IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. UNITED STATES POSTAL SERVICE, *et al.* Defendants.	Civ. Action No. 21-2156-TNM

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES*

Cases

* Authorities principally relied upon are designated by an asterisk (*).

Statutes

Other Authorities

INTRODUCTION

The Electronic Privacy Information Center ("EPIC") respectfully opposes the Defendants' Motion to Dismiss, ECF No. 14 which must be denied. First, EPIC has established Article III standing to bring its claims. The unlawful failure of the U.S. Postal Service and U.S. Postal Inspection Service to conduct required privacy impact assessments for the Internet Covert Operations Program has denied EPIC and its Members vital information to which they are entitled, causing them injuries in fact redressable by this Court. Second, the U.S. Postal Service is subject to the E-Government Act, notwithstanding the broad exemption from federal law contained in the Postal Reorganization Act. Third, EPIC has a cause of action under the Administrative Procedure Act because the Postal Inspection Service is not exempt from the APA when performing law enforcement functions beyond the scope of the Postal Reorganization Act. Finally, even if a cause of action is not available under the APA, EPIC is entitled to mandamus relief.

STATEMENT OF THE CASE

A. The E-Government Act of 2002

In 2002, Congress passed the E-Government Act with the aim of "promot[ing] better informed decisionmaking by policy makers"; "provid[ing] enhanced access to Government information"; and "mak[ing] the Federal Government more transparent and accountable." E-Government Act, Pub. L. No. 107-347, §§ 2(b)(7), (9), (11), 116 Stat. 2899, 2901 (Dec. 17, 2002) (codified at 44 U.S.C. § 3501 note).

In order to "ensure sufficient protections for the privacy of personal information," Section 208 of the E-Government Act requires federal agencies to conduct a privacy impact assessment ("PIA") (1) before "developing or procuring information technology that collects,

maintains, or disseminates information that is in an identifiable form" and (2) before "initiating a new collection of information" in an identifiable form that "will be collected, maintained, or disseminated using information technology" from ten or more persons. *Id.* §§ 208(a)–(b). After the completion of a PIA, the agency must "ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official" and, "if practicable," "make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." *Id.* § 208(b).

A privacy impact assessment must be "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information[.]" *Id.* § 208(b)(2)(B)(i). An assessment must address, in particular:

1. what information is to be collected;
2. why the information is being collected;
3. the intended use of the agency of the information;
4. with whom the information will be shared;
5. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
6. how the information will be secured; and
7. whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the 'Privacy Act').

Id. § 208(b)(2)(B)(ii).

The Office of Management and Budget ("OMB"), which is charged with "oversee[ing] the implementation of the privacy impact assessment process throughout the Government" and "develop[ing] policies and guidelines for agencies on the conduct of privacy impact assessments," *id.* §§ 208(b)(3)(A)–(B), has further clarified the minimum requirements for a privacy impact assessment. The OMB defines a "privacy impact assessment" as

> an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; to determine the risks and effects of creating, collecting, using, processing, storing,

> maintaining, disseminating, disclosing, and disposing of information in identifiable form in an electronic information system; and to examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.

OMB, OMB Circular A-130: Managing Information as a Strategic Resource (2016), app. II at 34 ("OMB Circular").[1] OMB regulations dictate that agencies must complete privacy impact assessments "from the earliest stages of "—and continuously throughout—the information collection process:

> A PIA is one of the most valuable tools Federal agencies use to ensure compliance with applicable privacy requirements and manage privacy risks. Agencies shall conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle. . . .
>
> Moreover, a PIA is not a time-restricted activity that is limited to a particular milestone or stage of the information system or PII life cycles. Rather, the privacy analysis shall continue throughout the information system and PII life cycles. Accordingly, a PIA shall be considered a living document that agencies are required to update whenever changes to the information technology, changes to the agency's practices, or other factors alter the privacy risks associated with the use of such information technology.

Id. at 10. The OMB also requires privacy impact assessments concerning "major information systems" to "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.

Id. § II.C.2.a.ii.

[1] https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/.

B. The United States Postal Inspection Service and the iCOP

The United States Postal Inspection Service ("Postal Inspection Service") is the component of the U.S. Postal Service ("Postal Service") authorized to perform law enforcement functions, including initiating investigations, making arrests, and seizing property. *See* 39 U.S.C. § 404; 18 U.S.C. § 3061. The Postal Service has "adopted policies to comply . . . with the [E-Government] Act's privacy provisions," though the Service states that such compliance is "voluntar[y]." USPS, Handbook AS-353, *Guide to Privacy, the Freedom of Information Act, and Records Management* 2-3.4.[2] These policies "include[] 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." *Id.* The Postal Service has a dedicated template for its privacy impact assessments, which it identifies as "Business Impact Assessments" ("BIAs"). USPS, *Information Resource Business Impact Assessment (BIA)* Version 5.10 (July 27, 2011.[3]

Since at least 2018, the Postal Service has run the Internet Covert Operations Program ("iCOP") with the stated purpose of facilitating "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." Am. Compl. ¶ 21.

