IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20009,

Plaintiff,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY,
Washington, D.C. 20528

Defendant.

Civ. Action No. 18-1268

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552; the Administrative Procedure Act ("APA"), 5 U.S.C. §§ 551–706; the E-Government Act of 2002, 44 U.S.C. § 3501 note; and the Declaratory Judgment Act, 28 U.S.C. § 2201(a), to secure the production and release of records requested by Plaintiff Electronic Privacy Information Center ("EPIC") from Defendant U.S. Department of Homeland Security ("DHS").

2. Specifically, EPIC seeks the release of a Privacy Impact Assessment ("PIA") for "Media Monitoring Services" and challenges (1) the DHS's failure to conduct and publish a PIA prior to the agency's April 3, 2018 solicitation of "Media Monitoring Services"; (2) the DHS's failure to make a timely decision about EPIC's FOIA request for the Media Monitoring Services PIA and related records; and (3) the DHS's failure to release records responsive to EPIC's request. EPIC seeks injunctive and other appropriate relief.

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331, 5 U.S.C. § 552(a)(6)(E)(iii), 5 U.S.C. § 552(a)(4)(B), 5 U.S.C. § 702, and 5 U.S.C. § 704. This Court has personal jurisdiction over Defendant DHS.

4. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B), 5 U.S.C. § 703, and 28 U.S.C. § 1391.

Parties

5. Plaintiff EPIC is a nonprofit organization, incorporated in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is education, oversight, and analysis of government activities that impact individual privacy, free expression, and democratic values in the information age.[1]

6. EPIC is a membership organization. The Members of EPIC's Advisory Board include distinguished experts in law, technology, and public policy.

7. EPIC maintains one of the most popular privacy websites in the world, https://epic.org, which provides EPIC's members and the public with access to information about emerging privacy and civil liberties issues. EPIC has a robust FOIA practice and routinely disseminates information obtained under the FOIA and other open government statutes to the public through the EPIC website, the biweekly EPIC Alert newsletter, and various news organizations. EPIC is a representative of the news media. *EPIC v. DOD*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

8. EPIC has brought numerous successful cases seeking the release of Privacy Impact Assessments. In *EPIC v. DHS*, No. 11-2261 (D.D.C. Dec. 20, 2011), EPIC obtained a PIA and

[1] *See* EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.

related records concerning a prior effort by the DHS to track social media users and journalists.[2] EPIC made the previously undisclosed documents available to the public on its website. In *EPIC v. FBI*, No. 14-1311 (D.D.C. Aug. 1, 2014), EPIC obtained unpublished PIAs from the Federal Bureau of Investigation concerning facial recognition technology, which EPIC also made available to the public on its website.[3] And in *EPIC v. DEA*, No. 15-667 (D.D.C. May 1, 2015), EPIC learned that the Drug Enforcement Administration had failed to produce PIAs for the agency's license plate reader program, a telecommunications records database, and other systems of public surveillance.[4] EPIC reported the agency's failure to produce a PIA on its website.

9. More recently, in *EPIC v. Presidential Advisory Commission on Election Integrity*, 266 F. Supp. 3d 297 (D.D.C.), *aff'd on other grounds*, 878 F.3d 371 (D.C. Cir. 2017), EPIC challenged the failure of the Presidential Advisory Commission on Election Integrity to undertake and publish a PIA prior to the collection of state voter data.[5] EPIC's suit led the Commission to temporarily suspend its data collection, discontinue the use of an unsafe computer server, and delete voter information that had been illegally obtained.[6]

10. Defendant Department of Homeland Security is a federal agency within the meaning of the FOIA, 5 U.S.C. § 552(f)(1); the APA, 5 U.S.C. § 551(1); and 44 U.S.C. § 3502(1). The DHS is headquartered in Washington, D.C.

