IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036,

Plaintiff,

v.

UNITED STATES POSTAL SERVICE
475 L'Enfant Plaza SW
Washington, DC 20260;

UNITED STATES POSTAL INSPECTION SERVICE
475 L'Enfant Plaza SW
Washington, DC 20260,

Defendants.

Civ. Action No. 21-2156-TNM

AMENDED COMPLAINT FOR INJUNCTIVE, MANDAMUS, AND DECLARATORY RELIEF

1. This is an action under the Administrative Procedure Act ("APA"), 5 U.S.C. §§ 551–706; the E-Government Act of 2002, Pub. L. 107-347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note); the Mandamus and Venue Act of 1962, 28 U.S.C. §§ 1361, 1391(e); and the Declaratory Judgment Act, 28 U.S.C. § 2201(a), to secure the timely completion and publication of a Privacy Impact Assessment ("PIA") by Defendants United States Postal Service ("USPS") and United States Postal Inspection Service ("USPIS").

2. Plaintiff Electronic Privacy Information Center ("EPIC") challenges Defendants' unlawful failure to conduct and publish a Privacy Impact Assessment before (1) initiating the Internet Covert Operations Program ("iCOP"); (2) procuring and using facial recognition and

social media surveillance tools under iCOP; and (3) initiating new collections of personal information under iCOP.

3. Accordingly, EPIC seeks an order directing Defendants (1) to conduct and publish the required Privacy Impact Assessment(s), and (2) to suspend the Internet Covert Operations Program and to cease and desist from using facial recognition and social media surveillance tools or collecting personal information under iCOP unless and until Defendants complete such Privacy Impact Assessment(s).

Jurisdiction and Venue

4. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331, 5 U.S.C. § 702, 28 U.S.C. § 1361, and 5 U.S.C. § 704. This Court has personal jurisdiction over Defendants USPS and USPIS.

5. Venue is proper in this district under 5 U.S.C. § 703 and 28 U.S.C. § 1391.

Parties

6. Plaintiff EPIC is a Washington, D.C. nonprofit organization 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 data collection activities.

7. EPIC is a dues-paying membership organization, as set forth in the EPIC Articles of Incorporation[1] and the EPIC Bylaws.[2] EPIC is governed by a Board of Directors, all of whom "must be Members of" EPIC.[3]

---

[1] EPIC, *Articles of Incorporation* (2018) ("The Corporation [EPIC] . . . may refer to people as 'members' pursuant to D.C. Code § 29-404.01, and the qualifications, rights, and privileges of such people shall be as set forth in the bylaws.").
[2] EPIC, *Bylaws of the Electronic Privacy Information Center* § 2.02 (as amended Jan. 26, 2018), https://epic.org/epic/bylaws.pdf.
[3] *Id.*

8. EPIC's Members are "distinguished experts in law, technology, and public policy."[4] New Members are designated by EPIC following "nomination by the current Members and a vote of the Board [of Directors.]"[5]

9. 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. DOD*, 241 F. Supp. 2d 5, 15 (D.D.C. 2003).

10. EPIC regularly seeks to halt unlawful surveillance and enforce mandatory publication of Privacy Impact Assessments through litigation under the E-Government Act of 2002. In *EPIC v. Department of Commerce*, 928 F.3d 95 (D.C. Cir. 2019), EPIC challenged the Census Bureau's failure to conduct and publish a PIA before collecting citizenship data through the 2020 Census.[6] The citizenship question was ultimately withdrawn by the Bureau. In *EPIC v. DHS*, No. 18-1268 (D.D.C. settled July 11, 2019), EPIC challenged the failure of the Department of Homeland Security to publish a PIA for a system designed to track journalists, bloggers, and social media users.[7] EPIC's suit revealed that the DHS had unlawfully failed to conduct a PIA prior to developing the "Media Monitoring Services" platform and secured a public commitment from the agency that it was not using the system.[8] EPIC also challenged the unlawful collection of personal voter data by the Presidential Advisory Commission on Election Integrity in *EPIC v. Commission*, 878 F.3d 371 (D.C. Cir. 2017).[9] EPIC's suit led the Commission to suspend data

---

[4] *Id.* § 5.01.
[5] *Id.*
[6] EPIC, *EPIC v. Commerce* (Census Privacy), https://epic.org/privacy/litigation/pia/epic-v-commerce/default.html.
[7] EPIC, *EPIC v. DHS (Media Monitoring Services)*, https://epic.org/foia/dhs/media-monitoring-services/.
[8] *Id.*
[9] EPIC, *EPIC v. Presidential Election Commission*, https://epic.org/privacy/litigation/voter/epic-v-commission/.

collection, discontinue the use of an unsafe computer server, and delete voter information that had been illegally obtained.