But the iCOP's work is not limited to investigating postal crimes, and its intelligence reports are distributed far beyond the Postal Service. In 2020, the iCOP began monitoring racial justice protests. Am. Compl. ¶ 23. In what the Postal Inspection Service terms open-source investigations, "iCOP assigns its analysts to patrol social media to look for information on

[2] https://about.usps.com/handbooks/as353/as353c2_006.htm.
[3] https://about.usps.com/who-we-are/privacy-policy/business-impact-assessment-template.pdf.

upcoming protests and search for potential threats of violence." Am. Compl. ¶ 33. iCOP intelligence bulletins containing social media posts have been distributed across the federal government. Am. Compl. ¶ 34.

To do this, iCOP analysts use sophisticated digital tools to go undercover in various online communities and to identify and track individuals. iCOP analysts have access to the powerful facial recognition and social media monitoring service Clearview AI. Am. Compl. ¶¶ 23, 31. Clearview AI offers a facial recognition product that can search a given image against a database of 3 billion images scraped off of social media sites and provide identifying information. Am. Compl. ¶¶ 24, 25. The iCOP program also experimented with Vigilant Solutions' facial recognition service, which allows for "near-real time video monitoring". Am. Compl. ¶ 26.

iCOP analysts use social media monitoring software from Zignal Labs to identify emerging narratives on social media and track those narratives back to their source. Am. Compl. 28. iCOP also uses on a product called Nfusion from the surveillance technology company Ntrepid to create fake digital identities and infiltrate online communities. Am. Compl. ¶ 29.

Despite initiating numerous information collections and utilizing new information collection systems, the Postal Service and Postal Inspection Service have not completed and published privacy impact assessments for the iCOP program or for its constituent facial recognition and social media monitoring technologies. On May 21, 2021, EPIC sent a Freedom of Information Request on its own behalf and on behalf of its members to Postal Inspection Service 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". Am. Compl. ¶ 42; Am. Compl. Ex. A, ECF

No. 13-1. On June 2, 2021 the Postal Inspection Service issued a final response to EPIC's request confirming that no such PIA existed. Am Compl. ¶ 43; Am. Compl. Ex. B, ECF No. 13-2. No known PIA covering the iCOP or its use of digital surveillance tools has been completed or publicly disclosed.

C. EPIC's lawsuit under the E-Government Act

On August 12, 2021, EPIC filed the instant suit against the United States Postal Service and the United States Postal Inspection Service (collectively "Defendants" or "USPS"). Compl., ECF No. 1. On October 19, 2021, Defendants moved to dismiss EPIC's Complaint. Mot. Dismiss, ECF No. 11. The parties then moved jointly to set a briefing schedule to allow EPIC to file an Amended Complaint. Mot., ECF No. 12. EPIC filed its Amended Complaint on November 9, 2021, ECF No. 13, and Defendants again moved to dismiss on December 7, 2021. ECF No. 14.

In the Amended Complaint, EPIC alleged that Defendants violated the E-Government Act and the Administrative Procedure Act ("APA") in two ways. First, EPIC alleged that USPS engaged in unlawful agency action by operating facial recognition and social media monitoring information collection programs without first conducting and publishing required privacy impact assessments. Am. Compl. ¶¶ 58–65 (Count I). Second, EPIC alleged that Defendants unlawfully withheld agency action by failing to perform the required privacy impact assessments and make them available to EPIC. Am. Compl. ¶¶ 66-72 (Count III). EPIC also alleged that USPS's violations of the E-Government Act are redressable through a writ of mandamus. Am. Compl. ¶¶ 73–78 (Count III).

In their renewed Motion to Dismiss, Defendants contend that EPIC lacks Article III standing to pursue its claims because EPIC has not alleged an injury in fact and because EPIC's

injuries are not redressable by the Court. Mot. Dismiss. 7–15. Defendants also assert that mandamus jurisdiction is not available to EPIC, *id.* 16–18, that EPIC lacks a cause of action under the APA, *id.* 18–19, and that Defendants are not subject to the E-Government Act, *id.* 19–26.

