IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER 1718 Connecticut Avenue, NW Suite 200 Washington, DC 20009, Plaintiff, v. U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT 500 12th Street SW Washington, DC 20536, Defendant.	Civ. Action No. 17-2684

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, for injunctive and other appropriate relief, seeking the release of agency records requested by the Plaintiff Electronic Privacy Information Center ("EPIC") from Defendant Immigration and Customs Enforcement ("ICE"), a component of the U.S. Department of Homeland Security ("DHS").

2. EPIC challenges ICE's failure to make a timely response to EPIC's Freedom of Information Act request ("EPIC's FOIA Request") for records about ICE's contracts and other information related to the FALCON systems and the Investigative Case Management ("ICM") system.

Jurisdiction and Venue

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

4. Venue is proper in this district under 5 U.S.C. § 552(a)(4)(B).

Parties

5. Plaintiff EPIC is a nonprofit organization, incorporated in Washington, DC, established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities. EPIC's Advisory Board includes distinguished experts in law, technology, public policy, and cybersecurity. EPIC routinely disseminates information to the public through the EPIC website, the EPIC Alert, and various other news organizations. EPIC is a representative of the news media. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

6. Defendant ICE is a component of the DHS, which is a federal agency within the meaning of 5 U.S.C. § 552(f)(1), and is headquartered in Washington, D.C.

Facts

7. ICE is one of the largest law enforcement agencies in the United States. The agency enforces federal border laws and conducts homeland security investigations, operating both at the U.S. border and the interior.[1]

8. In conducting these investigations, ICE has contracted with Palantir Technologies, Inc. ("Palantir"), a secretive data mining firm, to establish and manage key information systems such

[1] U.S. Immigration and Customs Enforcement, *Who We Are*, https://www.ice.gov/about (last visited Dec. 14, 2017).

as the FALCON and ICM systems that are designed to make determinations about specific, identifiable individuals.

9. Palantir is a data-mining firm that includes the CIA's venture capital arm, In-Q-Tel, as an early investor.[2] The company's work with government agencies has been a source of ongoing controversy.[3]

10. Palantir takes massive amounts of data on individuals and applying, secretive, proprietary techniques, makes determinations about their fitness for employment, travel, and whether they should be targeted for further investigations.[4] Palantir plays a growing role in the field of "automated policing."[5]

11. Palantir has established controversial databases that secretly and indiscriminately collect data on the public.[6]

12. Palantir's products provides the basis for deportation determinations.[7]

13. Palantir's "big data" systems raise far-reaching privacy and civil liberties risks.[8]

---

[2] IN-Q-TEL, *Palantir Technologies*, https://www.iqt.org/palantir-technologies/ (last visited Dec. 15, 2017).

[3] *See e.g.*, Sam Biddle, *How Peter Thiel's Palantir Helped The NSA Spy On The Whole World*, The Intercept (Feb. 22, 2017), https://theintercept.com/2017/02/22/how-peter-thiels-palantir-helped-the-nsa-spy-on-the-whole-world/.

[4] *See* Jacques Peretti, *Palantir: the 'special ops' Tech Giant That Wields As Much Real-World Power As Google*, The Guardian (July 30, 2017), https://www.theguardian.com/world/2017/jul/30/palantir-peter-thiel-cia-data-crime-police; Ashlee Vance and Brad Stone, *Palantir, the War on Terror's Secret Weapon*, Bloomberg (Nov. 22, 2011), https://www.bloomberg.com/news/articles/2011-11-22/palantir-the-war-on-terrors-secret-weapon.

[5] Mark Harris, *How Peter Thiel's Secretive Data Company Pushed Into Policing*, Wired (Aug. 9, 2017), https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/.

[6] *See, e.g.*, Jeff Blagdon, *Palantir Is Helping California Police Develop Controversial License Plate Database*, The Verge (June 29, 2013), https://www.theverge.com/2013/6/29/4478748/california-license-plate-reader-database-palantir.

[7] Spencer Woodman, *Palantir Provides the Engine For Donald Trump's Deportation Machine*, The Intercept (Mar. 2, 2017), https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/.

14. Through the FALCON and ICM databases, Palantir software allows ICE to secretly analyze and assess massive amounts of personal data across numerous federal databases containing information on individuals not suspected of any wrongdoing.[9]

15. The Palantir systems, as deployed by agencies of the U.S. government, raise far-reaching questions about compliance with the Privacy Act of 1974 and Section 208 of the E-Government Act of 2002, which requires a detailed Privacy Impact Assessment for records systems in the federal government containing personal information.