11. Defendant USPS is a federal agency within the meaning of 44 U.S.C. § 3502(1) and 5 U.S.C. § 701(b)(1) and is headquartered in Washington, D.C.

12. Defendant USPIS is a federal agency within the meaning of 44 U.S.C. § 3502(1) and 5 U.S.C. § 701(b)(1) and is headquartered in Washington, D.C.

Defendants' Obligation to Conduct and Publish Privacy Impact Assessments

13. Under section 208 of the E-Government Act, federal agencies—including the United States Postal Service and United States Postal Inspection Service—are required to "conduct," "ensure the review of," and "make . . . publicly available" a Privacy Impact Assessment before (1) "initiating a new collection of information" that will be electronically stored or transmitted "in an identifiable form," or (2) "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form."[10]

14. Information is in an identifiable form if it "permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."[11] This includes "combination[s] of gender, race, birth date, geographic indicator, and other descriptors" that would permit individuals to be uniquely identified, even in the absence of names, social security numbers, or other direct identifiers.[12] This definition also encompasses facial images,

[10] E-Government Act § 208(b)(1).
[11] *Id.* § 208(d).
[12] Joshua B. Bolten, Dir., Office of Mgmt. & Budget, Executive Office of the President, M03-22, Memorandum for Heads of Executive Departments and Agencies, Attachment A § II.A.2 (Sept. 26, 2003), https://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html [hereinafter OMB Guidance].

which can be used to identify a individuals through visual inspection and/or the use of facial recognition technology.

15. The Office of Budget and Management ("OMB"), which oversees enforcement of the E-Government Act government-wide, defines a PIA as:

> [A]n analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[13]

16. The USPS "has adopted policies to comply" with the E-Government Act's privacy provisions, "includ[ing] the requirement[] to conduct privacy impact assessments[.]."[14] The USPS conducts PIAs within its Business Impact Assessment ("BIA") process.[15] A PIA/BIA "must be completed for all information resources, whether the information resource is developed in house, outsourced or hosted in non-Postal Service facilities."[16]

17. To satisfy section 208, a PIA must specify, *inter alia*, "what information is to be collected"; "why the information is being collected"; "the intended use [by] the agency of the information"; "with whom the information will be shared"; "what notice or opportunities for consent would be provided"; and "how the information will be secured."[17] Additionally, a PIA

---

[13] *Id.* § II.A.6.
[14] U.S. Postal Serv., *Guide to Privacy, the Freedom of Information Act and Records Management* § 2-3.4 (2019), https://about.usps.com/handbooks/as353/as353c2_006.htm ("E–Government Act of 2002").
[15] U.S. Postal Serv., *Information Security* § 3-3 (June 2021), https://about.usps.com/handbooks/as805.pdf.
[16] *Id.* § 3-3.1.
[17] E-Government Act § 208(b)(2)(B)(ii).

"must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA."[18]

18. Where a PIA is required for a "major information system," the PIA should "reflect more extensive analyses of: 1. the consequences of collection and flow of information, 2. the alternatives to collection and handling as designed, 3. the appropriate measures to mitigate risks identified for each alternative and, 4. the rationale for the final design choice or business process."[19] A "major information system" includes any "system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources."[20] In these circumstances, a mere "checklist or template" will not satisfy an agency's PIA obligation.[21]

19. According to the OMB, "Agencies should commence a PIA when they *begin* to develop a new or significantly modified [information technology] system or information collection[.]"[22] Thus, when an agency intends to "develop . . . projects that collect, maintain or disseminate information in identifiable form from or about members of the public," the agency must first conduct a PIA.[23]

