epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

VIA E-MAIL

August 14, 2017

Catrina Pavlik-Keenan
FOIA Officer
United States Immigration and Customs Enforcement
Freedom of Information Act Office
500 12th Street, SW, Stop 5009
Washington, D.C. 20536-5009
ice-foia@dhs.gov

Dear Ms. Pavlik-Keenan,

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. 552(a)(3), and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to United States Immigration and Customs Enforcement ("ICE").

ICE has contracted with Palantir to build and/or maintain information systems that include vast amounts of information on individuals. These databases include the FALCON systems and the Investigative Case Management ("ICM") system.[1] EPIC seeks ICE's contracts, training materials, reports and analysis, agreements, policies and procedures, and other documents related to the purchase and use of theses systems.

Documents Requested

(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.

[1] 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/.

(3) Reports and analysis of the ICM system, including the results of the tests described in the ICE TECS Modernization Master Plan.[2]

(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 dissemiantion procedures.

Background

ICE is one of the largest law enforcement organizations in the United States. The agency enforces federal border laws and conducts homeland security investigations, operating both at the US border and the interior.[3] In conducting these investigations, ICE has partnered with Palantir Technologies, Inc. ("Palantir") to develop key information systems like the FALCON and ICM systems. While Privacy Impact Assessments ("PIAs") have been published related to these systems, many questions remain concerning their operations, including whether meaningful constraints exist, are communicated, and are enforced for the collection, use, disclosure, and retention of data.

FALCON Systems

FALCON is based on Palantir's Gotham platform, a proprietary software product which allows users to search, visualize, and analyize complex data sets.[4] FALCON serves as ICE's primary data storage and analysis system[5] and there are several FALCON modules, including FALCON Data Analysis and Research for Trade Transparency System (DARTTS), FALCON Search and Analysis System (SA), and FALCON-Roadrunnder System.

---

[2] DHS Office of the Chief Information Officer, *ICE TECS Modernization Program Test and Evaluation Master Plan (TEMP)* (Apr. 2, 2014).
[3] *Who We Are*, Ice.gov, https://www.ice.gov/about.
[4] 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/.
[5] *Id.*

FALCON-DARTTS looks at anomalies in data related to trade based crimes, including money laundering, smuggling, and other import-export crimes.[6] The data analyzed includes trade, financial, and law enforcement data provided by US and foreign governments. Investigators can upload ad hoc data from other sources, including "financial institutions, transportation companies, manufacturers, customs brokers, state, local, and foreign governments, free trade zones, and port authorities, and may include financial records, business records, trade transaction records, and transportation records."[7]

FALCON-SA is used "to search, analyze, and visualize volumes of existing information."[8] It aggregates, analyzes, and visualizes data from various, disparate sources. FALCON-Roadrunner is a module within the existing FALCON environment that conducts trend analysis and generates investigative leads related to illegal trafficking of weapons and technology.

Little is known by the public about the effectiveness of the FALCON system, the extent of training for the system, the constraints on dissemination of the data in FALCON, and the mechanisms in place for proper oversight and accountability.

Investigative Case Management (ICM) system

The Investigative Case Management (ICM) system is the modernization of ICE's legacy TECS[9] system.[10] A primary motivation for the modernization project was to enable ICE to more easily link investigative records within and between departments.[11] The ICM system includes the ICM application, which provides case management capabilities, as well as three additional capabilities: "1) an Interface Hub to control the movement of information between ICM and external information repositories; 2) the HSI Data Warehouse to store case information for the purpose of facilitating information sharing and reporting; and 3) the TLS application (and its interface with Pen-Link), which will store case-related telecommunications information obtained via subpoena or other means."[12]

---

[6] U.S. Department of Homeland Security 2016 Data Mining Report to Congress, 38-39 (Apr. 2017).
[7] *Id.* at 40.
[8] U.S. Department of Homeland Security, FALCON Search & Analysis System PIA, DHS/ICE/PIA-032(b) FALCON-SA (Oct 11, 2016), 4.
[9] TECS is not an acronym; it is an "updated and modified version of the former Treasury Enforcement Communications System." DHS/CBP/PIA-009 – TECS System: CBP Primary and Secondary Processing, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf.
[10] DHS/ICE/PIA-045 – ICE Investigative Case Management (ICM) at 3, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.
[11] *Id*. at 2.
[12] *Id*. at 1.