---

[2] *See* EPIC, *EPIC v. Department of Homeland Security: Media Monitoring* (2015), https://www.epic.org/foia/epic-v-dhs-media-monitoring/.
[3] *See* EPIC, *EPIC v. FBI – Privacy Assessments* (2016), https://epic.org/foia/fbi/pia/.
[4] *See* EPIC, *EPIC v. DEA – Privacy Impact Assessments* (2016), https://epic.org/foia/dea/pia/.
[5] *See* EPIC, *EPIC v. Presidential Election Commission* (2018), https://epic.org/privacy/litigation/voter/epic-v-commission/.
[6] *Id.*

Facts

The DHS's Obligation to Conduct and Publish Privacy Impact Assessments

11. Under Section 208 of the E-Government Act, the DHS must undertake and publish a Privacy Impact Assessment before the agency (1) "develop[s] or procur[es] information technology that collects, maintains, or disseminates information that is in an identifiable form," or (2) "initiat[es] a new collection of information" that "includes any information in an identifiable form."[7] Information is "in an identifiable form" if it allows the identity of an individual to be directly or indirectly inferred.[8]

12. A Privacy Impact Assessment evaluates potential privacy risks "at the beginning of and throughout the development life cycle of a program or system."[9] Through the creation and publication of a PIA, the public can learn what personally identifiable information ("PII") is being collected, "why it is being collected, and how it will be used, shared, accessed, secured, and stored."[10]

13. According to the Office of Management and Budget ("OMB"), which oversees enforcement of the E-Government Act government-wide, "Agencies should commence a PIA when they begin to develop a new or significantly modified [information technology] system or information collection."[11]

---

[7] E-Government Act of 2002, Pub. L. No. 107-347, § 208(b)(1)(A), 116 Stat. 2899 (2002).
[8] U.S. Dep't Homeland Sec., *Privacy Impact Assessments: The Privacy Office Official Guidance* 1 (2010), https://www.dhs.gov/sites/default/files/publications/privacy_pia_guidance_june2010_0.pdf [hereinafter *DHS PIA Official Guidance*].
[9] U.S. Dep't of Homeland Sec., *Privacy Compliance: Privacy Impact Assessment (PIA)* (Mar. 30, 2017), https://www.dhs.gov/compliance.
[10] *Id.*
[11] Office of Mgmt. and Budget, Exec. Office of the President, M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* at 5 (Sept. 26, 2003), https://www.whitehouse.gov/wp-content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-

14. A PIA at the "IT development stage" should "address the impact the system will have on an individual's privacy specifically identifying and evaluating potential threats[.]"[12] The PIA "may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis."[13]

15. The OMB's adopted definition of "information technology" includes "any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information."[14]

16. Under DHS Privacy Office guidelines, the DHS is also expected to complete a Privacy Threshold Analysis ("PTA") as a first step in the certification and accreditation of each new technology system.[15] The PTA "identif[ies] programs and systems that are privacy-sensitive" as well as how and to what extent personally identifiable information is collected, maintained, used, or disseminated.[16] A PTA allows the DHS Privacy Office to determine whether a DHS program or system requires additional privacy compliance documentation, such as a PIA.

Implementing-the-Privacy-Provisions-of-the-E-Government-Act-of-2002-1.pdf [hereinafter *OMB E-Government Act Guidance*].

[12] *Id.*

[13] *Id.* at 5–6.

[14] *OMB E-Government Act Guidance*, *supra* note 11, at 3 (citing Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6) (2011)).

[15] *DHS PIA Official Guidance*, *supra* note 8, at 1; *see also* U.S. Dept. of Homeland Sec., *Privacy Compliance: Privacy Threshold Analysis (PTA)* (Mar. 30, 2017), https://www.dhs.gov/compliance.

[16] U.S. Dep't Homeland Sec., *Privacy Compliance: Privacy Threshold Analysis (PTA)*, *supra* note 9; *see also* U.S. Dep't Homeland Sec., *Privacy Threshold Analysis (PTA)* (2014), https://www.dhs.gov/sites/default/files/publications/privacy-dhs-pta-template-20140123.pdf.