STANDARD OF REVIEW

Where a "claim arises under the laws of the United States," the Court's jurisdiction is established—and a motion under Fed. R. Civ. P. 12(b)(1) defeated—"[u]nless the alleged claim clearly appears to be immaterial and made solely for the purpose of obtaining jurisdiction, or [is] wholly insubstantial and frivolous." *Haddon v. Walters*, 43 F.3d 1488, 1490 (D.C. Cir. 1995). "To survive a Rule 12(b)(1) motion, a plaintiff must establish that the Court has jurisdiction by a preponderance of the evidence." *Lovelien v. United States*, No. 1:19-CV-00906 (TNM), 2019 WL 6117618, at *2 (D.D.C. Nov. 18, 2019) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992)). "When ruling on such a motion, the Court must 'assume the truth of all material factual allegations in the complaint and construe the complaint liberally, granting plaintiff the benefit of all inferences that can be derived from the facts alleged.'" *Id.* (quoting *Am. Nat'l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011)).

To survive a motion to dismiss under Fed. R. Civ. P. 12(b)(6), a complaint need only "contain sufficient factual matter, [if] accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). "In evaluating a Rule 12(b)(6) motion, the Court must construe the complaint in favor of the plaintiff, who must be granted the benefit of all inferences that can be derived from the facts alleged." *Bowser v. Smith*, 314 F. Supp. 3d 30, 33 (D.D.C. 2018) (quoting *Hettinga v. United States*, 677 F.3d 471, 476 (D.C. Cir. 2012)). The Federal Rules of Civil

Procedure "do not require 'detailed factual allegations' for a claim to survive a motion to dismiss," *Banneker Ventures, LLC v. Graham*, 798 F.3d 1119, 1129 (D.C. Cir. 2015) (quoting *Iqbal*, 556 U.S. at 678), but rather "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2).

Though plausibility requires "more than a sheer possibility that a defendant has acted unlawfully," it is not a "probability requirement." *Banneker Ventures*, 798 F.3d at 1129 (quoting *Iqbal*, 556 U.S. at 678). "A claim crosses from conceivable to plausible when it contains factual allegations that, if proved, would 'allow[ ] the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.'" Id. (quoting *Iqbal*, 556 U.S. at 678). "[A] well-pleaded complaint should be allowed to proceed 'even if it strikes a savvy judge that actual proof of [the alleged] facts is improbable, and that a recovery is very remote and unlikely.'" Id. (quoting *Twombly*, 550 U.S. at 556).

ARGUMENT

Defendants' Motion to Dismiss must be denied. First, EPIC has Article III standing to bring its claims. The USPS's unlawful failure to conduct required privacy impact assessments denied EPIC and its members vital information that EPIC would have otherwise obtained—and still intends to obtain—under the E-Government Act and the Freedom of Information Act, 5 U.S.C. § 552. The USPS's use of Clearview AI also caused EPIC's Members cognizable privacy injuries. Both types of injury are redressable by this Court. Second, the E-Government Act applies to the USPS and is not among the statutes from which the USPS is exempt under the Postal Reorganization Act. Third, EPIC has a cause of action under the Administrative Procedure Act because the Postal Inspection Service is not exempt from the APA when performing law

enforcement functions beyond the scope of the Postal Reorganization Act. Finally, even if a cause of action is not available under the APA, EPIC is entitled to mandamus relief.

I. EPIC HAS ESTABLISHED ARTICLE III STANDING.

EPIC has Article III standing to pursue its claims because the USPS's unlawful failure to conduct required privacy impact assessments for the iCOP caused EPIC and its members injuries that are redressable by this Court. To establish standing, EPIC need only demonstrate (1) injury in fact; (2) causation; and (3) redressability. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61(1992). EPIC "need not prove the merits of [the] case[.]" *Id.* at 493. "To survive a motion to dismiss for lack of standing," EPIC must simply "state a plausible claim" of standing. *Williams v. Lew*, 819 F.3d 466, 472 (D.C. Cir. 2016). EPIC has done so here.

A. EPIC and its Members have suffered informational injuries.

The Amended Complaint establishes that EPIC—both as an organization and through its Members—suffered informational injuries cognizable under Article III. A plaintiff suffers an informational injury "when agency action cuts him off from 'information which must be publicly disclosed pursuant to a statute.'" *Waterkeeper All. v. Env't Prot. Agency*, 853 F.3d 527, 533 (D.C. Cir. 2017) (quoting *FEC v. Akins*, 524 U.S. 11, 21 (1998)). To make out an informational injury, a plaintiff must simply show that "(1) it has been deprived of information that, on its interpretation, a statute requires the government or a third party to disclose to it, and (2) it suffers, by being denied access to that information, the type of harm Congress sought to prevent by requiring disclosure." *Friends of Animals v. Jewell*, 828 F.3d 989, 992 (D.C. Cir. 2016).

