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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

United States Postal Inspection Service

Notice of a revised system of records: General Privacy Act System of Records

86 Fed Reg. 71,679

January 18, 2022

The Electronic Privacy Information Center (EPIC) submits these comments in response to the U.S. Postal Inspection Service's (USPIS) proposed modification to its Inspection Service Investigative File System to take in more data from Postal Service customers.[1] USPIS proposes to expand the existing data collection by aggregating eight new data elements: name, address, 11-Digit Delivery Point ZIP Code (ZIP 11), phone number, email address, tracking number, IP address, and moniker. EPIC urges USPIS to protect postal consumer privacy by reversing the proposed expansion of this system of records.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving the Privacy Act safeguards enacted by Congress.[2] EPIC also has an ongoing interest in USPIS data

[1] 86 Fed Reg. 71,679.
[2] Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice, Docket No. DHS-2011-0094 (Dec. 23, 2011), http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010),

collection and surveillance activities, particularly the use of facial recognition and social media tracking in its iCOP program.[3]

I. Background

The U.S. Postal Inspection Service is component agency within the U.S. Postal Service charged with law enforcement, crime prevention, and security. The agency is tasked with supporting and protecting the Postal Service, enforcing the roughly 200 laws covering criminal usage of the mail, and ensuring the public trust in the mail.[4] According to USPIS, postal inspectors investigate any crime concerning the mail, including mail theft, fraud, dangerous and prohibited mails, and cybercrime.[5] Postal inspectors present these cases to and work with federal and local prosecutors.[6] Inspection Service staff "gather information, collect and analyze evidence, and build cases," while the Postal Police Officers are charged with physical security of "high-value deliveries, property, and postal buildings".[7]

The Postal Service, and therefore USPIS, generally receives no public funding and instead relies on the sale of postage, products, and services to fund its operations.[8] Postal Service consumers pay for the activities of the Postal Inspection Service through their patronage of USPS.

---

http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2016-0002, DHS-2016-0001 (Feb. 22, 2016), https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf.

[3] EPIC v. USPS, https://epic.org/documents/epic-v-u-s-postal-service/.

[4] Postal Inspection Service Annual Report for FY 2019, https://www.uspis.gov/wp-content/uploads/2020/02/2019AR.pdf.

[5] How We Do It, USPIS.gov, https://www.uspis.gov/about/how-we-do-it.

[6] *Id.*

[7] About, USPIS.gov https://www.uspis.gov/about.

[8] *See*, Top Facts, USPS.com, https://facts.usps.com/top-facts/.

II. The Postal Inspection Service is at serious risk of mission creep when the agency expands information collections and investigations beyond traditional postal crimes.

The Postal Inspection Service has a well-defined mission in protecting the mail, but the agency has often overstepped its bounds. The Postal Inspection Service now claims a "wide jurisdiction" to preserve the "safety, security, and integrity of the nation's mail system from criminal misuse."[9] Claims of expansive jurisdiction and over-collection of data both create the risk of mission creep for law enforcement agencies. Mission creep occurs when an agency or component has access to more tools or information than it needs to complete its designed mission and expands into another role outside the designed mission to utilize those tools.

A classic example of mission creep within the Postal Inspection Service is the use of authority over obscene materials to harass and target the LGBTQ community. In the 1950s and 60s, USPIS investigated the delivery of gay publications, searching homes under laws intended to restrict mailing of obscene materials.[10] In 1954, postal inspectors refused to deliver ONE Magazine, the first overtly gay periodical, setting up a legal battle that reached the Supreme Court in the case *One, Inc. v. Olson*, 355 U.S. 371 (1958). Despite a ruling that vindicated One Magazine in 1958, Postal Inspectors continued to harass gay men throughout the 1960s for receiving men's fitness magazines.[11] In 1962, the Supreme Court again rejected the Postal Service's attempts to expansively define obscenity, ruling in *Manual Enterprises, Inc. v. Day*, 370 U.S. 478 that images of nude male models were not obscene materials. Postal inspectors used the Comstock Act as a tool to persecute gay men, straying far beyond their assigned mission of preventing the transmission of obscene

[9] How We Do It, USPIS.gov, https://www.uspis.gov/about/how-we-do-it.
[10] German Lopez, *The homophobic history of the Post Office*, Vox (May 28, 2014), https://www.vox.com/2014/5/28/5756494/the-homophobic-history-of-the-post-office (interviewing scholar of LGBT history David Johnson).
[11] *Id.*

material. The agency lost its mooring and suffered major losses in court as homophobia enabled mission creep.