The DHS's Solicitation of "Media Monitoring Services"

17. On April 3, 2018, the DHS's National Protection and Programs Directorate ("NPPD") published a solicitation for "Media Monitoring Services."[17] According to the draft Statement of Work ("SOW"), the agency is searching for a contractor to "provide NPPD[] with traditional and social media monitoring and communications solutions," including "media comparison tools, design and rebranding tools, communication tools, and the ability to identify top media influencers." Ex. 1.[18]

18. The SOW calls for a contractor to provide the DHS with, *inter alia*, three primary media monitoring capabilities. First, the agency seeks the ability to "track online, print, broadcast, cable, radio, trade and industry publications, local sources, national/international outlets, traditional news sources, and social media." *Id.* § 2.1. This would include the capacity to monitor over "290,000 global news sources" in over "100 languages" and to "create unlimited data tracking, statistical breakdown, and graphical analysis on any coverage on an ad-hoc basis." *Id.*

19. Second, the DHS seeks "Media Intelligence and Benchmarking Dashboard Platform" to conduct "real-time monitoring" and analysis of media coverage. *Id.* This platform would enable to DHS to "analyze the media coverage in terms of content, volume, sentiment, geographical spread, top publications, media channels, reach, [advertising value equivalency], top posters, influencers, languages, momentum, [and] circulation." *Id.* The platform would include the ability

[17] U.S. Dep't Homeland Sec., RNBO-18-00041, *Media Monitoring Services* (Apr. 3, 2018), *available at* https://web.archive.org/web/20180408074928/https://www.fbo.gov/index?s=opportunity&mode=form&id=22aa793f75ce05efd160cfa36d7a8acc&tab=core&_cview=0.

[18] U.S. Dep't Homeland Sec., *Draft Statement of Work for Media Monitoring Services* § 1.3 (2018), *available at* https://www.scribd.com/document/375735809/DHS-Statement-of-Work-for-Media-Monitoring-Services [hereinafter *Draft Statement of Work*].

to "build media lists based on beat, location, outlet type/size, and journalist role." *Id.* The DHS also seeks the development of a mobile app and email alerts to monitor media coverage. *Id.* §§ 2.3, 2.4.

20. Third, the DHS seeks the creation of an internal "media influencer database," which would contain the locations, contact information, employer affiliations, and past coverage of untold numbers of "journalists, editors, correspondents, social media influencers, bloggers, etc." *Id.* § 2.5. The database would be searchable in multiple languages by "keywords, concepts, [and] Boolean search terms." *Id.*

21. The DHS's announcement that it was developing a media influencer database drew widespread criticism given the threat to privacy that the database poses and the chilling effect it would have on press freedoms.[19] Michelle Fabio, writing in *Forbes*, warned that the DHS's planned use of Media Monitoring Services is "enough to cause nightmares of constitutional proportions, particularly as the freedom of the press is under attack worldwide."[20]

[19] *See, e.g.*, Cary O'Reilly, *Homeland Security to Compile Database of Journalists, Bloggers*, Bloomberg Big Law Business (Apr. 5, 2018), https://biglawbusiness.com/homeland-security-to-compile-database-of-journalists-bloggers/; Press Release, PEN America, Department of Homeland Security's Plants for Journalists Database Must Be Quashed Immediately (Apr. 8, 2018), https://pen.org/press-release/dhs-journalist-database-must-bequashed/.

[20] Michelle Fabio, *Department of Homeland Security Compiling Database of Journalists and 'Media Influencers'*, Forbes (Apr. 6, 2018), https://www.forbes.com/sites/michellefabio/2018/04/06/department-of-homeland-security-compiling-database-of-journalists-and-media-influencers/.

The DHS's Failure to Conduct a Privacy Impact Assessment

22. The DHS's media monitoring tools and platform will necessarily include personally identifiable information from individuals identified in the media coverage tracked by the DHS. Ex. 1 §§ 2.1, 2.2.