20. An agency's privacy obligations under the E-Government Act do not end with the initial publication of a Privacy Impact Assessment. Rather, a PIA must be revised continually "to reflect changed information collection authorities, business processes or other factors affecting

[18] OMB Guidance § II.C.1.b.
[19] *Id.* § II.C.2.a.ii.
[20] *Id.* § II.A.4.
[21] *Id.* § II.C.2.a.iii.
[22] *Id.* § II.C.2 (emphasis added).
[23] *Id.* § II.B.1.a.

the collection and handling of information in identifiable form."[24] Specifically, a PIA must be "updated as necessary where a system change creates new privacy risks," including "when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)"; "when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form"; and "when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated."[25]

Facts

Defendants' Use of Surveillance Tools and Collection of Personal Data Under iCOP

21. The United States Postal Service and United States Postal Inspection Service operate a surveillance program known as the Internet Covert Operations Program ("iCOP").[26] This program has existed since at least 2018 as "one of seven functional groups within the Inspection Service Cybercrime program."[27] According to the Postal Inspection Service, iCOP is intended 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."[28] USPIS states that the broader Inspection Service Cybercrime program "investigate[s] security incidents and criminal activities affecting the USPS computer network,

---

[24] *Id.* § II.B.4.
[25] *Id.* § II.B.2.d.
[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.
[27] U.S. Postal Inspection Serv., *Fiscal Year 2019 Annual Report* 36 (Feb. 2020), https://www.uspis.gov/wp-content/uploads/2020/02/FY-2019-annual-report-508-web.pdf.
[28] *Id.*

USPS E-commerce products and services, and field investigations related to the Dark Web and cryptocurrencies."[29]

22. As part of iCOP, Defendants have used multiple electronic surveillance technologies, including facial recognition and social media monitoring tools.[30]

23. According to the Government Accountability Office, Defendants used Clearview AI's facial recognition service in the summer of 2020 to "help identify individuals suspected of criminal activity that took place in conjunction with the period of civil unrest, riots, or protests."[31]

24. Clearview AI performs facial recognition matching using a database of over 3 billion images scraped from Facebook and other social media sites. Clearview AI's combined facial recognition and social media monitoring product identifies (or purports to identify) an individual from their image and provides the user with links to the individual's personal information, social media profiles, and other related online material.[32]

25. Clearview AI has incurred extensive public backlash and legal scrutiny over its bulk scraping of images from social media websites without user consent and contrary to those

---

[29] *Id*.
[30] 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.
[31] U.S. Gov't Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (June 3, 2021), https://www.gao.gov/assets/gao-21-518.pdf.
[32] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

websites' terms of service.[33] The company is currently facing legal action in the European Union, Canada, and Illinois over its web-scraping practices.[34]

26. Defendants also used a trial of Vigilant Solutions' facial recognition service for at least ten months in 2017.[35] Vigilant Solutions' facial recognition product conducts image matching against a database of millions of images and can also perform "near-real-time monitoring" of video cameras against one or more watchlists.[36] Vigilant Solutions is also a provider of license plate reader surveillance technology.

27. Facial recognition services such as Clearview AI and Vigilant enable Defendants to identify individuals and collect personally identifiable information, including names, biographical information, and the contents of social media pages.

28. Defendants have also used Zignal Labs' social media surveillance platform, which is capable of tracking a social media "narrative" back to the individual who initiated the narrative and of identifying specific individuals as "influencers."[37]

---

[33] Louise Matsakis, *Scraping the Web Is a Powerful Tool. Clearview AI Abused It.*, Wired (Jan. 25, 2020), https://www.wired.com/story/clearview-ai-scraping-web/,

[34] Ian Carlos Campbell, *Clearview AI hit with sweeping legal complaints over controversial face scraping in Europe*, The Verge (May 27, 2021), https://www.theverge.com/2021/5/27/22455446/clearview-ai-legal-privacy-complaint-privacy-international-facial-recognition-eu; Office of the Privacy Comm'r of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada* (Feb. 2, 2021), https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/#toc2 (finding that Clearview AI violated Canadian law by obtaining images of individuals without consent and breached websites' terms of service).

[35] *Id*. at 14.