Here, EPIC and its Members suffered informational injuries because the USPS's failure to produce timely privacy impact assessments required by the E-Government Act "cut[EPIC] off from 'information which must be publicly disclosed pursuant to" the FOIA. *Waterkeeper All.*,

853 F.3d at 533. Although section 208 of the E-Government Act does not "vest a general right to information in the public," the FOIA "was designed to grant enforceable rights to information in the general public." *EPIC v. Commerce*, 928 F.3d 95, 103 (D.C. Cir. 2019); *see also TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2214 (2021) (noting that "public-disclosure or sunshine laws" like the FOIA "entitle all members of the public to certain information"). In contrast to *EPIC v. Commerce*—in which EPIC relied solely on the publication requirement of section 208—the USPS's failure to create required PIAs in this case prevented EPIC from accessing information that it would have otherwise obtained through its FOIA requests. Compl. ¶¶ 42–53.

The D.C. Circuit established in in *Waterkeeper Alliance* that informational injuries can arise from the interaction of two different statutes. 853 F.3d 527. In *Waterkeeper*, a group of environmental plaintiffs challenged an Environmental Protection Agency ("EPA") rule that would exempt certain factory farmers from reporting airborne animal waste discharges to the EPA as required by the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 ("CERCLA"). CERCLA contains no requirement that reports submitted under its provisions be disclosed to the public. *Id*. at 531. But another statute, the Emergency Planning and Community Right-to-Know Act of 1986 ("EPCRA"), requires both reporting of similar discharges of harmful chemicals and the public disclosure of those discharges. *Id*. CERCLA's reporting requirement provided the information that would ultimately be made available to the plaintiffs under EPCRA. *Id*. Accordingly, the D.C. Circuit held that by exempting factory farms from a requirement under CERCLA, the EPA "deprive[d] Waterkeeper of information, the public disclosure of which would otherwise be required by EPCRA." *Id*. at 534. The plaintiffs had therefore suffered an informational injury sufficient for Article III standing.

So too here. Section 208 of the E-Government Act requires agencies to compile a privacy impact assessment—a type of agency record—prior to collecting personal information or procuring information technology that will process personal information. That requirement was triggered by the USPS's acquisition and use of facial recognition, social media analysis, and covert intelligence gathering tools under the iCOP. Am. Compl. ¶¶ 35–36. Had the USPS fulfilled its PIA obligations, the FOIA would have "require[d] the government . . . to disclose" the resulting agency records—i.e., privacy impact assessments—in response to EPIC's repeated requests. *See Friends of Animals* 828 F.3d at 992; *see also id.* (noting that "[plaintiff's] interpretation" of the disclosure statute controls for the purposes of Article III standing). But because the USPS failed to create the privacy impact assessments under the E-Government Act, EPIC was denied information which by law it should have received under the FOIA. "For the purpose of standing, that's injury enough." *Waterkeeper All.,* 853 F.3d at 533.

Defendants assert that the *Waterkeeper* framework does not apply because section 208 and the FOIA "govern entirely different subject matter" and lack the "complex interplay" of the statutes at issue in *Waterkeeper*. Mot. Dismiss 11 (quoting *Jud. Watch, Inc. v. Off. of Dir. of Nat'l Intel.*, No. 1:17-CV-00508 (TNM), 2018 WL 1440186, at *4 (D.D.C. Mar. 22, 2018); *Waterkeeper All.,* 853 F.3d at 533). In *Judicial Watch*, this Court distinguished the statutes in *Waterkeeper* from the FOIA and Intelligence Community Directive 732, which requires the creation of damage assessments when classified information is disclosed. *Id*. But Defendants' reliance on *Judicial Watch* is misplaced. Unlike the statutes at issue in *Judicial Watch*, the FOIA and the E-Government Act do not "govern entirely distinct subject matter [or] have polar opposite purposes." *Id*. Section 208—like the FOIA—requires the publication of agency records subject to narrow exceptions. § 208(b)(1)(B)(iii) (requiring privacy impact assessments to be

made "publicly available through the website of the agency, publication in the Federal Register, or other means" so long as "practicable"). Indeed, agencies can even comply with the E-Government Act's publication directive by disclosing records pursuant to a FOIA request. Public access to information is also among the core purposes of the E-Government Act, which include "promot[ing] access to high quality Government information and services across multiple channels," "mak[ing] the Federal Government more transparent and accountable, and "provid[ing] enhanced access to Government information and services[.]" E-Government Act § 2(b). Section 208 of the E-Government Act and the FOIA are thus far from "polar opposite[s]," but rather statutes that seek to achieve the same goal of public disclosure.

