IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. UNITED STATES DEPARTMENT OF COMMERCE, et al., Defendants.	Civ. Action No. 18-2711 (DLF)

PLAINTIFF'S OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Constitutional Provisions

Other Authorities

SUMMARY

The Electronic Privacy Information Center ("EPIC") hereby respectfully opposes the Defendants' Motion to Dismiss, ECF No. 20, which must be denied. EPIC has plausibly alleged that the U.S. Department of Commerce and U.S. Census Bureau failed to conduct required privacy impact assessments prior to initiating the collection of citizenship status information via 2020 Census, a violation of section 208 the E-Government Act. Moreover, EPIC has Article III standing to bring these claims because EPIC's Members have been unlawfully denied critical information about the privacy risks posed by Defendants' imminent acquisition of their personal citizenship data. At this preliminary stage of the case, that is all EPIC must demonstrate.

Unique among federal agencies, the Census Bureau is authorized by law to compel—from every person in the United States—personal data including age, sex, race, ethnicity, family relationships, and homeownership status. The extraordinary reach of the Bureau into the private lives of Americans brings extraordinary risks to privacy. Accordingly, "Congress has provided assurances that information furnished to the [Census Bureau] by individuals is to be treated as confidential." *Baldrige v. Shapiro*, 455 U.S. 345, 354 (1982) (citing 13 U.S.C. §§ 8(b), 9(a)). These legal obligations, enacted by Congress, include the provisions of the E-Government Act, which require the Census Bureau to conduct and publish privacy impact assessments *before* initiating the collection of personal data.

But the Census Bureau has failed to comply with the law. The Bureau decided to collect sensitive personal data from more than a hundred million Americans—the apex of the assessment obligation envisioned by Congress—yet refused to undertake the necessary review mandated by the E-Government Act. As a result, the Bureau has denied EPIC access to

information vital to assess the privacy consequences of the Bureau's decision and has unduly jeopardized the privacy of EPIC's Members.

Because EPIC's Complaint alleges ample facts to conclude that Defendants have violated their privacy impact assessment obligations, thereby causing injury to EPIC's Members, the Court should deny Defendants' Motion to Dismiss.

BACKGROUND

I. 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). Among the "constituencies" accounted for in the Act are "the public access community," "privacy advocates," and "non-profit groups interested in good government." 148 Cong. Rec. 11,228 (2002) (statement of Sen. Lieberman).

In order to "ensure sufficient protections for the privacy of personal information," section 208 of the E-Government Act requires federal agencies to complete and publish a privacy impact assessment ("PIA") prior to "initiating" the process of collecting personal data. §§ 208(a)–(b). Specifically, "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, the agency must "conduct a privacy impact assessment"; "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). The agency must also "provide the Director [of the Office of Management and Budget] with a copy of the privacy

impact assessment" whenever "funding is requested" for a system of information. *Id.* § 208(b)(1)(D).

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:

> (I) what information is to be collected;
> (II) why the information is being collected;
> (III) the intended use of the agency of the information;
> (IV) with whom the information will be shared;
> (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
> (VI) how the information will be secured; and
> (VII) 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") 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). Accordingly, the OMB has clarified the minimum requirements for a privacy impact assessment and the role of privacy impact assessment in an agency's decision to collect (or to refrain from collecting) personal data.

OMB regulations dictate that agencies must complete privacy impact assessments "from the earliest stages of"—and continuously throughout—the information collection process: 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.

OMB, OMB Circular A-130: Managing Information as a Strategic Resource (2016), app. II at 10 ("OMB Circular").[1] 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.

Id. at 34. The OMB instructs that "PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA." Prelim. Inj. Mem. Ex. 15, ECF No. 8-7, Joshua B. Bolten, Dir., OMB, Executive Office of the President, M03-22, Memorandum for Heads of Executive Departments and Agencies, attachment A § II.C.1.b (Sept. 26, 2003) ("OMB Guidance").

According to the OMB, "Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection[.]" *Id.* § II.C.2. At this initial stage, a privacy impact assessment

> 1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;

[1] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) [of the OMB Guidance], to the extent these elements are known at the initial stages of development;
3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.

Id. § II.C.2.a.i. 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.

As the OMB explains, "the E-Government Act requires agencies to conduct a PIA before . . . initiating, *consistent with the Paperwork Reduction Act*, a new electronic collection of information in identifiable form for 10 or more persons." *Id.* § II.B.1.b (emphasis added). The Paperwork Reduction Act, 44 U.S.C. §§ 3501 *et seq.* ("PRA")—like the E-Government Act—is intended to "strengthen decisionmaking, accountability, and openness in Government and society[.]" 44 U.S.C. § 3501(4). The PRA requires an agency to conduct, review, publish, and submit to the OMB an assessment of paperwork burdens on the public whenever the agency introduces a collection of information. 44 U.S.C. §§ 3506(c), 3507(a)(1). Later, after the OMB has reviewed the required documentation for the agency's collection of information—and after OMB approval is granted or inferred—the agency may begin actually collecting data from the public. 44 U.S.C. §§ 3507(a), (a)(2). The E-Government Act borrows the PRA's definition of "collection of information," which means

> the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either--
>
> (i) answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States; or
>
> (ii) answers to questions posed to agencies, instrumentalities, or employees of the United States which are to be used for general statistical purposes[.]

44 U.S.C. § 3502(3)(A); *see also* E-Government Act § 201 ("Except as otherwise provided, in this title the definitions under sections 3502 and 3601 of title 44, United States Code, shall apply.").

The OMB has identified several specific events that "create[] new privacy risks" and that must not occur until *after* the agency has completed a new or revised privacy impact assessment. OMB Guidance § II.B.2. These include an agency's "adopt[ion] or alter[ation of] business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated," *Id.* § II.B.2.d; "agencies work[ing] together on shared functions involving significant new uses or exchanges of information in identifiable form," *Id.* § II.B.2.g; and "changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form." *Id.* § II.B.4.

II. The Department of Commerce order initiating the collection of personal data concerning citizenship status

In order to determine the apportionment of representatives "among the several States," the Census Clause of the U.S. Constitution, as amended, requires that an "actual Enumeration" of persons be undertaken every ten years "in such Manner as [Congress] shall by Law direct." U.S. Const. art. 1, § 2, cl. 3; *see also* U.S. Const. amend. XIV, § 2 ("Representatives shall be apportioned among the several States according to their respective numbers, counting the whole number of persons in each State, excluding Indians not taxed.").