[36] Vigilant Solutions, *Vigilant FaceAlert Facial Detection and Alerting* (2021), https://www.motorolasolutions.com/en_us/products/command-center-software/real-time-intelligence-operations/vigilant-facealert-facial-recognition-software.html.

[37] Winter, *supra* note 30.

29. Defendants have also used Nfusion software to create anonymous email accounts and social media profiles for information collection.[38]

30. From 2018 to 2019, Defendants, acting through the iCOP, used surveillance tools to identify at least nine previously unknown individuals.[39]

31. Defendants have used Clearview AI to "to help identify unknown targets in an investigation or locate additional social media accounts for known individuals[.]"[40]

32. Defendants have used Zignal Labs' social media surveillance platform and Nfusion software to collect social media information, including profiles and posts.

33. Under iCOP, the USPIS "assigns its analysts to patrol social media to look for information on upcoming protests and search for potential threats of violence."[41] For example, a March 2021 iCOP intelligence bulletin lists individual social media posts deemed "inflammatory" by the program.[42]

34. Defendants are known to have used social media monitoring software in the spring and summer of 2020 and again in spring of 2021. A March 2021 USPIS bulletin stated that "[a]nalysts with the United States Postal Inspection Service (USPIS) Internet Covert Operations Program (iCOP) monitored significant activity regarding planned protests occurring internationally and domestically on March 20, 2021."[43] Defendants distributed individuals' social media posts containing identifying information in the bulletin.[44] According to Yahoo

---

[38] *Id.*
[39] US Postal Inspection Serv., *supra* note 27, at 36.
[40] Winter, *supra* note 30.
[41] *Id.*
[42] *Id.*; U.S. Postal Inspection Serv., *Situational Awareness Bulletin* (Mar. 16, 2021), *available at* https://www.scribd.com/document/503807748/Post-Office-Redacted.
[43] *Id.*
[44] *Id.*

News, Defendants monitored Facebook, Parler, Telegram, and other social media sites during this time period.[45]

35. By using Clearview AI, Defendants undertook new collections of personally identifiable information, including facial images, identities derived from facial recognition matches, and social media accounts directly linked to identified individuals.

36. By using social media analysis and covert intelligence gathering software to collect social media accounts, posts, and identifying information, Defendants undertook new collections of personally identifiable information.

Defendants' Unlawful Failure to Assess the Privacy Impact of iCOP

37. To date, Defendants have not conducted or published a Privacy Impact Assessment concerning the Internet Covert Operations Program, the facial recognition and social media monitoring tools procured and used under iCOP, or the collection of personal information initiated under iCOP.

38. The USPS Privacy and Records Management Office ("USPS Privacy Office") maintains a list of PIAs on the USPS website.[46]

39. The filename of that list is "business-impact-assessment-8-2010.rtf," which indicates that the USPS Privacy Office has not updated the list since August 2010.

40. None of the PIAs listed on the USPS website address iCOP, the facial recognition and social media monitoring tools procured and used under iCOP, or the collection of personal information initiated under iCOP.

---

[45] Winter, *supra* note 26.
[46] U.S. Postal Serv., *Privacy Policy on Privacy Impact Assessments* (2021), https://about.usps.com/who-we-are/privacy-policy/privacy-impact-assessments.htm.

41. The USPS does not proactively publish PIAs on its website. Instead, the USPS Privacy Office claims to comply with the E-Government Act by offering PIAs upon request submitted to the Privacy Office's public email address, privacy@usps.com.

EPIC's Attempts to Obtain the iCOP PIA Under FOIA

42. On May 21, 2021, EPIC sent a Freedom of Information Act ("FOIA") request to USPIS headquarters seeking 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" and other documents related to the PIA. *See* Ex. A.

43. On June 2, 2021, EPIC received a final response from the USPIS FOIA Unit stating that "A search was conducted of the Postal Inspection Service records at National Headquarters. This search disclosed no records." *See* Ex. B.

44. On the day that EPIC sent its FOIA request to USPIS—May 21, 2021—EPIC also sent a copy of the same request to the USPS Privacy Office.