Accordingly, Defendants' failure to conduct required privacy impact assessments frustrated EPIC's attempts to obtain the assessments under the FOIA, causing EPIC to suffer a cognizable informational injury.

B. EPIC's Members have suffered privacy injuries.

EPIC also has demonstrated injury in fact by virtue of the privacy harms suffered by its Members, whose "name[s] and/or image[s] are likely contained" in the Clearview AI database unlawfully used by the USPS. Am. Compl. Ex. D ¶ 9; Am. Compl. Ex. E ¶ 9. Because "EPIC is a membership organization," *EPIC v. Commerce*, 928 F.3d at 101, it may generally sue on behalf of its Members if one of those Members has suffered a redressable injury in fact caused by the defendant. *Am. Library Ass'n v. FCC*, 401 F.3d 489, 492–93 (D.C. Cir. 2005); *see also Conference of State Bank Supervisors v. Office of Comptroller of Currency*, 313 F. Supp. 3d 285, 294 (D.D.C. 2018).

"To plausibly show a privacy injury" in the context of the E-Government Act, "EPIC must allege harm that is distinct from a simple failure to comply with the procedural

requirements of § 208." *EPIC v. Commerce*, 928 F.3d at 102. Although the D.C. Circuit has said that "in the privacy context, such harm would *ordinarily* stem from the disclosure of private information," *id.* (emphasis added), the Supreme Court recently underscored that government collection of personal information can work concrete harm "[e]ven if there [is] no disclosure to the general public." *Americans for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2388 (2021) (quoting *Shelton v. Tucker*, 364 U.S. 479, 486 (1960)). That is precisely the scenario here.

Two of EPIC's Members in particular—Woodrow Hartzog and Adrian Gropper—maintain social media profiles containing their images and personal information. Am. Compl. Ex. D ¶ 9; Am. Compl. Ex. E ¶ 9. Those Members are highly likely to be in Clearview AI's facial recognition database of more than 3 billion faces, which was constructed through the systematic scraping of images and profile data from major social media platforms. Am. Comp. ¶¶ 24, 25. Clearview AI's facial recognition product works by taking an image of an unknown individual, converting it into a facial recognition template, and comparing that template against the billions of templates Clearview AI already has in its database. *Id*. Provided (as is likely) that images of EPIC's Members are contained in the Clearview AI database, any use of Clearview AI by USPS would necessarily have involved the comparison of images against facial recognition templates extracted from EPIC's Members. Am. Compl. ¶¶ 63, 71. Further, EPIC's members were active on social media in 2020 at a time when iCOP agents were known to have patrolled Twitter, Facebook, and other websites for information about protests. *Id*. Because USPS procured and used information technology that likely processed the personal information of EPIC's Members—yet failed to first conduct a required analysis of the resulting privacy risks—EPIC's Members have alleged privacy injury sufficient for Article III standing.

Indeed, EPIC's Members are precisely the types of individuals section 208 is meant to protect: those whose privacy is imperiled by the USPS's collection and use of their personal information. *See* E-Government Act § 208(a). Section 208 imposes privacy obligations on federal agencies and directs agencies to publish privacy impact assessments to allow affected individuals to assess the risks to their privacy imposed by agency action. Without the required assessments for Clearview AI and other iCOP surveillance tools, EPIC's Members have been denied "a full and timely assessment of how their privacy interests would and will be affected." Am. Compl. ¶¶ 72. EPIC's Members are therefore likely to have suffered "the type of harm that Congress sought to prevent by requiring disclosure." *Friends of Animals v. Jewell*, 828 F.3d 989, 992 (D.C. Cir. 2016).

C. The injuries to EPIC and its Members are redressable by this Court.

Contra Defendants, EPIC's informational and privacy injuries are redressable by this Court. To meet this requirement of Article III, redress of EPIC's injuries need only be "likely" rather than "speculative." *Lujan*, 504 U.S. at 561. As previously explained, an order directing the USPS to conduct the required privacy impact assessments for the iCOP program would make those impact assessments available through the FOIA, thereby redressing EPIC's informational injury. EPIC's Complaint also identifies several other remedies—including an injunction or writ of mandamus compelling Defendants to publish and disclose privacy impact assessments for the iCOP program and an order halting the operation of the iCOP program until Defendants comply with the requirements of the E-Government Act—that would redress both the informational and privacy injuries suffered by EPIC and its Members. Am. Compl. 20 ("Requested Relief").