In its 2018 Budget in Brief, DHS listed $20.3 million in FY 2018 funding for ICM (also referred to as the TECS Modernization Project).[13] DHS stated that ICM had 11,000 HSI users by June 27, 2016, that ICM would be at full operational capacity in FY 2018, and that it would enter the Operations and Maintenance phase in FY 2019.[14] There are contracts between ICE and Palantir for the ICM system worth over $41 million.[15]

The PIA for ICM makes clear that audit logs exist. The PIA states that "audit logs capture user activity including, but not limited to, uploading records or data, extracting information from the system, resolving entities, searches, and viewing records."[16] The PIA further states that "[t]he audit logs account for ICM transactions, as well as information sharing activity that occurs through the Interface Hub and queries of the HSI Data Warehouse."[17] These audit and log files are stored "in a separate data repository" where they are retained for 7 years.[18] According to the PIA, ICM users are presented with a "warning banner" upon logging in "advising the user that he or she has no expectation of privacy with respect to any actions taken while in the system."[19]

The PIA also states that "ICM users must take and pass an ICM user training course that includes in-depth privacy training" and that they must "recertify" their ICM training "every year" or else be denied access to the system by an automated "guard."[20] All ICE employees are also required to take an annual DHS privacy training and ICE Information Assurance Awareness Training.[21]

Additionally, the PIA mentions contracts between commercial data providers and ICE, who are required to "maintain reasonable physical, technical, and administrative safeguards to appropriately protect the shared information," inform ICE of any confirmed or potential unauthorized access to the data, and refrain from re-disclosing ICE information.[22] The PIA also references policies regarding case management and disclosure procedures.[23]

---

[13] *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 .

[14] *Id*. at 37.

[15] ICE Investigative Case Management System, FBO.org, https://www.fbo.gov/index?s=opportunity&mode=form&id=36fb3b697a2ccb4ec7084b4e0ec6cdb9&tab=core&_cview=1.

[16] DHS/ICE/PIA-045 – ICE Investigative Case Management (ICM) at 26, https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-icm-june2016.pdf.

[17] *Id*. at 34-35.

[18] *Id*. at 34.

[19] *Id*. at 26.

[20] *Id*. at 35.

[21] *Id*.

[22] *Id* at 31.

[23] *Id*. at 20, 21, 24, 29, 30, 31

Finally, the PIA mentions the existence of Memoranda of Agreement[24] and Memoranda of Understanding (MOUs) for sharing information, as well as addenda to these MOUs.[25]

Previous documents released to the public reference documents of interest to the public. The Statement of Objectives references the implementation of the Test and Evaluation Master Plan (TEMP), and a training and educational plan.[26] The ICE TECS Modernization Master Plan describes various tests that were to be conducted with respect to the ICM program, including functional testing, interoperability testing, performance testing, Section 508 Compliance testing, User Acceptance testing, Security Authorization testing, and an Operational Test and Evaluation.[27]

Both the FALCON and ICM systems compile great quantities of sensitive personal information that are used, retained, and disseminated by ICE. These systems, which include individuals not suspected of criminal activity, implicate core privacy interests,.

Request for "News Media" Fee Status and Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. Dep't of Def.*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on EPIC's status as a "news media" requester, EPIC is entitled to receive the requested record with only duplication fees assessed. 5 U.S.C. § 552(a)(4)(A)(ii)(II); 6 C.F.R. § 5.11(d)(1).

Further, any duplication fees should also be waived because (1) disclosure of the requested information is "in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government" and (2) disclosure is "not primarily in the commercial interest of the requester." 5 U.S.C. §552(a)(4)(A)(iii); 6 C.F.R. § 5.11(k). This FOIA request meets all of ICE's considerations for granting a fee waiver. 6 C.F.R. § 5.11(k)(2-3).