23. The DHS's media monitoring tools and platform therefore constitute both a "develop[ment] or procur[ement of] information technology that collects, maintains, or disseminates information that is in an identifiable form" and a "a new collection of information that . . . includes [] information in an identifiable form permitting the physical or online contacting of a specific individual[.]"[21]

24. Because the DHS has already "beg[u]n to develop" the media monitoring tools and platform,[22] the DHS was required—and is still required—to conduct and publish an applicable PIA.[23]

25. The DHS's media influencer database will include personally identifiable information about "journalists, editors, correspondents, social media influencers, [and] bloggers."[24]

26. The DHS's media influencer database therefore constitutes both a "develop[ment] or procur[ement of] information technology that collects, maintains, or disseminates information that is in an identifiable form" and a "a new collection of information that . . . includes [] information in an identifiable form permitting the physical or online contacting of a specific individual[.]"

[21] E-Government Act, *supra* note 7, at § 208(b)(1).
[22] *OMB E-Government Act Guidance* at 5.
[23] E-Government Act, *supra* note 7, at § 208(b)(1).
[24] *Id.*

27. Because the DHS has already "beg[u]n to develop" the media influencer database,[25] the DHS was required—and is still required—to conduct and publish an applicable PIA.[26]

28. The DHS has not published a Privacy Impact Assessment for any aspect of Media Monitoring Services, including both the media monitoring tools and platform and the media influencer database.[27]

29. On information and belief, the DHS has not conducted a Privacy Impact Assessment for any aspect of Media Monitoring Services, including both the media monitoring tools and platform and the media influencer database.

EPIC's FOIA Request

30. On April 13, 2018, EPIC submitted a FOIA request ("EPIC's FOIA Request") to the U.S. Department of Homeland Security ("DHS"). Ex. 2. The FOIA request was transferred to DHS's National Protection and Programs Directorate ("NPPD") for a direct response. Ex. 3.

31. EPIC's FOIA Request sought the NPPD's Privacy Impact Assessment for "Media Monitoring Services" and related records. Specifically, EPIC sought:

1) The required Privacy Impact Assessment conducted for the April 3, 2018 solicitation for "Media Monitoring Services,"

2) Any associated agency records including but not limited to policy guidelines, memoranda, email communications, and Privacy Threshold Analysis related to "Media Monitoring Services,"

3) All awarded contracts for "Media Monitoring Services."

Ex. 2 at 1.

---

[25] *OMB E-Government Act Guidance*, *supra* note 11, at 5.
[26] E-Government Act, *supra* note 7, at § 208(b)(1).
[27] *See* U.S. Dep't Homeland Sec., *Privacy Documents for the National Protection and Programs Directorate (NPPD)* (Dec. 7, 2016), https://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd.

32. EPIC sought "news media" fee status under 5 U.S.C. § 552(4)(A)(ii)(II) and a waiver of all duplication fees under 5 U.S.C. § 552(a)(4)(A)(iii). Ex. 2 at 5.

33. EPIC also sought expedited processing under 5 U.S.C. § 552(a)(6)(E)(v)(II). Ex. 2 at 4.

34. In an e-mail dated April 13, 2018, the NPPD FOIA Office acknowledged receipt of EPIC's FOIA Request. Ex 3. The request was assigned reference number 2018-NPFO-00373. The NPPD granted EPIC's request for expedited treatment and a request for a fee waiver.

35. Today is the 48th day since DHS component NPPD received EPIC's FOIA Request.

36. The DHS has failed to make a determination regarding EPIC's FOIA Request within the time period required by 5 U.S.C. § 552(a)(6)(A)(i).

37. There is substantial public interest and significant urgency in the release of the requested records. Little information is publicly known about the extent or purpose of the agency's planned media monitoring tools, other than what is described in the SOW. The six-page SOW contains no Privacy Impact Assessment and makes no reference to any privacy safeguards.[28]

Count I

Violation of FOIA: Failure to Comply with Statutory Deadlines

38. Plaintiff asserts and incorporates by reference paragraphs 1–37.

39. Defendant DHS has failed to make a determination regarding EPIC's request for 48 days and has thus violated the deadlines under 5 U.S.C. § 552(a)(6)(A)(i) and 5 U.S.C. § (a)(6)(E)(ii)(I).