In furtherance of the Census Clause, Congress has directed the Secretary of Commerce to "take a decennial census of population," 13 U.S.C. § 141(a), and to "determine the inquiries, and the number, form, and subdivisions" of the questionnaires to be used in the census. 13 U.S.C. § 5. Congress has also established the Census Bureau as an agency under the Department of Commerce. 15 U.S.C. § 1501. The Department of Commerce and the Bureau (collectively, "Defendants," "the Census Bureau," or "the Bureau") will administer the next Census in 2020. *See* U.S. Census Bureau, *2020 Census* (Oct. 19, 2018).[2] By law, any person who refuses to answer "any of the questions . . . submitted to him in connection with any census"—or who willfully gives a false answer to a census question—is subject to criminal penalties. 13 U.S.C. § 221(a)–(b).

On March 26, 2018, Secretary of Commerce Wilbur Ross stated that he "ha[d] determined that reinstatement of a citizenship question on the 2020 decennial census [wa]s necessary" and that he was "directing the Census Bureau to place the citizenship question last on the decennial census form." Compl. ¶ 30; *see also* Prelim. Inj. Mem. Ex. 1, ECF No. 8-4, Letter from Wilbur Ross, Secretary of Commerce, to Karen Dunn Kelley, Under Secretary for Economic Affairs, at 8 (Mar. 26, 2018) ("Ross Letter"). No such question appeared on the 2010 Census, nor has the Bureau posed a citizenship question to all census respondents since 1950. Compl. ¶ 30. Secretary Ross stated that the citizenship question was added in response to a December 2017 request by the Department of Justice ("DOJ"), which allegedly sought citizenship data to enable "more effective enforcement" of the Voting Rights Act. *Id*. Secretary Ross's explanation for his decision is at odds with the extensive evidence uncovered in litigation

[2] https://www.census.gov/programs-surveys/decennial-census/2020-census.html.

over the citizenship question. *See New York v. U.S. Department of Commerce*, 351 F. Supp. 3d 502, 517–18 (S.D.N.Y. 2019).

On March 28, 2018, the Bureau officially reported to Congress its intention to add a citizenship question to the 2020 Census. Compl. ¶ 32; *see also* Prelim. Inj. Mem. Ex. 2, ECF No. 8-4, U.S. Census Bureau, *Questions Planned for the 2020 Census and American Community Survey* 7 (March 2018). The version of the question presented to Congress asked: "Is this person a citizen of the United States?" Compl. ¶ 32. Five responses were listed: "Yes, born in the United States"; "Yes, born in Puerto Rico, Guam, the U.S. Virgin Islands, or Northern Marianas"; "Yes, born abroad of U.S. citizen parent or parents"; "Yes, U.S. citizen by naturalization – *Print year of naturalization*"; and "No, not a U.S. Citizen[.]" *Id.*

III. The privacy implications of collecting citizenship status information

Although the Census Bureau's collection of personally identifiable information carries inherent privacy risks, the addition of a citizenship question to the 2020 Census poses a unique threat to privacy, personal security, and the accuracy of the census. The citizenship question would compel the disclosure of respondents' citizenship status—and by extension, the immigration status of many respondents—which could in turn expose individuals and their family members to investigation, sanction, and deportation.

Secretary Ross's stated basis for adding the citizenship question was to provide the DOJ with "census block level citizen voting age population ('CVAP') data," Compl. 38—data that is susceptible to reidentification. Compl. ¶ 42; *see also* Prelim. Inj. Mem. Ex. 3, ECF No. 8-4, Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000). The Bureau has indicated that census response data—including individuals' citizenship status information—may be transferred in "[b]ulk" to other federal agencies "[f]or criminal law enforcement activities." Compl ¶ 39; *see also* Prelim.

Inj. Mem. Ex. 6, ECF No. 8-4, U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN08 Decennial Information Technology Division (DITD)* at 5, 7, 9 (approved Sep. 28, 2018). And in a June 12, 2018 email exchange between DOJ officials, disclosed in the course of litigation against Secretary Ross, DOJ officials "privately discussed the possibility that in the future census information could be shared with law enforcement." Compl. ¶ 40.

Historically, the misuse of census data has caused considerable harm to the public, particularly to vulnerable populations. Compl. ¶¶ 43–44. The law governing the 1910 census prohibited the use of information supplied by businesses for non-statistical, non-census purposes, but there was no such prohibition regarding individual citizen data. Act of Jul. 2, 1909 (to provide for the expenses of the Thirteenth December Census, and for other purposes), ch. 2, § 25, 36 Stat. 1, 9. As a result, the Census Bureau was able to disclose census records to the Department of Justice and local draft boards during World War I. Margo Anderson & William Seltzer, *Challenges to the Confidentiality of U.S. Federal Statistics, 1910-1965*, 23 J. Official Stat. 1, 6–7 (2007). Similarly, in 1920, the Department of Justice requested census data about individuals' citizenship for use in deportation cases. *Id.* at 8–9.

In 1930, Congress passed a census statute prohibiting the Bureau from publishing any data identifying individuals. Act of June 18, 1929 (to provide for the fifteenth and subsequent decennial censuses and to provide for apportionment of Representatives in Congress), ch. 28, § 11, 46 Stat. 21, 25. Yet the Second War Powers Act weakened this restriction and permitted the Bureau in 1943 to provide the U.S. Secret Service with the names, addresses, occupations, and citizenship status of every Japanese American residing in the Washington, D.C. area. Margo Anderson & William Seltzer, *Census Confidentiality Under the Second War Powers Act (1942–1947)* at 16 (Mar. 31, 2007) (unpublished manuscript). The Bureau also provided the War

Department with census-block level data on Japanese Americans residing in western states to facilitate their internment. Comm'n on Wartime Relocation and Internment of Civilians, *Personal Justice Denied* 104-05 (1982).[3]

In 2004, an EPIC Freedom of Information Act ("FOIA") request revealed that the Census Bureau had provided the Department of Homeland Security with a list of cities containing more than 1,000 Arab-American residents and a ZIP code-level breakdown of Arab-American populations throughout the United States, sorted by country of origin. Compl. ¶ 45 (citing EPIC, *Department of Homeland Security Obtained Data on Arab Americans From Census Bureau* (2004);[4] Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*, N.Y. Times (Jul. 30, 2004)).[5] The Census Bureau and U.S. Customs and Border Protection revised their data request policies following EPIC's FOIA case. Compl. ¶ 45 (citing Lynette Clemetson, *Census Policy On Providing Sensitive Data Is Revised*, N.Y. Times (Aug. 31, 2004);[6] U.S. Customs and Border Protection, *Policy for Requesting Information of a Sensitive Nature from the Census Bureau* (Aug. 9, 2004)).[7]