45. On May 26, 2021 the USPS Privacy Office confirmed receipt of EPIC's request.

46. On May 26, 2021 EPIC received a determination from USPS Privacy and Records Management Information Specialist Tai Thompson concluding that the Postal Service component of USPS "is not the appropriate agency to respond to [EPIC's] request." Thompson stated that she had "forwarded [EPIC's] request to the FOIA Requester Service Center for the Inspection Service for action and direct response to [EPIC]." The USPS Privacy Office stated that the USPIS was the agency responsible for maintaining Postal Service law enforcement records.

47. USPS Privacy and Records Management closed EPIC's FOIA request without performing a search. *See* Ex. C.

48. On May 26, 2021 EPIC Law Fellow Jake Wiener responded to Ms. Thompson by email, asking the USPS Privacy Office to reconsider the determination. Mr. Wiener explained that the Postal Service Privacy Office is responsible for conducting Privacy Impact Assessments for both the USPS and the USPIS.[47] As such, the USPS Privacy Office was likely to have the iCOP PIA (if one was conducted).

49. EPIC received no response to its May 26, 2021 email.

50. One June 14, 2021, EPIC submitted a renewed FOIA request to the USPS Privacy Office seeking the iCOP PIA and clarifying why the USPS Privacy Office was likely to have the iCOP PIA (if one was conducted). EPIC noted that the USPS Privacy Office is responsible for creating and maintaining PIAs for all USPS components.

51. On June 23, 2021 the USPS Privacy Office determined that EPIC's June 14 request was duplicative of EPIC's May 26 request and closed the renewed request without performing a search.

52. EPIC did not receive a PIA for iCOP and/or the facial recognition and social media monitoring tools procured and used under iCOP in response to any of its FOIA requests.

53. EPIC maintains an ongoing interest in any PIA(s) relating to the iCOP or facial recognition and social media monitoring technologies used by USPS and USPIS. EPIC will continue to seek these records under the Freedom of Information Act.

---

[47] *See* U.S. Postal Serv., *Privacy Impact Assessments/Business Impact Assessments* (2010), https://about.usps.com/who-we-are/privacy-policy/business-impact-assessment-8-2010.rtf (listing Privacy Impact Assessments for, *inter alia*, the "Inspection Service Integrated Information System (ISIIS)" and the "Inspection Service National Assets Tracking System (ISNATS)").

EPIC's Attempts to Obtain the iCOP PIA Directly From the USPS Privacy Office

54. On May 25, 2021, EPIC Law Fellow Jake Wiener sent an email and letter to the USPS Privacy Office's publicly listed email addresses (privacy@usps.gov and privacy@usps.com) requesting the iCOP PIA. *See* Ex. D.

55. On June 2, 2021 EPIC fellow Jake Wiener sent a follow-up email to the Privacy Office's public email accounts again requesting the iCOP PIA and seeking to confirm if such a PIA exists.

56. To date EPIC has received no response from the USPS Privacy Office to these inquiries and has not received a PIA for iCOP and/or the facial recognition and social media monitoring tools procured and used under iCOP.

57. EPIC maintains an ongoing interest in any PIA(s) relating to the iCOP or facial recognition and social media monitoring technologies used by USPS and USPIS. EPIC will continue to seek these records directly from the USPS Privacy Office.

Count I

Violation of APA: Unlawful Agency Action

58. Plaintiff asserts and incorporates by reference paragraphs 1–57.

59. Defendants have unlawfully (1) initiated the Internet Covert Operations Program, (2) procured and used facial recognition and social media monitoring tools under the iCOP, and (3) used facial recognition and social media monitoring tools to initiate or significantly modify collections of personal information under the iCOP without first conducting and publishing the full and complete Privacy Impact Assessment(s) required by section 208(b) of the E-Government Act.

60. In violating section 208(b) the E-Government Act, Defendants have taken agency actions that are arbitrary, capricious, an abuse of discretion, and 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).

61. Defendants' initiation of the iCOP, procurement and use of facial recognition and social media monitoring tools, and collection of personal information are final agency actions within the meaning of 5 U.S.C. § 704.

62. Plaintiff EPIC is adversely affected, aggrieved, and injured in fact by Defendants' actions. By initiating the iCOP, procuring and using facial recognition and social media monitoring tools, and collecting personal information without first conducting and publishing the full and complete Privacy Impact Assessment(s) required by section 208(b) of E-Government Act, Defendants have frustrated Plaintiff's longstanding mission to educate the public about the government's collection of personally identifiable information and—in particular—about the unique privacy harms caused by advanced electronic surveillance technologies.

