epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

VIA EMAIL

Tammy Warner
Office of Counsel
U.S. Postal Inspection Service
475 L'Enfant Plaza SW, Room 3301
Washington, DC 202260

May 21, 2021

RE: Freedom of Information Act Request

Dear Ms. Warner,

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, 39 C.F.R. § 265.1 et seq., and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the U.S. Postal Inspection Service ("USPIS").

EPIC seeks the U.S. Postal Service's Privacy Impact Assessment(s) ("PIA") and Privacy Threshold Assessment(s) ("PTA") for the Internet Covert Operations Program ("iCOP"). Please provide all documents in searchable electronic format, preferably as searchable PDF files.

Documents Requested

1. The required Privacy Impact Assessment(s)/Business Impact Assessment(s) for the Internet Covert Operations Program ("iCOP") and/or facial recognition and social media monitoring systems used by iCOP;

2. The Privacy Threshold Assessment(s) for the Internet Covert Operations Program and/or facial recognition and social media monitoring systems used by iCOP;

3. In the event that there is no finalized PIA/BIA as described in Item 1, please search for any draft Privacy Impact Assessment(s)/Business Impact Assessment(s) related to the iCOP program and/or facial recognition and social media monitoring systems used by iCOP. If there is a finalized PIA/BIA covering the above systems, do not perform this search.

Background

The United States Postal Inspection Service runs a "covert operations program" used to monitor social media for perceived threats, including protests. First disclosed to the public on April

21, 2021, the Internet Covert Operations Program ("iCOP") has existed since at least 2018.[1] iCOP analysts "assume fake identities online, use sophisticated intelligence tools and employ facial recognition software" including Clearview AI's facial recognition program.[2] Clearview AI's product comprises a powerful facial recognition algorithm and a dataset of over 3 billion images scraped from social media platforms.[3] USPIS's other surveillance technology includes Zignal Labs software capable of tracking social media "narratives" back to the individual who initiated the "narrative," identifying specific "influences."[4] The iCOP program also has access to Nfusion, a program for creating anonymous emails and social media accounts.[5]

Although the Postal Service claims that iCOP is intended to protect postal workers, the program monitored protesters during the Black Lives Matter uprising of 2020 and anti-lockdown protests in March 2021.[6] The Postal Service disseminated information about the protests to the Department of Homeland Security, local police, and fusion centers.[7]

As of May 19, 2021 there is no publicly available Privacy Impact Assessment or Privacy Threshold Assessment for the iCOP program listed on the Postal Service website.[8]

PIA Requirement

Under Section 208 of the E-Government Act, a federal agency (including the Postal Service[9]) is required to undertake a Privacy Impact Assessment ("PIA") when the agency "develop[s] or procur[es] information technology that collects, maintains, or disseminates information that is in an identifiable form," and (2) when the agency "initiat[es] a new collection of information" that

---

[1] Jana Winter, *The Postal Service is running a 'covert operations program' that monitors Americans' social media posts*, Yahoo! News (Apr. 21, 2021), https://news.yahoo.com/the-postal-service-is-running-a-running-a-covert-operations-program-that-monitors-americans-social-media-posts-160022919.html?soc_src=social-sh&soc_trk=tw&tsrc=twtr, Jana Winter, *Facial recognition, fake identities and digital surveillance tools: Inside the post office's covert internet operations program*, Yahoo! News (May 18, 2021), https://news.yahoo.com/facial-recognition-fake-identities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program-214234762.html.

[2] Jana Winter, *Facial recognition, fake identities and digital surveillance tools: Inside the post office's covert internet operations program*, Yahoo! News (May 18, 2021), https://news.yahoo.com/facial-recognition-fake-identities-and-digital-surveillance-tools-inside-the-post-offices-covert-internet-operations-program-214234762.html.

[3] *Id*.

[4] *Id.*; Zignal Enterprise, Zignal Labs (2021), https://zignallabs.com/products/zignal-enterprise/.

[5] Winter, *Facial recognition, fake identities and digital surveillance tools: Inside the post office's covert internet operations program, supra*.

[6] Coral Murphy Marcos, *Outcry over US Postal Service reportedly tracking social media posts*, Guardian (Apr. 23, 2021), https://www.theguardian.com/business/2021/apr/23/usps-covert-program-postal-service-social-media.

[7] *Id.*

[8] *See*: List of Privacy Impact Assessments/Business Impact Assessments, United States Postal Service (2021), https://about.usps.com/who-we-are/privacy-policy/privacy-impact-assessments.htm.

[9] *Compare* 44 U.S.C. § 3502(1) (defining "agency" for the purposes of the Paperwork Reduction Act and E-Government Act to include any "establishment in the executive branch of the Government"); *with* 39 U.S.C. § 201 (forming the United States Postal Service as an "establishment of the executive branch of the Government").