Many Americans remain fearful that their census responses will be "used against them or their loved ones" by federal agencies. *New York*, 351 F. Supp. 3d at 515. As the Census Bureau has previously acknowledged, "[q]uestions as to citizenship are particularly sensitive in minority communities and would inevitably trigger hostility, resentment and refusal to cooperate." *Fed'n for Am. Immigration Reform v. Klutznick*, 486 F. Supp. 564, 568 (D.D.C. 1980). This has

[3] https://www.archives.gov/files/research/japanese-americans/justice-denied/chapter-3.pdf.
[4] https://epic.org/privacy/census/foia/.
[5] https://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html.
[6] https://www.nytimes.com/2004/08/31/us/census-policy-on-providing-sensitive-data-is-revised.html.
[7] https://epic.org/privacy/census/foia/policy.pdf.

consequences for the accuracy of census data. Fear over the misuse of census responses can lead individuals to provide false or incomplete information, which "harms the quality of the census count, and would [result in] substantially less accurate citizenship status data than are available from" other government sources. Compl. ¶ 46; *see also* Prelim. Inj. Mem. Ex. 4, ECF No. 8-4, Memorandum from John M. Abowd, Chief Scientist, U.S. Census Bureau, to Wilbur L. Ross, Sec'y of Commerce, at 1 (Jan. 19, 2018); *Fed'n for Am. Immigration Reform*, 486 F. Supp. at 568 ("[A]ccording to the Bureau; any effort to ascertain citizenship will inevitably jeopardize the overall accuracy of the population count.").

IV. The lack of privacy impact assessments analyzing the citizenship question

As this Court previously noted, Defendants concede that they must "prepare PIAs that adequately address the collection of citizenship data in the 2020 Census." Mem. Op. 6, ECF No. 17 (citing Defs.' Opp'n to Pl.'s Mot. for Prelim. Inj. at 1, 12, ECF No. 12). At present, none of the privacy impact assessments published by the Bureau address the citizenship question that Secretary Ross chose to add to the 2020 Census. Compl. ¶ 52.

When the Census Bureau produces a privacy impact assessment concerning Bureau activities, the assessment is published on the Bureau's privacy impact assessment webpage. Compl. ¶ 48 (citing Dep't of Commerce, Office of Privacy & Open Gov't, *U.S. Census Bureau Privacy Impact Assessments (PIAs) and Privacy Threshold Analysis (PTA)* (Oct. 1, 2018)).[8] This webpage lists Census Bureau systems and divisions that collect, process, and store personally identifiable information. *Id.* The page also provides links to (1) the most recent privacy impact assessment for each system, and (2) the most recent privacy threshold analysis for each system. *Id.*

[8] http://www.osec.doc.gov/opog/privacy/Census-pias.html.

At least five of the CEN systems and divisions identified on the Bureau's privacy impact assessment webpage (CEN05, CEN08, CEN11, CEN13, and CEN18) will be used to collect, process, and/or store personally identifiable information obtained through the 2020 Census, including citizenship data. Compl. ¶ 49; *see also* Prelim. Inj. Mem. Ex. 5, ECF No. 8-5, U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN05 Field Systems Major Application System* at 1 (approved June 22, 2018); Prelim. Inj. Mem. Ex. 6 at 1, 5; Prelim. Inj. Mem. Ex. 7, ECF No. 8-5, U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN11 Demographic Census, Surveys, and Special Processing* at 1, 4 (approved June 22, 2018); Prelim. Inj. Mem. Ex. 8, ECF No. 8-5, U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN13 Center for Economic Studies (CES)* at 1 (approved June 26, 2018); Prelim. Inj. Mem. Ex. 9, ECF No. 8-5, U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN18 Enterprise Applications* at 1 (approved June 26, 2018).

EPIC, on its own behalf and on behalf of its Members, sought out the most recent privacy impact assessment for these five CEN systems. Compl. ¶ 53; *see also* Prelim. Inj. Mem. Ex. 10, ECF No. 8-6, Declaration of Christopher Wolf ¶ 13 (Nov. 29, 2018); Prelim. Inj. Mem. Ex. 11, ECF No. 8-6, Declaration of Bruce Schneier ¶ 13 (Nov. 29, 2018); Prelim. Inj. Mem. Ex. 12, ECF No. 8-6, Declaration of Harry R. Lewis ¶ 13 (Dec. 3, 2018). Although a recent privacy impact assessment exists for each CEN, three of the five do not mention personal data concerning citizenship status at all, while the other two include no analysis of how the collection, maintenance, and dissemination of citizenship data would affect the privacy of census respondents. Compl. ¶ 53.

EPIC, on its own behalf and on behalf of its Members, sought out the privacy impact assessment for "CEN05 Field Systems Major Application" by visiting the Census Bureau

privacy impact assessment webpage. Compl. ¶ 53. CEN05 is a "major information system" that "plans, organizes, coordinates, and carries out the Bureau's field data collection program for sample surveys, special censuses, the Economic Census, and the Decennial census." *Id.* But the most recent privacy impact assessment for CEN05 does not acknowledge that the system would handle citizenship information or analyze the privacy impact of that data collection. Compl. ¶ 54.

EPIC, on its own behalf and on behalf of its Members, also sought out the privacy impact assessment for "CEN08 Decennial Information Technology Division (DITD)" by visiting the Census Bureau privacy impact assessment webpage. Compl. ¶ 55. CEN08 is a Census Bureau division and information system "consist[ing] of both general support systems and major applications," including applications that "process response data from census tests and 2020 Census operations[.]" *Id*. Although the most recent privacy impact assessment for CEN08 acknowledges the existence of the citizenship question through a single word ("Citizenship"), the assessment contains no specific analysis of the impact of collecting citizenship status information. Compl. ¶ 56.

EPIC, on its own behalf and on behalf of its Members, also sought out the privacy impact assessment for "CEN11 Demographic Census, Surveys, and Special Processing" by visiting the Census Bureau privacy impact assessment webpage. Compl. ¶ 57. CEN11 is an information system "comprised of components that support the Demographic Directorate business functions" and includes "a Commercial off the Shelf (COTS) product used by Census Bureau demographic programs for data access, transformation, reporting, and statistical analysis." *Id*. Although the most recent privacy impact assessment for CEN11 acknowledges the existence of the citizenship question through a single word ("Citizenship"), the assessment contains no specific analysis of the impact of collecting citizenship status information. Compl. ¶ 58.

EPIC, on its own behalf and on behalf of its Members, also sought out the privacy impact assessment for "CEN13 Center for Economic Studies (CES)" by visiting the Census Bureau privacy impact assessment webpage. Compl. ¶ 59. The "data holdings [of CEN13] include census and survey data which may contain name, gender, age, date of birth etc. from across the Census Bureau[.]" *Id.* Nonetheless, the most recent privacy impact assessment for CEN13 does not acknowledge that the system would handle citizenship information or analyze the privacy impact of that data collection. Compl. ¶ 60.

