fundamental system architecture." *Id.* at 4.
19. PTAs provide only checklist-based answers to basic questions about the information system. DOJ IPA Guidance.
20. Both initial and final agency privacy assessments must be completed prior to the implementation of an information system. *See* Office of Privacy and Civil Liberties United States Department of Justice, *Privacy Impact Assessments: Official Guidance* 2 (Revised July 2015); *See also* U.S. Dep't of Justice Office of Privacy and Civil Liberties (OPCL), *Initial Privacy Assessments (IPA) Instructions & Template* (Revised March 2010).

[3] https://www.justice.gov/opcl/file/629231/download.
[4] https://www.justice.gov/opcl/file/631431/download.

21. PIAs and PTAs inform the public of potential privacy risks associated with its information systems and help "promote trust between the public and the Department by increasing transparency of the Department's systems and missions." Office of Privacy and Civil Liberties United States Department of Justice, *Privacy Impact Assessments: Official Guidance* 2 (Revised July 2015).
22. Congress intended PIAs to be made "publicly available." E-Government Act § 208(b)(1)(B)(iii).
23. The PCLU and its officers do not engage in law enforcement investigations. FBI, *Today's FBI: Facts and Figures 2010–2011*, at 56 (Tamara R. Harrison, ed., 2011).
24. The Privacy and Civil Liberties Officer "assists in developing and evaluating legislative, regulatory, and other policy proposals that implicate privacy issues," and "oversees, coordinates, and facilitates agency privacy compliance with laws, regulations, and policies relating to information privacy." Hardy Decl. ¶ 23.
25. The FBI is withholding the "terminology" used to refer to the systems that the agency was required under federal privacy law to analyze in the PIAs and PTAs. *See* Def.'s Mot. at 17; Hardy Decl. ¶ 38; Ex. 1 at 3, 35–66, 68, 70, 74–78, 87–88, 94–98, 101–105, 108, 119, 122, 127–135, 138, 145, 155–163.[5]

[5] Bates numbers EPIC-2, EPIC-217, EPIC-219 through EPIC-222, EPIC-227 through EPIC-233, EPIC-252 through EPIC-257, EPIC-372 through EPIC-378, EPIC-379 through EPIC-385, EPIC-504, EPIC-563, EPIC-587 through EPIC-592, EPIC-717 through EPIC-718, EPIC-811 through EPIC-814, EPIC-834, EPIC-866 through EPIC-870, EPIC-928, EPIC-1349, EPIC-1497, EPIC-1562 through EPIC-1569, EPIC-1712, EPIC-1927, EPIC-2217 through EPIC-2219, EPIC-2258 through EPIC-2263.

26. Disclosure of "FBI units, and or joint units, partners (e.g. federal contractors) participating in program and system development, and system testing" would not reveal investigative techniques or procedures.
27. Disclosure of "software and hardware specifications, system infrastructure, and security protocols used to operate and maintain" FBI systems would not reveal investigative techniques or procedures.

Dated: June 3, 2016

Respectfully submitted,

MARC ROTENBERG
EPIC President

ALAN JAY BUTLER
EPIC Senior Counsel

/s/ Jeramie D. Scott
JERAMIE D. SCOTT
D.C. BAR # 1025909
EPIC National Security Counsel
Electronic Privacy Information Center
1718 Connecticut Ave., NW
Suite 200
Washington, DC 20009

Counsel for Plaintiff