Nevertheless, Defendants assert that EPIC's injuries are not redressable. Mot. Dismiss 14 Defendants point to the language of section 208 to argue that, even if ordered to produce privacy

impact assessments, the Postal Service could decide not to disclose the assessment or so thoroughly redact the document that EPIC would learn nothing about the iCOP program. *Id.* at 15. But as noted, EPIC's informational injury arises from the USPS's failure to disclose under the FOIA records that should have been created pursuant to the E-Government Act. For the purposes of an Article III standing analysis, EPIC's "view of the law" is decisive, *FEC v. Akins*, 524 U.S. 11, 21 (1998), and EPIC has plausibly asserted that it would obtain pursuant to the FOIA some or all of the privacy impact assessments ordered by this Court. Defendants' argument thus fails.

Moreover, even given the iCOP's law enforcement mission, some amount information about surveillance conducted under the iCOP could almost certainly be disclosed without risking the program's "effectiveness." Mot. Dismiss 15. Given the scant public record on the iCOP, even the most basic information about USPS's use of facial recognition technology and social media monitoring tools would substantially add to EPIC's (and the public's) understanding of the program.

Finally, Defendants do not even engage with the other relief requested in EPIC's Complaint. For example, a halt of iCOP's operations until the USPS's privacy impact assessment process is complete would certainly mitigate the risk of ongoing privacy harms to EPIC's Members. *See* Am. Compl. 20. Accordingly, EPIC has demonstrated the redressability of its injuries by this Court and established standing under Article III.

II. THE POSTAL SERVICE IS SUBJECT TO THE E-GOVERNMENT ACT.

Defendants argue that both the Postal Reorganization Act and the Paperwork Reduction Act (from which the E-Government Act borrows its definition of "agency") excuse the USPS

from the privacy impact assessment obligations applicable to nearly every other federal agency. Neither argument is availing.

First, although 39 U.S.C. § 410(a) lays out numerous categories of federal law that the USPS is generally exempt from, those categories do include statutes like the E-Government Act. Congress could have easily dictated that exercise of the Postal Service's powers would be exempt from *all* federal statutes; instead, the exemption extends only to laws "dealing with public or Federal contracts, property, works, officers, employees, budgets, or funds, including the provisions of chapters 5 and 7 of title 5[.]" 39 U.S.C. § 410(a). Indeed, that Congress believed it necessary to list two particular sections of Title 5 in § 410(a) demonstrates that some federal statutes are still beyond the broad exemptive language of the provision. *See Nat'l Easter Seal Soc. for Crippled Child. & Adults v. USPS*, 656 F.2d 754, 766 (D.C. Cir. 1981).

The E-Government Act is one such law. Congress enacted the E-Government Act chiefly to "enhance citizen access to Government information and services[.]" E-Government Act pmbl. The E-Government Act is an information disclosure statute intended to open the cybersecurity and information collection practices of the federal government to public scrutiny. Section 208, in particular, was intended to ensure the protection of privacy. Neither of these purposes suggests the statute is one concerning "public or Federal contracts, property, works, officers, employees, budgets, or funds"; instead, the statute is intended to provide certain information and protections to the public. 39 U.S.C. § 410(a). Thus the USPS cannot escape coverage of the E-Government Act.

Defendants' alternative argument—that the U.S. Postal Service does not even constitute an agency to begin with under the E-Government Act—also falls flat. The E-Government Act

imposes privacy impact assessment obligations on "agenc[ies]," E-Government § 208, a term which draws its meaning from the Paperwork Reduction Act's definition of "agency":

> (1) the term "agency" means any executive department, military department, Government corporation, Government controlled corporation, or other **establishment in the executive branch of the Government** (including the Executive Office of the President), or any independent regulatory agency, but does not include—
>
> (A) the Government Accountability Office;
> (B) Federal Election Commission;
> (C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or
> (D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities;

44 U.S.C. § 3502(1). As Defendants note, the Postal Service is defined as "an independent establishment of the executive branch of the Government of the United States," 39 U.S.C. § 201—language which evinces clear Congressional intent to bring the Postal Service within the definition of an "agency" under § 3502(1).