Finally, EPIC, on its own behalf and on behalf of its Members, sought out the privacy impact assessment for "CEN 18 Enterprise Applications" by visiting the Census Bureau privacy impact assessment webpage. Compl. ¶ 61. CEN18 is an information system "used to deliver applications to end users of the U.S. Census Bureau network." *Id.* The system maintains "survey and census information," including "personal names, personal addresses, personal contact information (telephone numbers, email address), business information, occupation, medical information, tax information, etc." *Id.* Nonetheless, the most recent privacy impact assessment for CEN18 does not acknowledge that the system would handle citizenship information or analyze the privacy impact of that data collection. Compl. ¶ 62.

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

On November 20, 2018, EPIC filed the instant suit against the U.S. Census Bureau and the Department of Commerce (collectively, "the Defendants," "the Census Bureau," or "the Bureau"). EPIC alleged that Defendants violated the E-Government Act and Administrative Procedure Act ("APA") in two respects. First, EPIC alleged that Defendants took unlawful action in violation of 5 U.S.C. § 706(2) and E-Government Act § 208(b) by initiating a new collection of information without first producing required privacy impact assessments. Compl. ¶¶ 64–70 (Count I). Second, EPIC alleged that Defendants unlawfully withheld production of

required privacy impact assessments in violation of 5 U.S.C. § 706(1) and E-Government Act § 208(b). Compl. ¶¶ 71–76 (Count II). EPIC also brought a claim under the Declaratory Judgment Act, 28 U.S.C. § 2201(a). Compl. ¶¶ 77–78 (Count III). As relief, EPIC sought, *inter alia*, the suspension and revocation of the citizenship question pending completion and publication of the required privacy impact assessments. Compl. pp. 26–27.

On January 18, 2019, EPIC moved for a preliminary injunction to prevent the Government from initiating the collection of citizenship status information pending final resolution of EPIC's claims. Pl.'s Mot. Prelim. Inj., ECF No. 8. The Bureau opposed EPIC's motion on the merits but did not dispute that EPIC had "associational standing to challenge the Defendants' alleged failure to publish a PIA consistent with the requirements of Section 208 of the E-Government Act[.]" Defs.' Opp'n at 19–20.

On February 8, 2019, this Court denied EPIC's motion for a preliminary injunction. The Court noted the Bureau's "conce[ssion]" that it must "prepare PIAs that adequately address the collection of citizenship data in the 2020 Census," Mem. Op. 6, and the Court acknowledged the "negative policy consequences" that can result "if an agency drags its feet in performing its PIA obligations." *Id.* at 17. The Court also rejected the Bureau's arguments that EPIC's APA claims suffered from a "lack of ripeness or final agency action," *Id.* at 18 n.10. However, the Court concluded that EPIC had failed to demonstrate a likelihood of success on the merits because the Bureau's duty to conduct, review, and publish the requisite privacy impact assessments would not come due "until the Bureau mails its first set of [census] questionnaires to the public in January 2020." *Id.* at 8. The Court also concluded that EPIC did not demonstrate a likelihood of irreparable harm. *Id.* at 20. The Court thus determined that EPIC had failed to satisfy the four-part test for a preliminary injunction. *Id.*

VI. Related rulings concerning the citizenship question

On January 15, 2019, the U.S. District Court for the Southern District of New York entered a final judgment in *New York v. U.S. Department of Commerce*, 351 F. Supp. 3d 502, a separate lawsuit challenging the addition of the citizenship question under the APA, the Enumeration Clause of the U.S. Constitution, and the Fifth Amendment of the U.S. Constitution. The court, finding "no dispute" that Secretary Ross's decision to add a citizenship question constituted "final agency action," concluded that the Secretary "violated the APA in several respects" and "violated the public trust." *Id.* at 518, 627. Accordingly, the court "vacat[ed] Secretary Ross's decision to add a citizenship question to the 2020 census questionnaire" and "enjoin[ed] Defendants from implementing Secretary Ross's March, 26, 2018 decision or from adding a question to the 2020 census questionnaire without curing the legal defects identified" by the Court. *Id.* at 679. On February 15, 2019, the U.S. Supreme Court granted the government's petition for a writ of certiorari before judgment in the case. *Dep't of Commerce v. New York*, 139 S. Ct. 953 (2019). Oral argument is scheduled for April 23, 2019.

On March 6, 2019, the U.S. District Court for the Northern District of California similarly enjoined the Bureau "from including the citizenship question on the 2020 Census." *California v. Ross*, No. 18-1865, 2019 WL 1052434, at *70 (N.D. Cal. Mar. 6, 2019). The court agreed that Secretary Ross's decision to add the citizenship question violated the APA, *id.* at *1–2, but the court went on to conclude that his decision also "violate[d] the Enumeration Clause of the Constitution." *Id.* at *69. On March 15, 2019, the Supreme Court ordered the parties in *New York* to "brief and argue" the question of whether the addition of the citizenship question violates the Enumeration Clause. *Dep't of Commerce v. New York*, No. 18-966, 2019 WL 1216251, at *1 (U.S. Mar. 15, 2019).

STANDARD OF REVIEW

I. 12(b)(1) 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). Although "the plaintiff bears the burden of establishing jurisdiction by a preponderance of the evidence," *Wigfall v. Office of Compliance*, 332 F. Supp. 3d 159, 166 (D.D.C. 2018), "the court must treat the plaintiff's factual allegations as true and afford the plaintiff the benefit of all inferences that can be derived from the facts alleged." *Id.* (quoting *Jeong Seon Han v. Lynch*, 223 F. Supp. 3d 95, 103 (D.D.C. 2016)). Further, "a court may consider documents outside the pleadings to evaluate whether it has jurisdiction." *Id.* (citing *Jerome Stevens Pharm., Inc. v. FDA*, 402 F.3d 1249, 1253 (D.C. Cir. 2005)).

II. 12(b)(6) standard of review

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)). "Well-pleaded factual allegations are 'entitled to [an] assumption of truth,' and the court construes the complaint 'in favor of the plaintiff, who must be granted the benefit of all inferences that can be derived from the facts alleged[.]'" *Moore v. United States Dep't of State*, 351 F. Supp. 3d 76, 87 (D.D.C. 2019) (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

The Census Bureau's Motion to Dismiss must be denied. First, as both the Court and the Bureau recognized at an earlier stage of this proceeding, EPIC has Article III standing to bring its claims. That is so because the Bureau's failure to disclose privacy impact assessments denies EPIC's Members vital information about the Bureau's data collection activities to which they are legally entitled. Second, EPIC has plausibly alleged that the Bureau's failure to conduct and publish privacy impact assessments prior to initiating the collection of citizenship status information violates the E-Government and the Administrative Procedure Act in multiple respects. Thus, the Bureau's Motion fails.