40. Plaintiff has constructively exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

[28] *See Draft Statement of Work*, *supra* note 18.

Count II

Violation of FOIA: Unlawful Withholding of Agency Records

41. Plaintiff asserts and incorporates by reference paragraphs 1–37.

42. Defendant DHS has wrongfully withheld agency records requested by Plaintiff.

43. Plaintiff has exhausted all applicable administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

44. Plaintiff is entitled to injunctive relief with respect to the release and disclosure of the requested records.

Count III

Violation of APA: Unlawful Agency Action

45. Plaintiff asserts and incorporates by reference paragraphs 1–37.

46. Defendant DHS's solicitation of Media Monitoring Services prior to creating, reviewing, and/or publishing a Privacy Impact Assessment, 44 U.S.C. § 3501 note, is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law under 5 U.S.C. § 706(2)(a) and short of statutory right under 5 U.S.C. § 706(2)(c).

47. Defendant's solicitation of "Media Monitoring Services" and its decision to develop those services are final agency actions within the meaning of 5 U.S.C. § 704.

48. Plaintiff is adversely affected, aggrieved, and injured in fact by Defendant's actions. By failing to produce and disclose a Privacy Impact Assessment for Media Monitoring Services, Defendant has frustrated Plaintiff's longstanding mission to educate the public about the privacy implications of government databases that contain personally identifiable information.

49. Plaintiff has exhausted all applicable administrative remedies.

Count IV

Violation of APA: Agency Action Unlawful Withheld

50. Plaintiff asserts and incorporates by reference paragraphs 1–37.

51. Defendant DHS has failed to create, review, and/or publish a Privacy Impact Assessment for Defendant's solicitation for Media Monitoring Services, as required by 44 U.S.C. § 3501.

52. Defendant's failure to take these steps constitutes agency action unlawfully withheld or unreasonably delayed in violation of 5 U.S.C. § 706(1).

53. Plaintiff is adversely affected, aggrieved, and injured in fact by Defendant's inaction. By failing to produce and disclose a Privacy Impact Assessment for Media Monitoring Services, Defendant has frustrated Plaintiff's longstanding mission to educate the public about the privacy implications of government databases that contain personally identifiable information.

54. Plaintiff has exhausted all applicable administrative remedies.

Count V

Claim for Declaratory Relief

55. Plaintiff asserts and incorporates by reference paragraphs 1–37.

56. Plaintiff is entitled under 28 U.S.C. § 2201(a) to a declaration of the rights and other legal relations of the parties with respect to the claims set forth in Counts I-IV.

Requested Relief

WHEREFORE, Plaintiff requests this Court:

A. Order Defendant to immediately conduct a reasonable search for all responsive records;

B. Order Defendant to disclose promptly to Plaintiff all responsive, non-exempt records;

C. Order Defendant to produce the records sought without the assessment of search fees;

D. Order Defendant to suspend the development and use of Media Monitoring Services pending the completion and publication of a Privacy Impact Assessment;

E. Order Defendant to conduct, review, and publish a Privacy Impact Assessment for Media Monitoring Services;

F. Award EPIC costs and reasonable attorney's fees incurred in this action; and

G. Grant such other relief as the Court may deem just and proper.

Respectfully Submitted,

/s/ Alan Butler
ALAN BUTLER, D.C. Bar # 1012128
EPIC Senior Counsel

MARC ROTENBERG, D.C. Bar # 422825
EPIC President and Executive Director

JOHN DAVISSON, D.C. Bar #1531914[29]
EPIC Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: May 30, 2018

[29] Scheduled to be sworn into the bar of this Court on June 4, 2018.