First, EPIC's request satisfies all four considerations ICE evaluates to determine whether the first requirement for fee waiver – that disclosure "in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government" - is met. § 5.11(k)(2). ICE considers: (i) the "subject of the

[24] *Id*. at 15.
[25] *Id*. at 29, 36.
[26] ICE Office of Chief Information Officer and Homeland Sec. Investigations (HSI), *ICE ICM Statement of Objectives Version 1.0*, Dep't of Homeland Sec. (May 1, 2014) at 6-7, https://www.documentcloud.org/documents/3478481-ICE-ICM-Statement-of-Objectives.html.
[27] ICE Office of the Chief Information Officer, *ICE TECS Modernization Master Plan Version 2.0*, Dep't of Homeland Sec. (Apr. 12, 2014), at 5-6, https://theintercept.com/document/2017/03/02/ice-tecs-modernization-master-plan/.

request must concern identifiable operations or activities of the federal government, with a connection that is direct and clear, not remote or attenuated"; (ii) disclosure "must be meaningfully informative about government operations or activities in order to 'likely to contribute' to an increased public understanding of those operations or activities"; (iii) "disclosure must contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester" and it "shall be presumed that a representative of the news media will satisfy this consideration"; and/or (iv) the "public's understanding of the subject in question must be enhanced by the disclosure to a significant extent." § 5.11(k)(2)(i-iv).

To the first consideration, this request "concern[s] identifiable operations or activities of the federal government, with a connection that is direct and clear, not remote or attenuated." § 5.11(k)(2)(i). The subject of the request is self-evidently a federal activity. The request involves ICE's use of large-scale databases and the technology the agency uses to analyze these databases to carry out law enforcement functions.

To the second consideration, disclosure of the requested information will "be meaningfully informative about government operations or activities." § 5.11(k)(2)(ii). Most citizens are not aware of the amount of information ICE collects in the FALCON and ICM systems, the capabilities the agency has to anaylyze these systems, and the extent of access to this information by local and state agencies as well as other federal agencies. While many individuals may have an idea that the government collects and analyze data, they are likely unaware of the extent of this data collection, that information about individuals not suspected of criminal activity are in these databases, and the extent of that this information is disclosed to other entities. The disclosure of training material, policies and procedures, agreements, and other documents by ICE will provide a better understanding of government operations at the border.

To the third consideration, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in the subject, as opposed to the individual understanding of the requester," because, as stated in the relevant FOIA regulation, it "shall be presumed that a representative of the news media will satisfy this consideration." § 5.11(k)(2)(iii).

To the fourth consideration, the "public's understanding of the subject in question" will be "enhanced by the disclosure to a significant extent." § 5.11(k)(2)(iv). As described in this request, despite the release of related Privacy Impact Assessments, the public still lacks an understanding of how these systems are used, the actual policies and procedures in place, the extent of the disclosure of the information in the data systems, and the effectiveness of these data systems. The requested information will, therefore, enhance the public's understanding of these systems to a "significant extent." *Id*.

Second, EPIC's request also satisfies both considerations ICE evaluates to determine whether the second requirement for fee waiver – that disclosure is "not primarily in the commercial interest of the requester" - is met. § 5.11(k)(3). ICE

considers: (i) whether there is "any commercial interest of the requester… that would be furthered by the requested disclosure"; and/or (ii) whether "the public interest is greater than any identified commercial interest in disclosure." § 5.11(k)(3)(i-ii).

To the first consideration, EPIC has no "commercial interest . . . that would be furthered by the requested disclosure." § 5.11(k)(3)(i). EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[28]

To the second consideration,"the public interest is greater than any identified commercial interest in disclosure" because, as provided in the FOIA regulations, "[c]omponents ordinarily shall presume that where a news media requester has satisfied the public interest standard, the public interest will be the interest primarily served by disclosure to that requester." § 5.11(k)(3)(ii). As already described in detail above, EPIC is both news media requester and satisfies the public interest standard.

For these reasons, a full fee waiver should be granted.

Conclusion

Thank you for your consideration of this request. I anticipate your determination on our request within 20 calendar days. 5 U.S.C. § 552(a)(6)(A)(i).

For questions regarding this request I can be contacted at 202-483-1140 x108 or FOIA@epic.org.

Respectfully submitted,

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC National Security Counsel

[28] *About EPIC*, http://epic.org/epic/about.html