Defendants raise a variety of arguments to counter the plain-text conclusion that the Postal Service qualifies as an agency within the meaning of the Paperwork Reduction Act and E-Government Act. But as this Court has previously suggested, the phrase "establishment in the executive branch" in one statutory provision is best read to carry the same meaning as "establishment of the executive branch" in another. *See EPIC v. Nat'l Sec. Comm'n on Artificial Intelligence*, 419 F. Supp. 3d 82, 86 (D.D.C. 2019) (quoting *Energy Research Found. v. Def. Nuclear Facilities Safety Bd.*, 917 F.2d 581, 582–83 (D.C. Cir. 1990)). ("It would be a tall piece of statutory construction' . . . 'to say that an 'establishment in the executive branch' as used in § 2286(a) is not an 'establishment in the executive branch' within the meaning of § 552(f).'"). As it has done before, the Court should reject Defendants' invitation "like a stranger offering candy to a child . . . not to read [the law] literally," *EPIC v. Nat'l Sec. Comm'n on Artificial Intelligence*,

419 F. Supp. at 87 (D.D.C. 2019), and hold that the Postal Service is an agency subject to the E-Government Act.

III. EPIC HAS A CAUSE OF ACTION UNDER THE APA.

The Administrative Procedure Act provides a cause of action to EPIC. 5 U.S.C. § 702. Defendants' sole challenge to judicial review under the APA is that the APA does not apply to actions (or failures to take required action) by the Postal Inspection Service. But the language of 39 USC § 410(a) does not excuse the Postal Inspection Service from judicial review under the APA when it exercises its law enforcement powers outside the scope of the Postal Reorganization Act, as it did in operating the iCOP.

As noted, the Postal Reorganization Act provides that "no Federal law dealing with public or Federal contracts, property, works, officers, employee, budgets, or funds, including the provisions of chapter 5 and 7 of title 5, shall apply *to the exercise of the powers of the Postal Service*." 39 USC § 410(a) (emphasis added). In construing this provision, the D.C. Circuit has recognized that the business activities of the Postal Service cannot be challenged under the APA. *N. Air Cargo v. USPS*, 674 F.3d 852, 858 (D.C. Cir. 2012) (holding that plaintiffs lacked a cause of action under the APA to challenge the decision of USPS to authorize certain air carriers to operate in remote areas of Alaska); *Nat'l Easter Seal Soc'y v. USPS*, 626 F.2d 754 (D.C. Cir. 1981) (holding USPS's decision to deviate from approved rates for certain classes of mail exempt from the APA). But the exemptions of § 410(a) end at the limit of "the exercise of the powers of the Postal Service." *Am. Postal Workers Union, AFL-CIO v. Bush*, 588 F. Supp. 2d 5, 7 (D.D.C. 2008) (holding that the strictures of the FACA applied to and superseded a section of the Postal Reorganization Act creating an advisory council for the Postal Service).

The U.S. Postal Inspection Service operates under both the limited grant of authority in 39 U.S.C. §404(a)(6) and under the general law enforcement authority of the federal government 18 U.S.C. § 3061. Section 404(a) of the PRA grants the Postal Inspection Service the specific power "to investigate postal offenses and civil matters relating to the Postal Service." Significantly, the PRA's grant of law enforcement is confined to 39 U.S.C. § 404 ("Specific powers") and not set out in 39 U.S.C. § 401 ("General powers of the Postal Service") The Postal Inspection Service's law enforcement powers are bounded under the PRA.

But the Postal Inspection Service also operates under the authority of Title 18, which provides for the Service's law enforcement powers to serve warrants, make arrests with or without a warrant, carry firearms, and seize property. 18 U.S.C. § 3061(a). Postal inspectors may use those powers, "in the enforcement of laws regarding property in the custody of the Postal Service, property of the Postal Service, the use of the mails, and other postal offenses." 18 U.S.C. § 3061(b)(1). Postal inspectors may also use those powers when "authorized by the Attorney General pursuant to agreement between the Attorney General and the Postal Service, in the enforcement of other laws of the United States". 18 U.S.C. § 3061(b)(2). When the Service acts pursuant to that broader authority, it is not exercising "the powers of the Postal Service" within the meaning of 39 USC § 410(a). Rather, it is exercising an independent grant of law enforcement authority distinct from the "powers of the Postal Service." Because these activities fall outside the exemption in 39 U.S.C. § 410(a), judicial review remains available under the Administrative Procedure Act.

At least some of the iCOP's activities appear to fall under the Postal Inspection Service's broader grant of authority under Title 18. In March 2021, the iCOP disseminated a bulletin across the federal government. Am. Compl. ¶ 34. The bulletin contained intelligence gleaned by

iCOP from Facebook groups, Twitter, and Parler describing possible nationwide protests against the rollout of 5G wireless internet. *Id*. That bulletin did not identify any specific threat to or impact on Postal Service activities.

The systems for which EPIC is seeking privacy impact assessments—the social media monitoring and facial recognition tools used under iCOP—were apparently used in furtherance of the Postal Inspection Service's broader law enforcement authorities. Because those activities are subject to the APA, EPIC has a cause of action and may obtain judicial review under 5 U.S.C. § 702.