FALCON Systems

16. The FALCON systems are based on Palantir's "Gotham" platform, a proprietary software technique that analyzes complex data sets, containing detailed personal information, concerning individuals.[10]

17. FALCON serves as ICE's primary data storage and analysis system.[11] There are several FALCON modules, including FALCON Data Analysis and Research for Trade Transparency ("DARTTS"), FALCON Search and Analysis system (FALCON-SA), and the FALCON Roadrunner System.

18. The FALCON Systems include sensitive, personal information that is gathered from various sources including other DHS databases, databases from other agencies, and databases

---

[8] Quentin Hardy, *The Risk to Civil Liberties of Fighting Crime With Big Data*, N.Y. Times (Nov. 6, 2016), https://www.nytimes.com/2016/11/07/technology/the-risk-to-civil-liberties-of-fighting-crime-with-big-data.html.

[9] *See* Spencer Woodman, *Palantir Enables Immigration Agents to Access Information From the CIA*, The Intercept (Mar. 17, 2017), https://theintercept.com/2017/03/17/palantir-enables-immigration-agents-to-access-information-from-the-cia/.

[10] *Id.*

[11] *Id.*

from state, local, as well as foreign entities.[12] The FALCON system also incorporates data from public record systems, such as current address, geospatial data, and civil litigations.[13]

19. FALCON records can include name, date of birth, place of birth, Social Security number, passport information, citizenship, nationality, bank account and transaction numbers, call transactions and subscriber information, and social media information.

20. On May 4, 2017, ICE published a System of Records Notice for FALCON that included a broad set of "routine uses" that allows information in the system to be disclosed numerous entities including federal, state, and local agencies as well as the news media and other third parties.[14]

21. On May 4, 2017, ICE published a Notice of Proposed Rulemaking that sought to exempt FALCON from several Privacy Act safeguards including the requirement to maintain accurate, relevant, timely, and complete records.[15]

22. Beyond a few Privacy Impact Assessments, the Systems of Record Notice, and a few other documents providing general descriptions about the FALCON system, little is known by the public, particularly with respect to the use of the data in the system, mechanisms for oversight and accountability, or the broader relationship between ICE and Palantir.

Investigative Case Management system

23. The ICM system is a Palantir-based system that replaces ICE's legacy TECS system.

[12] U.S. Department of Homeland Security, *Privacy Impact Assessment Update for the FALCON Search & Analysis System DHS/ICE/PIA-032(a)* (Jan. 16, 2014), https://www.dhs.gov/sites/default/files/publications/privacy_pia_ice_falconsa_january2014.pdf.
[13] *Id.* at 10.
[14] 82 Fed. Reg. 20905, 20908 (May 4, 2017).
[15] 82 Fed. Reg. 20844, 20846 (May 4, 2017).

24. The ICM allows ICE to access various databases, containing personal information, including the FALCON system described above and Customs and Border Protection's Automated Targeting System ("ATS").[16]

25. The information contained in ICM includes biographical data such as name, date of birth, and Social Security number; and descriptive data like eye color, hair color, height, weight, and unique physical characteristics (e.g. tattoos).[17] The ICM also includes financial data, location-related data, license plate reader data, and telecommunications data.[18]

26. ICE disseminates information from the ICM to federal, state, local, and foreign law enforcement agencies. The information is also disseminated to "fusion centers, FBI Joint Terrorism Task Forces, and international organizations such as INTERPOL."[19]

27. According to the Privacy Impact Assessment, ICM is covered by the DHS/ICE-009 External Investigations System of Records Notice.[20]

28. The DHS/ICE-009 External Investigations System of Records Notice creates broad "routine uses" for the records in the covered databases.[21]

29. A final rule for the External Investigations System of Records exempts ICM from several Privacy Act safeguards including the requirement to maintain accurate, relevant, timely, and complete records.[22]

---

[16] U.S. Department of Homeland Security, *Privacy Impact Assessment for ICE Investigative Case Management DHS/ICE/PIA-045*, 16-17 (June 16, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.
[17] *Id.* at 10.
[18] *Id.* at 11.
[19] *Id.* at 29-30.
[20] *Id.* at 8.
[21] 75 Fed. Reg. 404, 408-09 (Jan. 5, 2010) (updating and reissuing the systems of records notice but leaving in place previous Privacy Act exemptions), https://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31269.pdf.

30. In the DHS 2018 Budget in Brief, the DHS sought $20.3 million in FY 2018 funding for ICM.[23]

31. Both the FALCON and ICM systems pose significant threats to privacy. Both systems collect a significant amount of personal information, both are exempt from many of the protections of the Privacy Act, and both disseminate personal data broadly among other government and law enforcement agencies—any of which could use the information as a reason to subject an individual for scrutiny.

32. Both the FALCON and ICM systems contain extensive data on U.S. citizens, lawful personal residents, and those covered under the recent amendments to the Privacy Act covering EU residents.