Similarly, the Cybercrime unit's iCOP program purports to facilitate the "identification, disruption, and dismantling of individuals and organizations that use the mail or USPS online tools to facilitate black market Internet trade or other illegal activities."[12] This program has been used, however, to monitor individuals and produce intelligence products distributed across the federal government.[13] Analysts in the program utilize USPS systems and tools to "provide open source intelligence and cryptocurrency blockchain analysis in support of all Inspection Service investigations."[14] The availability of those tools facilitated monitoring protesters and organizers engaging in protected First Amendment activities. The Postal Inspection Service should be wary of onboarding new tools and new data sources given the agency's troubled history with mission creep.

The risk of mission creep has only increased as USPIS has more frequently worked with other law enforcement agencies on matters only tangentially related the mail. The Postal Inspection Service's Fiscal Year 2019 Annual Report describes how the cybercrime unit worked with other federal and international law enforcement agencies to prosecute the administrators of the Wall Street Dark Web marketplace.[15] Moreover, the Service's partnerships and task forces with other agencies have dragged the Inspection Service into investigating drug and human trafficking networks, foreign criminals, and possible acts of terrorism.[16] In 2011, the USPS OIG found that 34% of all USPIS investigations "do not directly support protection of Postal Service assets, Postal Service employees, or the mail system. Further, by pursuing work outside of these core areas, the Postal Inspection

[12] 2019 Annual Report at 36.
[13] 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.
[14] 2019 Annual Report at 36.
[15] *Id*. at 37.
[16] How We Do It, USPIS.gov, https://www.uspis.gov/about/how-we-do-it.

Service has moved away from its primary responsibility to protect the Postal Service, secure the nation's mail system and ensure public trust in the mail."[17] USPIS has become the "silent service" behind many federal and local law enforcement operations, threatening the privacy and civil liberties of individuals across the country.

III. The Postal Inspection Service is seeking to expand its system of records to include data from USPS customers who have done nothing to warrant law enforcement surveillance.

The Postal Service is proposing to modify its Inspection Service Investigative File System to ingest new types of data. Under the proposed changes, USPIS will collect and aggregate eight data elements: name, address, 11-Digit Delivery Point ZIP Code (ZIP 11), phone number, email address, tracking number, IP address, and moniker.[18] This information will be taken from Customer Registration, Inspection Service Investigative File System, Click-n-Ship, and National Meter Accounting and Tracking System (NMATS).[19] The Postal Service collects name, address, and ZIP codes from customers to verify addresses for shipping as the information is crosschecked with the USPS address database.[20] Similarly, the Postal Service collects phone number, email address, and tracking number enable end-to-end item tracking and communication for the service.[21] USPS collects IP address and moniker information when customers use its website for tracking services.[22] All of this data is collected through the commercial wing of the Postal Service, but USPS is now proposing to transmit it to the law enforcement wing.

[17] USPS OIG, Report No. FF-AR-11-009, Audit Report – New Approaches to Reduce Costs (Jun. 14, 2011), https://www.uspsoig.gov/sites/default/files/document-library-files/2015/FF-AR-11-009.pdf.
[18] 86 Fed Reg. 71,679.
[19] *Id*.
[20] DPV, usps.com, https://postalpro.usps.com/address-quality/dpv.
[21] *See*, Package Tracking FAQs, usps.com, https://faq.usps.com/s/topic/0TOt00000004HFmGAM/usps-tracking-?tabset-44809=2.
[22] Privacy Policy, usps.com, https://m.usps.com/m/PrivacyPolicy.

All this information attaches a greater amount of personal data, including digital trails, to customers using USPS services. This data collection is in addition to investigative records already accessible to USPIS in the system, such as "person names, Social Security Numbers, case number, addresses, reports of postal inspectors and third parties; physical identifying characteristics (including fingerprints, voiceprints, handwriting samples, polygraph tests, photographs, or other biometrics); and employment and payroll information maintained by USPS."[23]

Access to this kind of commercial data without a warrant is unique to the Postal Service and the Inspection Service. Ordinarily, government agencies must obtain warrant or court order to compel companies to produce sensitive data about its customers.[24] The Electronic Communications Privacy Act prohibits companies from voluntarily disclosing Americans' personal information to government agencies.[25] When a customer uses shipping services provided by USPS, they typically do not—and should not—expect that their commercial data will be given to a law enforcement agency. The fact that USPIS is funded by the commercial activities of the Postal Service yet still has access to the Service's user data for law enforcement purposes creates a dangerous tension between the commercial and enforcement goals of the institution. The Postal Inspection Service can mitigate this tension by opting not to further exploit USPS customer data.