63. Plaintiff EPIC is also adversely affected, aggrieved, and injured in fact by Defendants' actions through EPIC's Members. EPIC's Members, many of whom reside in the United States, use social media platforms including Facebook and Twitter. Clearview AI conducted bulk scraping of images from social media sites used by EPIC's members, making it virtually certain that EPIC's Members are included in Clearview AI's database of 3 billion facial images. Defendants then procured the Clearview AI system and used the personal information contained in the database to conduct facial recognition queries and comparisons. Likewise, EPIC's Members were active on social media platforms in the summer of 2020, when Defendants are known to have used social media monitoring tools to collect the personal data of platform users. By procuring facial recognition and social media tools and using those tools to collect and

process personal information without first publishing the Privacy Impact Assessment(s) required by section 208(b) of the E-Government Act, Defendants have unlawfully denied EPIC's Members—and by extension, EPIC—a full and timely assessment of how their privacy interests would and will be affected. *See* Exs. E, F.

64. Plaintiff's initiation of the iCOP, procurement and use of facial recognition and social media monitoring tools, and collection of personal information without first completing and publishing the requisite Privacy Impact Assessments(s) prevented EPIC from obtaining information about the iCOP under the Freedom of Information Act at the time EPIC was legally entitled to it, thereby denying EPIC's Members—and by extension, EPIC—the ability to assess how their privacy interests have been affected by Defendants' use of facial recognition and social media monitoring tools.

65. Plaintiff has exhausted all applicable administrative remedies.

Count II

Violation of APA: Agency Action Unlawfully Withheld

66. Plaintiff asserts and incorporates by reference paragraphs 1-57.

67. Defendants have failed to conduct and publish the Privacy Impact Assessment(s) required by section 208(b) of the E-Government Act before (1) initiating the iCOP, (2) procuring and using facial recognition and social media monitoring tools under the iCOP, and (3) using facial recognition and social media monitoring tools to initiate or significantly modify collections of personal information under the iCOP.

68. In failing to take the steps required by section 208(b) of the E-Government Act, Defendants have unlawfully withheld or unreasonably delayed agency action in violation of 5 U.S.C. § 706(1).

69. Plaintiff EPIC is adversely affected, aggrieved, and injured in fact by Defendants' inaction. By failing to conduct and publish the full and complete Privacy Impact Assessment(s) required by section 208(b) of the E-Government Act before initiating the iCOP, procuring and using of facial recognition and social media monitoring tools, and collecting personal information, Defendants have frustrated Plaintiff's longstanding mission to educate the public about the government's collection of personally identifiable information and—in particular—about the unique privacy harms caused by advanced electronic surveillance technologies.

70. By failing to create the required Privacy Impact Assessment(s), Defendants have unlawfully denied Plaintiff EPIC access to information about the iCOP and Defendants' use of facial recognition and social media monitoring tools that EPIC would have otherwise received under the Freedom of Information Act, 5 U.S.C. § 552. Plaintiffs have a statutory right to access the information in Privacy Impact Assessments under the Freedom of Information Act. By procuring and using facial recognition and social media monitoring tools without first conducting the requisite Privacy Impact Assessment(s), Defendants denied EPIC timely access to the information that it should have received in response to its FOIA request, causing EPIC to suffer an injury in fact. *Waterkeeper Alliance v. Environmental Protection Agency*, 853 F.3d 527 (D.C. Cir. 2017).

71. Plaintiff EPIC is also adversely affected, aggrieved, and injured in fact by Defendants' actions through EPIC's Members. EPIC's Members, many of whom reside in the United States, use social media platforms including Facebook and Twitter. Clearview AI conducted bulk scraping of images from the social media sites used by EPIC's members, making it virtually certain that EPIC's Members are included in Clearview AI's database of 3 billion facial images. Defendants then procured the Clearview AI system and used the personal information contained

in Clearview AI's database to conduct facial recognition queries and comparisons. Likewise, EPIC's Members were active on social media platforms in the summer of 2020, when Defendants are known to have used social media monitoring tools to collect the personal data of platform users. By procuring facial recognition and social media tools and using those tools to collect and process personal information without first publishing the Privacy Impact Assessment(s) required by section 208(b) of the E-Government Act, Defendants have unlawfully withheld from EPIC's Members—and by extension, EPIC—a full and timely assessment of how their privacy interests would and will be affected. *See* Exs. E, F.