EPIC's FOIA Request

33. On August 14, 2017, EPIC submitted a FOIA Request to ICE's Freedom of Information Act Office via email.

34. EPIC's FOIA Request sought records pertaining to the FALCON and Investigative Case Management systems. Specifically, EPIC sought:

> (1) Any records, contracts, or other communications with Palantir regarding the FALCON program and the ICM system, including but not limited to documents concerning contract IDs HSCETC-13-F-00030, HSCETC-15-C-00001, and HSCETC-14-C-00002.
>
> (2) Any training materials, presentations, manuals, or publications associated with training provided to those who use the FALCON system, including training from Palantir and training/policies specific to the ad hoc addition of data into the sytem.
>
> (3) Reports and analysis of the FALCON system, including but not limited to reports related to effectiveness of the system, compliance testing, and audits.

---

[22] 74 Fed. Reg. 45081 (Aug. 20, 2009), https://www.gpo.gov/fdsys/pkg/FR-2009-08-31/html/E9-20762.htm.

[23] *FY 2018 Budget in Brief,* Dep't of Homeland Sec. at 37, https://www.dhs.gov/sites/default/files/publications/DHS%20FY18%20BIB%20Final.pdf.

(3) Reports and analysis of the ICM system, including the results of the tests described in the ICE TECS Modernization Master Plan.[24]

(4) Memoranda of Agreement, Memoranda of Understanding (MOUs), or similar agreements between ICE and federal, state, or local agencies, as well as private companies—including any addenda to these agreements—regarding the collection, use, dissemination, disclosure, or retention of data in the ICM system.

(5) All documents related to ICM user training courses, including but not limited to the course on privacy.

(6) Any audit logs or audit reports for the ICM system.

(7) Any contracts between ICE and commercial data providers concerning the ICM system.

(8) Any policies and procedures related to the ICM system, including but not limited to case management, disclosure, and dissemination procedures.

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

36. In an email dated August 23, 2017, the ICE FOIA Office acknowledge receipt of EPIC's FOIA request.

37. EPIC has received no further communication about EPIC's FOIA request from ICE.

38. The status of EPIC's FOIA request per DHS' "Check Status Request" page listed the status on November 1, 2017 as "Request for Docs Sent." The same status was listed as of December 14, 2017.

<u>EPIC's Constructive Exhaustion of Administrative Remedies</u>

39. Today is the 123rd day since the ICE received EPIC's FOIA Request.

40. ICE 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).

41. ICE's failure to make a determination within the statutory time limit violates the FOIA.

---

[24] DHS Office of the Chief Information Officer, *ICE TECS Modernization Program Test and Evaluation Master Plan (TEMP)* (Apr. 2, 2014).

42. EPIC has constructively exhausted all administrative remedies under 5 U.S.C. § 552(a)(6)(C)(i).

Count I

Violation of FOIA: Failure to Comply With Statutory Deadlines

32. Plaintiff asserts and incorporates by reference paragraphs 1-42.

33. Defendant ICE has failed to make a determination regarding EPIC's FOIA Request within twenty days, and has thus violated the deadline under 5 U.S.C. § 552 (a)(6)(A)(i) and 6 C.F.R. § 5.5.

34. Plaintiff has constructively exhausted all applicable administrative remedies with respect to EPIC's FOIA Request. 5 U.S.C. § 552(a)(6)(C)(i).

Count II

Violation of FOIA: Unlawful Withholding of Agency Records

35. Plaintiff asserts and incorporates by reference paragraphs 1-42.

36. Defendant has wrongfully withheld agency records requested by Plaintiff.

37. Plaintiff has constructively exhausted applicable administrative remedies with respect to Defendant's withholding of the requested records.

38. EPIC has exhausted the applicable administrative remedies with respect to EPIC's FOIA Request. 5 U.S.C. § 552(a)(6)(C)(i).

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

Requested Relief

WHEREFORE, Plaintiff prays that this Court:

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

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

C. Order Defendant to provide an affidavit detailing the agency's search methodology including search terms and the type of search performed, and confirming that all files likely to contain responsive materials were searched;

D. Order Defendant to produce a *Vaughn* Index identifying any records or portions of records withheld, if such records exist, stating the statutory exemption claimed and explaining how disclosure would damage the interests protected by the claimed exemption;

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

F. Order Defendant to grant EPIC's request for fee waiver.

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

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

Respectfully submitted,

By: __*s/ Jeramie D. Scott*____
Jeramie D. Scott, D.C. Bar # 1025909
EPIC National Security Counsel

Marc Rotenberg, D.C. Bar# 422825
EPIC President and Executive Director

Alan Butler, D. C. Bar# 1012128
EPIC Senior 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: December 15, 2017