"includes any information in an identifiable form."[10] This identifiable information, referred to as personally identifiable information ("PII"), includes any information in a program or system that allows the identity of an individual to be directly or indirectly inferred. Here the Postal Service iCOP program collects social media information, including usernames and profiles associated with individual persons. The Office of Management and Budget ("OMB"), for the purposes of the E-Government Act, follows the Clinger-Cohen Act definition of information technology: "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."[11]

The OMB further states: "Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection." PIAs at the "IT development stage":

1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;
3. 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.[12]

The Postal Service has adopted policies to comply with the E-Government Act's PIA provisions.[13] "This includes requirements to conduct privacy impact assessments, to post privacy policies on Web sites used by the public, and to translate privacy policies into a standardized machine–readable format."[14] The Postal Service conducts a PIA/BIA "for all IT systems, including

[10] E-Government Act of 2002, Pub. L. No. 107-347, § 208 (b)(1)(A)(i)-(ii), 116 Stat. 2899, 2921–22 (2002), 44 U.S.C. § 3502 note.
[11] 40 U.S.C. § 11101(6) (2011) (emphasis added); *see also* Exec. Office of the President, Office of Mgmt and Budget, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), https://www.whitehouse.gov/wp- content/uploads/2017/11/203-M-03-22-OMB-Guidance-for-Implementing-the-Privacy-Provisions-of-the- E-Government-Act-of-2002-1.pdf [hereinafter OMB E-Government Act Guidance].
[12] OMB E-Government Act Guidance, *supra* at 5–6 (emphasis added).
[13] *Handbook AS-353, Guide to Privacy, the Freedom of Information Act, and Records Management, Postal Service*, USPS.com (Feb. 2019), https://about.usps.com/handbooks/as353/welcome.htm.
[14] *Id.*

those containing customer or employee information."[15] The Postal Service completes a PIA during the Information Resource Certification and Accreditation process.[16]

Request for Expedition and Fee Waiver

(a) Expedited Processing

EPIC is entitled to expedited processing of this request under the FOIA and the Postal Service's FOIA regulations. 5 U.S.C. § 552(a)(6)(E)(v)(II); 39 C.F.R. § 265.5(c)(1)(ii). Specifically, this request is entitled to expedited processing because, first, there is an "urgency to inform the public about an actual or alleged federal government activity," and, second, because the request is "made by a person who is primarily engaged in disseminating information." § 265(c)(1)(ii).

First, there is an "urgency to inform the public about an actual or alleged federal government activity." § 265(c)(1)(ii). The "actual...federal government activity" at issue is the Postal Service's operation of the iCOP program and use of several social media surveillance systems requiring a PIA.

Second, EPIC is an organization "primarily engaged in disseminating information." 39 C.F.R. § 265.5(c)(1)(ii). EPIC maintains a website, epic.org, for publishing information including that obtained through FOIA requests. As the Court explained in *EPIC v. DOD*, "EPIC satisfies the definition of 'representative of the news media'" entitling it to preferred fee status under FOIA. 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

In submitting this request for expedited processing, I certify that this explanation is true and correct to the best of my knowledge and belief. 39 C.F.R. § 265.5(c)(2); 5 U.S.C. § 552(a)(6)(E)(vi).

(b) Fee Waiver

EPIC is a "representative of the news media" for fee classification purposes. *EPIC v. DOD*, 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), 39 C.F.R. § 265.9(d)(1).

Further, any duplication fees should also be waived because (i) "disclosure of the requested information is in the public interest because it is likely to contribute to the public understanding of the operations or activities of the Postal Service" and (ii) "disclosure of the information is not primarily in the commercial interest" of EPIC, the requester. 39 C.F.R. § 265.9(j)(1); 5 U.S.C. § 552(a)(4)(A)(iii). EPIC's request satisfies this standard based on the Postal Service's considerations for granting a fee waiver. 39 C.F.R. § 265.9(j)(2)-(5).

---

[15] *Privacy Impact Assessments (PIA)*, USPS.com (2021), https://about.usps.com/who-we-are/privacy-policy/privacy-impact-assessments.htm.

[16] U.S. Postal Service, *Information Resource Business Impact Assessment* at 6 (July 27, 2011), https://about.usps.com/who-we-are/privacy-policy/business-impact-assessment-template.pdf.

(1) Disclosure of the requested information is likely to contribute to the public understanding of the operations or activities of the government.

First, disclosure of the requested documents is "in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the Postal Service". 39 C.F.R. § 265.9(j)(2)(i). The Postal Service evaluates these four factors to determine whether this requirement is met: (i) the "subject of the request must concern identifiable operations or activities of the Postal Service, 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 be '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 (iv) "[t]he public's understanding of the subject in question must be enhanced by the disclosure to a significant extent." 39 C.F.R. § 265.9(j)(2).

On the first factor, the subject of the request self-evidently concerns "identifiable operations or activities of the federal government" because the records requested relate to the actions of the USPIS Internet Covert Operations Program, operations performed by postal service investigative agents in the course of their employment.