I. EPIC HAS CONCLUSIVELY ESTABLISHED ARTICLE III STANDING

The Census Bureau is correct that EPIC, as the plaintiff, "bears the burden of invoking the court's subject matter jurisdiction, including establishing the elements of standing." *Arpaio v. Obama*, 797 F.3d 11, 18 (D.C. Cir. 2015). The same requirement applied at the preliminary

injunction stage. *See In re Navy Chaplaincy*, 534 F.3d 756 (D.C. Cir. 2008) (Kavanaugh, J.). But neither the Bureau nor the Court raised any question as to EPIC's satisfaction of the requirements of Article III during the preliminary injunction proceedings. The agency, in its opposition to EPIC's Motion, assumed that EPIC "could establish it has associational standing to challenge the Defendants' alleged failure to publish a PIA consistent with the requirements of Section 208 of the E-Government Act." Defs.' Opp'n 19. The Court did not mention standing once in the Memorandum Opinion, in which the Court exercised Article III jurisdiction to consider the underlying merits of EPIC's claims under the E-Government Act and the APA. Federal courts "must ensure that they have jurisdiction before considering the merits of a case." *B&J Oil & Gas v. FERC*, 353 F.3d 71, 75 (D.C. Cir. 2004) (citing *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 94-102 (1998)). There was simply no question that EPIC had standing to bring these claims.

Yet now the Bureau offers several different theories as to why EPIC should not be allowed to have this case decided in federal court. These arguments lack merit and should be rejected. EPIC has associational standing to sue on behalf of its Members when they face an actual or imminent, concrete, and particularized injury-in-fact that is caused by a defendant and redressable by a court. *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). EPIC "need not prove the merits of [the] case in order to demonstrate . . . Article III standing." *Id*. at 493. "To survive a motion to dismiss for lack of standing," all that is required is that EPIC's Complaint "state a plausible claim" for Article III standing. *Williams v. Lew*, 819 F.3d 466, 472 (D.C. Cir. 2016). The Court must also accept all "well-pleaded factual

allegations as true and draw all reasonable inferences from those allegations in the plaintiff's favor." *Id.*

EPIC's Complaint and exhibits clearly establish that it has standing to seek injunctive relief against the Department of Commerce and the Census Bureau. EPIC and its Members will be irreparably harmed by the Census Bureau's failure to disclose "information [that] is highly relevant to an ongoing and highly public matter." *EPIC v. Presidential Advisory Comm'n on Election Integrity*, 266 F. Supp. 3d 297, 319 (D.D.C. 2017) [hereinafter *EPIC v. PACEI I*], *aff'd on other grounds*, 878 F.3d 371 (D.C. Cir. 2017). EPIC is a membership organization, as its bylaws conclusively establish. Compl. ¶ 10; *see also* Prelim. Inj. Mem. Ex. 18 §§ 2.02, 5.01–5.05, ECF No. 8-7. As such, EPIC has standing to sue on behalf of its Members whenever "(1) [EPIC's] members would otherwise have standing to sue in their own right; (2) the interests [EPIC] seeks to protect are germane to the organization's purpose; and (3) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Sorenson Commc'ns, LLC v. FCC*, 897 F.3d 214, 224 (D.C. Cir. 2018) (quoting *Ctr. for Sustainable Econ. v. Jewell*, 779 F.3d 588, 596 (D.C. Cir. 2015)) (internal quotation marks omitted). EPIC readily satisfies these criteria here.

First, EPIC's Members have suffered and continue to suffer concrete and particularized informational injuries as a result of Defendants' failure to conduct and publish privacy impact assessments required under section 208 of the E-Government Act. *See* Prelim. Inj. Mem. Ex. 10; Prelim. Inj. Mem. Ex. 11; Prelim. Inj. Mem. Ex. 12. EPIC's Members (1) are subject to the Census Bureau's proposed collection of information, and (2) have been denied access to, and irreparably harmed by, the Census Bureau's unlawful failure to publish the required privacy impact assessments. *Id*. These facts are "accepted as true" at the motion to dismiss stage, and the

Bureau has not even attempted to argue that EPIC's allegations are not "plausible." *Arpaio*, 797 F.3d at 19 (quoting *Iqbal*, 556 U.S. at 678).

The Bureau's argument that EPIC cannot sue on behalf of its Members to vindicate their right to information under section 208 cannot be squared with the D.C. Circuit's holding in *EPIC v. Presidential Advisory Comm'n on Election Integrity*, 878 F.3d 371 (D.C. Cir. 2017) [hereinafter *EPIC v. PACEI II*]. EPIC's Members are precisely the "individuals" whose interests, the D.C. Circuit held, section 208 was enacted to protect. *Id*. And EPIC had already established in the district court proceedings in the *PACEI* case that a failure to publish a privacy impact assessment required under the E-Government Act worked an informational injury. *EPIC v. PACEI I*, 266 F. Supp. 3d at 313–14. There is simply no basis to conclude that the E-Government Act does not provide a "right to information." Mem. in Supp. of Defs.' Mot. Dismiss 14. For the purposes of determining Article III jurisdiction, courts must accept the plaintiff's "view of the law" on which the plaintiff's claims are based, *FEC v. Akins*, 524 U.S. 11, 21 (1998), so long as they are nonfrivolous. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 89 (1998) ("It is firmly established in our cases that the absence of a valid (as opposed to arguable) cause of action does not implicate subject-matter jurisdiction, *i.e.*, the courts' statutory or constitutional power to adjudicate the case.").

EPIC's Members would clearly have standing in their own right because they have suffered judicially redressable injuries caused by the Census Bureau that are "concrete, particularized, and actual or imminent." *Conference of State Bank Supervisors*, 313 F. Supp. 3d at 295 (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409 (2013)). EPIC's Members sought and were denied information which, as EPIC argues, the Bureau is required to disclose under section 208: "comprehensive and meaningful" assessments of how the collection,

processing, and storage of personal citizenship information will affect the privacy of EPIC's Members. OMB Guidance § II.C.2.a.b; *see also* Prelim. Inj. Mem. Ex. 10 ¶¶ 11–15; Prelim. Inj. Mem. Ex. 11 ¶¶ 11–15; Prelim. Inj. Mem. Ex. 12 ¶¶ 11–15. A plaintiff "suffers an 'injury in fact' when"—as here—"the plaintiff fails to obtain information which must be publicly disclosed pursuant to a statute." *Akins*, 524 U.S. at 21 (quoting *Public Citizen v. DOJ*, 491 U.S. 440, 449 (1989)); *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549–50 (2016) (reiterating the *Akins–Public Citizen* rule that a denial of information that Congress has ordered disclosed "constitute[s] injury in fact").