IV. IF APA REVIEW IS UNAVAILABLE, EPIC IS STILL ENTITLED TO MANDAMUS RELIEF.

If the Court determines that EPIC lacks a cause of action under the APA, EPIC is nevertheless entitled to relief the under Mandamus and Venue Act, 28 U.S.C. § 1361. The Court may grant mandamus if "(1) the plaintiff has a clear right to relief; (2) the defendant has a clear duty to act; and (3) there is no other adequate remedy available to plaintiff." *Baptist Mem'l Hosp. v. Sebelius*, 603 F.3d 57, 62 (D.C. Cir. 2010). EPIC's claim for a writ of mandamus meets all three criteria.[4]

The E-Government Act imposes a clear duty on agencies—including the Postal Service and the Postal Inspection Service—to conduct, review, and in most cases publish a privacy impact assessment prior to collecting personal information or procuring information technology that will process personal information. *See* E-Government Act § 208(b)(1)(A) ("An agency *shall*

[4] While Defendants are correct that this Court's mandamus powers are governed by Rule 81(b) of the Federal Rules of Civil Procedure, Mot. Dismiss 16, courts continue to refer to the grant of mandamus relief as a writ. *See e.g.*, Order at 1, *EPIC v. National Security Commission on Artificial Intelligence*, 466 F. Supp. 3d 100 (D.D.C. 2020) ("ORDERED that writs of mandamus hereby issue to the National Security Commission on Artificial Intelligence and its officers[.]").

take actions described under subparagraph (B)…."); *id.* § 208(b)(1)(B) ("To the extent required under subparagraph (A), each agency shall…."). As explained above, *supra* I.A–B, the duties imposed by section 208 exist in part for the benefit of individuals for whose "privacy of personal information" is implicated by agency activities and information technology, including in this case EPIC's Members. E-Government Act § 208(a). Therefore, relief is owed to EPIC and its members. And if the Court holds that judicial review is unavailable to EPIC under the APA, no other adequate remedy will be available.

Defendants challenge EPIC's right to mandamus relief on the view that the Postal Inspection Service has no "clear and undisputable" duty to act. Mot. Dismiss 16–17 (quoting *13th Regional Corp. v. Dep't of the Interior*, 654 F.2d 758, 760 (D.C. Cir. 1980)). Not so. First, while "the term 'duty' as used in section 1361 'must be narrowly defined . . . [t]his does not mean that mandamus actions are ruled out whenever the statute allegedly creating the duty is ambiguous.'" *Lovitky v. Trump*, 949 F.3d 753, 760 (D.C. Cir. 2020) (quoting *In re Cheney*, 406 F.3d 723, 729 (D.C. Cir. 2005)) Second, the commands of the E-Government Act could hardly be more "clear and unambiguous": before initiating a new information collection or procuring information technology that will process personal information, an agency "shall" conduct, review, and in most cases publish a privacy impact assessment. These obligations leave little room for agency discretion.

Defendants also argue that the existence of narrow exceptions to the section 208 disclosure requirement—when disclosure is not "practicable" or when an assessment must be withheld to "for security reasons, or to protect classified, sensitive, or private information contained in an assessment"—mean that the E-Government Act imposes no clear duty susceptible to mandamus jurisdiction. Mot. Dismiss 17 (quoting E-Government Act §§

208(b)(1)(B)(iii), (b)(1)(C)). But a duty that has substantive limitations is still a duty. Defendants had a duty to create a privacy impact assessment under the E-Government Act and a duty to provide that assessment EPIC under both the E-Government Act and the FOIA, subject to any applicable exemptions. Here, as in *EPIC v. National Security Commission on Artificial Intelligence*, 466 F. Supp. 3d 100, 123 (D.D.C. 2020), the fact that Defendants might be able to invoke an exemption to withhold some information does not give them blanket relief from the mandatory duty of disclosure. In *National Security Commission*, the mere availability of FOIA exemptions to the Commission did not negate EPIC's right to mandamus relief requiring the Commission to disclose documents under the FACA. *See id.* at 123. Nor is EPIC's claim a "generalized grievance": EPIC actually sought the required privacy impact assessments through the USPS's FOIA process, and EPIC's members were likely subject to processing of personal information by the Postal Service for which a PIA is required.

Whether the Postal Inspection Service has enacted safeguards to protect the public while using highly invasive surveillance technologies to monitor sensitive activities is a matter of immense public concern. This case is one of the "extraordinary situations" in which mandamus relief is necessary and merited. *In re Cheney*, 334 F.3d 1096, 1101-02 (D.C. Cir. 2003).

CONCLUSION

For the above reasons, Defendants' Motion to Dismiss EPIC's Amended Complaint should be denied.

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
davisson@epic.org

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

Dated: January 4, 2022