On the second factor, disclosure would also be "meaningfully informative about" these operations or activities and is thus "'likely to contribute' to an increased understanding of government operations or activities" for two reasons. First, a PIA is required for information collection systems including facial recognition and social media monitoring under Section 208 of the E-Government Act. Whether the Postal Service complied with this requirement and did not publicize the resulting PIA, or failed to comply with the requirement altogether, will inform the public's understanding of how the iCOP program came to exist and whether privacy safeguards were implemented. Second, the contents of the required PIA, if one exists, will provide more information on the activities, capabilities, and attempts to mitigate privacy harms associated with the iCOP program. Currently the public information on iCOP is limited to news stories. Documents describing the program would meaningfully inform the public about iCOP and enhance the public's understanding.

On the third factor, disclosure will "contribute to the understanding of a reasonably broad audience of persons interested in the subject" because EPIC has "expertise in the subject area" and has the "ability and intention to effectively convey information to the public". 39 C.F.R. § 265.9(j)(2)(iii). EPIC is a non-profit that publishes information about privacy, technology, surveillance, and federal privacy protections. EPIC regularly comments on administrative agency rules to highlight the impact of surveillance technologies on individuals and vulnerable communities.[17] EPIC also routinely publishes information obtained through open government statutes on its website and receives other media coverage of those publications.[18] As a

[17] *See* EPIC, *EPIC Administrative Procedure Act (APA) Comments*, https://epic.org/apa/comments/.
[18] *See e.g.*, Mila Jasper, *Lawmakers, Experts, Industry Highlight Need for Ethics After Defense Commission Releases Final AI Report*, Nextgov, https://www.nextgov.com/emerging-tech/2021/03/lawmakers-experts-industry-highlight-need-ethics-after-defense-commission-releases-final-ai-report/172704/ (noting that EPIC

"representative of the news media," EPIC intends to publish the requested documents and has the capability to inform a "reasonably broad audience of persons" through the intended publication.

Finally, on the fourth factor, the public's understanding will "be enhanced by the disclosure to a significant extent". The existence or non-existence of documents required by statute will provide information not currently in the public record on the iCOP program. Furthermore, the contents of a PIA or PTA will shed light on the capabilities of the iCOP program and existence of privacy safeguards.

(2) Disclosure of the information is not primarily in the commercial interest of the requester.

Second, "[d]isclosure of the information is not primarily in the commercial interest" of EPIC. 39 C.F.R. § 265.9(j)(1)(ii). In determining whether this second requirement is met, the Postal Service evaluates the following two factors: (i) whether there is "a commercial interest . . . that would be furthered by the requested disclosure"; and/or (ii) whether "any identified commercial interest of the requester in disclosure outweighs the public interest." 39 C.F.R. § 265.9 (j)(3). The Postal Service, "ordinarily shall presume that if a news media requester has satisfied the public interest standard, the public interest is the primary interest served by the requested disclosure." *Id.*

On the first factor, there is not "a commercial interest of the requester . . . that would be furthered by the requested disclosure." 39 C.F.R. § 265.9 (j)(3)(i). EPIC has no commercial interest in the requested records. EPIC is a registered non-profit organization committed to privacy, open government, and civil liberties.[27]

On the second factor, whether "any identified commercial interest of the requester in disclosure outweighs the public interest . . . in disclosure." 39 C.F.R. § 265.9 (j)(3)(ii). Again, EPIC has no commercial interest in the requested records and has established that there is significant public interest in the requested records. Moreover, the Postal Service should presume that EPIC has satisfied 39 C.F.R. § 265.9 (j)(3)(ii). The Postal Service FOIA regulations state that a "component ordinarily shall presume that if a news media requester has satisfied the public interest standard, the public interest is the primary interest served by the requested disclosure." *Id*. EPIC is a news media requester and, as set out above, this request satisfies the public interest standard.

For these reasons, a full fee waiver should be granted for EPIC's request.

"successfully sued [the National Security Commission on Artificial Intelligence] to enforce compliance with Freedom of Information Act and Federal Advisory Committee Act transparency obligations"); *Mueller report issued with fewer redactions released on eve of election*, CNN (Nov. 3, 2020), https://www.cnn.com/2020/11/03/politics/mueller-report-fewer-redactions-election-eve/index.html ("Read the report, printed with permission from the Electronic Privacy Information Center, which obtained it in a Freedom of Information Act request[.]"); Lucas Mearian, *Feds may already have found a way to hack into Apple iPhone*s, Computerworld (Jan. 21, 2020), https://www.computerworld.com/article/3514209/feds-may-already-have-found-a-way-to-hack-into-apple-iphones.html ("Cellebrite's UFED Cloud Analyzer tool can purportedly unlock, decrypt and extract phone data . . . according a document obtained through a Freedom of Information Act request filed by the Electronic Privacy Information Center (EPIC).").

Conclusion

Thank you for your consideration of this request. We anticipate your determination on our request within 10 business days. For questions regarding this request, please contact Jake Wiener at FOIA@epic.org.

Respectfully,

/s Jake Wiener
Jake Wiener
EPIC Law Fellow

/s John Davisson
John Davisson
EPIC Senior Counsel