Second, the interests EPIC seeks to protect through this suit—the right to privacy and access to information about government data collection activities—are the very core of EPIC's organizational mission. Compl. ¶¶ 5–9; *see also* Prelim. Inj. Mem. Ex. 18 § 1.02 ("The Corporation is organized for the charitable and educational purposes of promoting personal privacy and constitutional rights."); Prelim. Inj. Mem. Ex. 10 ¶ 4 ("Central to EPIC's mission is oversight of government activities that impact individual privacy, free expression, and democratic values."). EPIC therefore satisfies the requirement of "pertinence between litigation subject and organizational purpose." *Ctr. for Sustainable Econ.*, 779 F.3d at 597.

Third, neither the claims nor the relief at issue in this case require the direct participation of EPIC's Members. "Member participation is not required where a 'suit raises a pure question of law' and neither the claims pursued nor the relief sought require the consideration of the individual circumstances of any aggrieved member of the organization." *Id.* at 597 (quoting *Int'l Union, United Auto., Aerospace & Agric. Implement Workers of Am. v. Brock*, 477 U.S. 274, 287–88 (1986)). Whether the Bureau has initiated a collection of information and impermissibly failed to publish valid privacy impact assessments are pure questions of law. This suit does not

implicate the specific factual circumstances of individual EPIC Members beyond what those Members have already declared. *See* Prelim. Inj. Mem. Ex. 10; Prelim. Inj. Mem. Ex. 11; Prelim. Inj. Mem. Ex. 12. EPIC therefore has associational standing to bring this suit on behalf of its Members.

The Bureau's other standing arguments do not warrant serious consideration. There is nothing "abstract," Defs.' Mem. 12, about EPIC's Members' informational interest in obtaining a legally required privacy impact assessment that addresses the compulsory collection of their citizenship status information. EPIC's Members are individuals subject to that collection. *EPIC v. PACEI II*, 878 F.3d at 378. The Bureau also cannot undermine EPIC's informational standing claim by "explain[ing] that it *will* conduct" revised privacy impact assessments by some unknown later date. Defs.' Mem. 12–13 (emphasis added). As the D.C. Circuit has explained, "stale information is of little value[.]" *Judicial Watch, Inc. v. DHS*, 895 F.3d 770, 778 (D.C. Cir. 2018) (quoting *Payne Enters., Inc. v. United States*, 837 F.2d 486, 494 (D.C. Cir. 1988)). EPIC alleges that it is entitled to the requisite information under section 208 *now*—not at the Bureau's leisure.

Indeed, providing information to the public is among the express statutory objectives of the E-Government Act, of which 208(b)(1)(B)(iii) is an integral part. Like the rest of section 208, the PIA publication requirement "ensure[s] sufficient protections for the privacy of personal information" and "promote[s] better informed decisionmaking by policy makers" by forcing federal agencies to come clean about their privacy and data collection practices. E-Government Act §§ 2(b)(7), 208(a). But section 208(b)(1)(B)(iii) also "provide[s] enhanced access to Government information" and "make[s] the Federal Government more transparent and accountable." The Bureau, in attempting to distinguish section 208 from analogous public

disclosure statutes, pretends as though this prefatory language does not exist. Defs.' Mem. 14. But Congress was careful to include it. By contrast, the Federal Election Campaign Act ("FECA")—to which the Bureau favorably cites—contains no such statement of Congressional purpose and no express indication that it is a general "transparency" statute. The vast majority of the FECA pertains to campaign finance rather than the publication of information. Pub. L. No. 92–225, 86 Stat. 3 (1972). Yet the Supreme Court had no difficulty concluding that a denial of information subject to public disclosure under the FECA gives rise to a cognizable informational injury. *Akins*, 524 U.S. at 21. The same logic applies to section 208. There—as here—"nothing in the Act that suggests Congress intended to exclude [individuals] from the benefits of these provisions, or otherwise to restrict standing[.]" *Akins*, 524 U.S. at 20.

The Bureau also incorrectly asserts that EPIC's E-Government Act claims are distinguishable from claims brought under similar assessment and disclosure statutes in the D.C. Circuit. Defs.' Mem. 14–15. But the harms suffered by EPIC's Members are closely analogous to the harms at issue in cases brought under the National Environmental Policy Act ("NEPA"), 42 U.S.C. § 4321 *et seq*. As the Court recently explained, NEPA "obligates every federal agency to prepare an adequate environmental impact statement *before* taking any major action." *Oglala Sioux Tribe v. U.S. Nuclear Reg. Comm'n*, 896 F.3d 520, 523 (2018) (emphasis in original). Like plaintiffs in NEPA cases, EPIC has established that it will suffer irreparable harm as a result of the agency's failure to conduct privacy impacts assessments, "combined with" the "concrete injur[ies]" of (1) the violation of EPIC Members' informational rights, and (2) the imminent, unauthorized collection of EPIC Members' personal data. *See Comm. of 100 on Federal City v. Foxx*, 87 F. Supp. 3d 191, 202 (D.D.C. 2015) (articulating the standard outlined in *Fund for Animals v. Clark*, 27 F. Supp. 2d 8, 14 (D.D.C. 1998)). Indeed, the injury in this case is even

more direct than the injuries at issue in NEPA cases because EPIC's Members are subject to the challenged data collection.

Like the NEPA, the E-Government Act's privacy impact assessment requirement serves a critical "'action-forcing' purpose." *Oglala Sioux Tribe*, 896 F.3d at 532 (quoting *Robertson v. Methow Valley Citizens Council*, 490 U.S. 332, 349 (1989)). In both statutes, impact assessments "ensur[e] that the agency, in reaching its decision, will have available, and will carefully consider, detailed information concerning significant" impacts (environmental impacts under NEPA, privacy impacts under the E-Government Act). *Winter v. NRDC*, 555 U.S. 7, 23 (2008). The laws "also guarantee[e] that the relevant information will be made available to the larger audience that may also play a role in both the decisiomaking process and the implementation of that decision." *Oglala Sioux Tribe*, 896 F.3d at 532 (quoting *Robertson*, 490 U.S. at 349).