72. Plaintiff has exhausted all applicable administrative remedies.

Count III

Violation of the E-Government Act: Failure to Conduct Privacy Impact Assessment(s)
(Relief in the Nature of Mandamus)

73. **Plaintiff asserts and incorporates by reference paragraphs** 1-57.

74. Defendants have failed to conduct and publish the Privacy Impact Assessment(s) required by section 208(b) of the E-Government Act before (1) initiating the iCOP, (2) procuring and using facial recognition and social media monitoring tools under the iCOP, and (3) using facial recognition and social media monitoring tools to initiate or significantly modify collections of personal information under the iCOP.

75. By failing to conduct and publish the required Privacy Impact Assessment(s), Defendants have unlawfully denied Plaintiff EPIC access to information about the iCOP and Defendants' use of facial recognition and social media monitoring tools that EPIC would have otherwise received under the Freedom of Information Act, 5 U.S.C. § 552. Plaintiffs have a statutory right to access the information in Privacy Impact Assessments under the Freedom of Information Act. By procuring and using facial recognition and social media monitoring tools without first conducting

the requisite Privacy Impact Assessment(s), Defendants denied EPIC timely access to the information that it should have received in response to its FOIA request, causing EPIC to suffer an injury in fact. *Waterkeeper Alliance v. Environmental Protection Agency*, 853 F.3d 527 (D.C. Cir. 2017).

76. Plaintiff EPIC is adversely affected, aggrieved, and injured in fact by Defendants' violation of the E-Government Act. By failing to conduct and publish the full and complete Privacy Impact Assessment(s) required by section 208(b) of the E-Government Act before initiating the iCOP, procuring and using of facial recognition and social media monitoring tools, and collecting personal information, Defendants have frustrated Plaintiff's longstanding mission to educate the public about the government's collection of personally identifiable information and—in particular—about the unique privacy harms caused by advanced electronic surveillance technologies

77. Plaintiff has exhausted all applicable administrative remedies.

78. Plaintiff is entitled to a writ of mandamus (1) compelling Defendants United States Postal Service and United States Postal Inspection Service to conduct and publish the Privacy Impact Assessment(s) required by section 208(b) of E-Government Act, and (2) compelling Defendants to suspend the Internet Covert Operations Program and to and cease and desist from any use of facial recognition and social media surveillance tools thereunder until the Defendants have conducted, reviewed, and published the full and complete Privacy Impact Assessment(s) required by section 208(b) of E-Government Act.

Requested Relief

WHEREFORE, Plaintiff prays that this Court:

A. Hold unlawful and set aside Defendants' initiation of the Internet Covert Operations Program, Defendants' procurement and use of facial recognition and social media surveillance tools through iCOP, and Defendants' collection of personal information using such tools;

B. Issue an injunction and/or a writ of mandamus compelling Defendants to conduct, review, publish, and disclose to EPIC the full and complete Privacy Impact Assessment(s) required by section 208(b) of E-Government Act for the Internet Covert Operations Program, for any facial recognition and social media surveillance tools procured or used under iCOP, and for any collection of personal information initiated or significantly modified under iCOP;

C. Order Defendants to suspend the Internet Covert Operations Program and to and cease and desist from any use of facial recognition and social media surveillance tools thereunder until the Defendants have conducted, reviewed, published and disclosed to EPIC the full and complete Privacy Impact Assessment(s) required by section 208(b) of E-Government Act;

D. Issue a declaration of the rights and other legal relations of the parties under 28 U.S.C. § 2201(a) with respect to all claims;

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

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

Respectfully Submitted,

ALAN BUTLER, D.C. Bar #1012128
EPIC President and Executive Director

/s/ John L. Davisson
JOHN L. DAVISSON, D.C. Bar #1531914
EPIC Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC

Dated: November 9, 2021