IV. Increased access to customer data poses privacy risks for customers of the Postal Service.

The USPIS has already increased data collection without publishing a privacy impact assessment of its iCOP program.[26] Since 2018, iCOP has used a suite of surveillance tools, including facial recognition and social media monitoring services, to track individuals and produce intelligence

[23] 86 Fed Reg. 71,679.
[24] *See Carpenter v. United States*, 138 S. Ct. 2206, 201 L. Ed. 2d 507 (2018).
[25] https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/
[26] 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.

products distributed across the federal government. The program used Clearview AI's facial recognition product and social media monitoring tools to surveil protesters in the summer of 2020. [27] USPIS also monitored online activity after the January 6, 2021 insurrection in Washington, D.C., and its officers adopted covert online identities and attempted to identify upcoming protests and "inflammatory" posts on various social media sites. [28] EPIC has filed a lawsuit under the E-Government Act of 2002 to stop the U.S. Postal Service's law enforcement arm from using facial recognition and social media monitoring tools based on its failure to perform a privacy impact assessment for new information collection technology. [29]

The Postal Service has a poor track record managing sensitive personal data, as evidenced by its treatment of mail covers and data breaches. A mail cover is a surveillance tool used by the Postal Service to monitor the mail of a person suspected of criminal activity by recording the information on the outside of all letters and packages delivered to a home or business.[30] Mail covers are not subject to any judicial oversight, and the Postal Inspection Service has taken advantage of the program, granting an extraordinary number of requests for mail surveillance.[31] From 2010 to 2014, the Postal Inspection Service approved 118,577 mail covers requested by its postal inspectors and 39,966 requested by external law enforcement authorities.[32] In 2014, an OIG report found that Postal Service employees did not always safeguard mail cover information or follow procedures for recording information, posing serious privacy risks.[33]

---

[27] *Id.*
[28] EPIC v. USPS, https://epic.org/documents/epic-v-u-s-postal-service/.
[29] *Id.*
[30] Ron Nixon, *Postal Service Failed to Protect Personal Data in Mail Surveillance, Report Say*, N.Y. Times (Sept. 25, 2015), https://www.nytimes.com/2015/09/25/us/postal-service-failed-to-protect-personal-data-in-mail-surveillance-report-says.html.
[31] *Id.*
[32] *Id.*
[33] U.S.P.S. Office of Inspector General, Report No. HR-AR-15-007, U.S. Postal Inspection Service Mail Covers Program — Phase II (Sept. 15, 2015, https://www.uspsoig.gov/document/us-postal-inspection-service-mail-covers-program-%E2%80%94-phase-ii.

USPS customers have already suffered privacy harms due to lax cybersecurity practices at the Postal Service. In 2018, a security vulnerability on the USPS website allowed anyone to see the personal account information of its customers, including usernames and street addresses.[34] As a result, sensitive information from more than 60 million individuals was exposed.[35] This breach went unaddressed for an entire year.[36] The Postal Inspection Service should not compound the risk of data breach to Postal Service customers by aggregating their data in another database. The expansion proposed in the SORN will not only magnify the risk of data breach, it will also expose more individuals to wrongful surveillance.

Conclusion

EPIC urges the Postal Inspection Service to protect itself and individuals across the country by abandoning its proposed expansion of information collection from Postal Service consumers. The more personal information the Postal Inspection Service takes in through its surveillance activities, , the likelier it is to stray beyond USPIS's core mission. By demanding access to more postal data, the Postal Inspection Service is exposing USPS customers to wrongful surveillance and a greater threat of data breach. The Postal Service and the Postal Inspection Service should separate their information collection procedures and ensure that USPS customers do not come under greater surveillance simply by using a government mail carrier.

[34] Shannan Liao, *USPS took a year to fix a vulnerability that exposed all 60 million users' data*, Verge (Nov. 22, 2018), https://www.theverge.com/2018/11/22/18107945/usps-postal-service-data-vulnerability-security-patch-60-million-users.
[35] *Id*.
[36] *Id*.

Respectfully Submitted,

Jake Wiener
Jake Wiener
EPIC Law Fellow

Noah Huffman
Noah Huffman
EPIC Volunteer