Finally, the Bureau incorrectly attempts to inject into the standing analysis a discussion of "functional equivalence" factors used to evaluate whether non-membership organizations can nevertheless satisfy the requirements of associational standing. Defs.' Mem. 16–17. The Bureau relies on two cases: *American Legal Foundation v. FCC*, 808 F.2d 84 (D.C. Cir. 1987), and *Fund Democracy, LLC v. SEC*, 278 F.3d 21 (D.C. Cir. 2002). But these cases concern the question of "whether an organization that *has no members* in the traditional sense may nonetheless assert associational standing" (the so-called "functional equivalence" test). *Fund Democracy*, 278 F.3d at 25. That question is simply irrelevant here because EPIC's bylaws establish that it is a membership organization—a fact which is not in dispute. Compl. 10; *see also* Prelim. Inj. Mem. Ex. 18 §§ 2.02, 5.01–5.05. The functional equivalence test is simply not applied in cases involving traditional membership organizations like EPIC. *See, e.g.*, *Sierra Club v. Jewell*, 764 F.3d 1 (D.C. Cir. 2014); *NRDC v. EPA*, 489 F.3d 1364 (D.C. Cir. 2007).

In sum, EPIC has clearly established Article III standing to brings its claims on behalf of EPIC's Members.

II. EPIC HAS PLAUSIBLY STATED CLAIMS FOR RELIEF.

EPIC has alleged sufficient facts entitling it to relief under the E-Government Act and Administrative Procedure Act. First, EPIC has plausibly alleged (1) that the Bureau unlawfully failed to conduct, review, and publish required privacy impact assessments before initiating the collection of citizenship status information, Compl. ¶¶ 64–70, and (2) that the Bureau unlawfully initiated data collection absent the required assessments, Compl. ¶¶ 71–76. And second, EPIC's suit satisfies the applicable requirements for bringing an action under the APA.

Although the Court, in denying EPIC's Motion for a Preliminary Injunction, ruled that EPIC had not shown a likelihood of success on the merits, the Court did not reach a conclusive determination on EPIC's E-Government Act claims. Moreover, at the motion to dismiss stage—unlike a motion for a preliminary injunction—EPIC need only "state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570). Because EPIC has validly stated claims for relief under the E-Government Act and APA entitling it to relief, the Court must deny the Bureau's Motion to Dismiss.

A. EPIC has plausibly alleged that the Bureau is in violation of the E-Government Act.

As this Court previously noted, the Bureau "concede[s]" that it must "prepare PIAs that adequately address the collection of citizenship data in the 2020 Census," *id.* at 6 (citing Defs.' Opp'n at 1, 12). Nevertheless, the Bureau argues that it may postpone completion of the required privacy impact assessments until it actually distributes census questionnaires in 2020, Defs.' Mem. 21, and that EPIC therefore fails to state a claim. But the deadline for the Census Bureau to conduct and publish the required privacy impact assessments was over a year ago: March 26,

2018. That is the day Secretary Ross ordered the addition of a citizenship question to the 2020 Census, thereby initiating a new collection of citizenship status information.

An agency must conduct, review, and publish a valid privacy impact assessment before "initiating a new collection of information[.]" E-Government Act § 208(b)(1)(A). As the Court previously explained, Mem. Op. 7, the word "initiate" variously means "[t]o begin, commence, enter upon; to introduce, set going, give rise to, originate, 'start' (a course of action, practice, etc.)," *Initiate*, Oxford English Dictionary (2019);[9] "to cause or facilitate the beginning of: set going," *Initiate*, Merriam-Webster (2019);[10] and "to '[c]ommence, start; originate; introduce,'" *Initiate*, Black's Law Dictionary (6th ed. 1990). Collectively, these definitions "contemplate 'the first actions, steps, or stages of' the activity initiated." Mem. Op. 7 (quoting Webster's Third New International Dictionary 1164 (3d ed. 1976)).

The phrase "collection of information" is defined by statute as "the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency[.]" 44 U.S.C. § 3502(3)(A). Notably, Congress's use of gerunds in this definition indicates that that the "collection of information" is a beginning-to-end process—not a discrete, one-off action. *See, e.g.*, *Doe v. Bridgeport Police Dep't*, 434 F. Supp. 2d 107, 116 (D. Conn. 2006) ("First, the gerund 'injecting' . . . connotes 'the process of injection,' in contrast to 'to inject,' which connotes, to a greater degree, the specific and direct act of introducing a substance into a human body parenterally."); *N. Nat. Gas Co. v. Comm'r*, 44 T.C. 74, 78 (1965) ("The word 'acquiring' (in the regulation) is a gerund and as such its use . . . is indicative of a

[9] http://www.oed.com/view/Entry/96066?rskey=wxG1jD&result=2&is Advanced=false#eid.
[10] https://www.merriam-webster.com/dictionary/initiate.

continuing transaction and is a clear recognition that the acquisition of possession may be a gradual process[.]").

Combining these meanings, an agency must complete and publish a privacy impact assessment before it begins, originates, introduces, sets going, facilitates the beginning of, or takes the first steps in "the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency[.]" 44 U.S.C. § 3502(3)(A). The Department of Commerce initiated a collection of information on March 26, 2018, when it took final agency action by ordering the Census Bureau to add a citizenship question to the 2020 Census. On that day, Defendants concluded their decisionmaking process and began, originated, introduced, set going, facilitated the beginning of, and took the first steps in "the obtaining, causing to be obtained, soliciting, or requiring the disclosure" of citizenship status information—even though no information was actually solicited or obtained. 44 U.S.C. § 3502(3)(A). This transition from *deciding* on a course of action to *implementing* that course of action is precisely what constitutes "final agency action." *See U.S. Army Corps of Eng'rs v. Hawkes Co.*, 136 S. Ct. 1807, 1813 (2016) (quoting *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997)) (explaining that final agency action "mark[s] the consummation of the agency's decisionmaking process" and is a step "by which rights or obligations have been determined, or from which legal consequences will flow").

Yet the Bureau contends that it may put off its obligation to conduct and publish a privacy impact assessment until the moment before it "mail[s] or distribute census forms to individuals." Defs.' Mem. 21. This arbitrary temporal line cannot be squared with the plain text of the E-Government Act and PRA, the implementing OMB regulations, or the fundamental purpose of a privacy impact assessment.

First, the statutory context of the phrase "initiating a new collection of information" confirms EPIC's reading of the statute. Section 208 expressly distinguishes between the moment when an agency "initiat[es] a new collection of information" and the later point in time at which the information "*will* be collected, maintained, or disseminated[.]" E-Government Act § 208(b)(1)(A)(ii). Congress understood these to be two independent events—the former occurring at the very beginning of the information collection process, the latter occurring when information is actually solicited or obtained.

This reading is reinforced by preceding clause of the statute, which sets out a parallel trigger for privacy impact assessments. Under E-Government Act § 208(b)(1)(A)(i), agencies must complete an assessment before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form[.]" Notably, this is not a requirement to complete an assessment before "using" or "activating" or "deploying" a new IT system. The obligation attaches far sooner, at a point when the results of the assessment can still inform the agency's decisionmaking process. Section 208 thus forces an agency to consider the privacy implications of a proposed system before the agency commits to a potentially wasteful, ill-advised, or unlawful acquisition decision. The same "action-forcing" purpose animates the environmental assessment requirement in the National Environmental Policy Act. *See Oglala Sioux Tribe*, 896 F.3d at 532 (quoting *Robertson*, 490 U.S. at 349).

So too with "new collection[s] of information." E-Government Act § 208(b)(1)(A)(ii). In order to "ensure sufficient protections for the privacy of personal information," E-Government Act § 208(a), Congress requires agencies to conduct, review, and publish an assessment before initiating the collection process. It would be strange indeed for Congress to require early-stage privacy impact assessments for new IT systems while allowing new collections of personal

information to go unexamined by agencies until the very last minute. *See SAS Inst., Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018) (quoting *Univ. of Texas Sw. Med. Ctr. v. Nassar*, 570 U.S. 338, 353 (2013)) ("'[J]ust as Congress' choice of words is presumed to be deliberate' and deserving of judicial respect, 'so too are its structural choices.'"). Had Congress actually intended such divergent treatment of IT systems and information collections, it could have borrowed the familiar terminology of the PRA and required agencies to complete an assessment only before "*conduct[ing]*" a new collection of information. 44 U.S.C. § 3507(a) (emphasis added). But that is not the verb Congress used, and "[t]he fact that [Congress] did not adopt this readily available and apparent alternative" is telling. *Knight v. Comm'r*, 552 U.S. 181, 188 (2008). Instead, Congress recognized the "collection of information" is a process that *culminates*, not *begins*, with the actual collecting of information.

This view is repeatedly confirmed in the PRA, where the phrase "collection of information" is used at least twenty times to refer to "collection[s]" for which no information has been solicited or obtained. *See* 44 U.S.C. § 3505 (noting agencies' obligation to internally "review . . . collections of information," even though no information has been solicited or obtained); 44 U.S.C. §§ 3506(c)(1)(A), (c)(1)(A)(i), (c)(1)(A)(v), (c)(3) (detailing agencies' obligation to internally "review each collection of information," even though no information has been solicited or obtained); 44 U.S.C. §§ 3507(d)(4)(A), (d)(4)(B), (d)(4)(C), (d)(4)(D), (d)(4)(D)(i), (d)(4)(D)(i)(ii), (d)(6), (e)(1), (h)(2), (h)(2)(A), (h)(2)(B), (j)(1), (j)(1)(A), (j)(1)(B)(iii) (detailing the OMB Director's authority to approve or reject certain "collection[s] of information" for which no information has been solicited or obtained); 44 U.S.C. § 3510(a) (distinguishing between "a collection of information" and the "information obtained by" that collection); 44 U.S.C. § 3517(a) (noting the OMB Director's power to review "collections of

information" for which no information has been solicited or obtained). The OMB cannot review, approve, or reject something that supposedly does not exist (not even in the form of a plan or proposal). If a "collection of information" only comes into being once data has actually been solicited, Congress has repeatedly commanded the OMB to do the impossible in the PRA.

It is clear, then, that agency need not actually acquire or solicit "facts or opinions" for a collection of information to exist, so long as the *process* of "obtaining," "soliciting," "causing to be obtained," or "requiring . . . disclosure" is underway. 44 U.S.C. § 3502(3)(A). Indeed, the OMB further defines "collection of information" to include "a *plan* and/or an instrument calling for the collection or disclosure of information[.]" 5 C.F.R. § 1320.3(c) (emphasis added); *see also EPIC v. PACEI II*, 878 F.3d at 380 (noting that an agency must "prepare a privacy impact assessment [if] it *plans* to collect information" (emphasis added)). Even an "algorithm" can constitute a "collection of information" under 44 U.S.C. § 3502(3)(A) if it "impose[s] a 'reporting requirement'" on members of the public. *Benkelman Tel. Co. v. FCC*, 220 F.3d 601, 607 (D.C. Cir. 2000) (quoting *Saco River Cellular, Inc. v. FCC*, 133 F.3d 25, 33 (D.C. Cir. 1998)).

The plain meaning of the phrase "initiating a new collection of information" is clear from analogy to other complex legal and administrative processes. For example, a couple "initiates an adoption" when it completes the requisite agency paperwork to begin the adoption process—not months or years later when the couple meets or takes custody of their child. *See, e.g.*, *Submitting a Case*, U.S. Embassy in Ethiopia (2013).[11] ("[T]he adoption dossier submitted by prospective adoptive parents . . . to initiate an adoption, will need to include the PAIR letter issued by

[11] https://et.usembassy.gov/u-s-citizen-services/child-family-matters/adoption/who-can-adopt/submitting-a-case/.

USCIS."). And the Coast Guard's duty under 6 U.S.C. § 394 to assess certain preliminary factors "before initiating a comprehensive evaluation" certainly does not permit the Coast Guard to postpone an assessment until *after* it has spent voluminous resources preparing a comprehensive evaluation.

Finally, the Bureau's proposed timeline for its privacy impact assessment obligations is incompatible with the purposes of section 208. Congress enacted section 208 to "ensure sufficient protections for the privacy of personal information"; "promote better informed decisionmaking by policy makers"; "provide enhanced access to Government information"; and "make the Federal Government more transparent and accountable." E-Government Act §§ 208(a), 2(b)(7), (9), (11). None these objectives would be served if the assessment requirement did not mature until the last minute—potentially months or years *after* an agency had made the final decision to collect personal information.

The core purposes of an impact assessment, as this Court has explained in the NEPA context, are (1) to ensure that "the agency, in reaching its decision, will have available, and will carefully consider, detailed information concerning" the impact of a pending agency action, and (2) to "guarantee[] that the relevant information will be made available to the larger audience that may also play a role in both the decisionmaking process and the implementation of that decision." *Oglala Sioux Tribe*, 896 F.3d at 532 (quoting *Robertson*, 490 U.S. at 349); *see also Jones v. D.C. Redevelopment Land Agency*, 499 F.2d 502, 512 (D.C. Cir. 1974) (noting that impact assessments "ensure that decisions about federal actions w[ill] be made only after responsible decisionmakers ha[ve] fully adverted" to the "consequences of the[ir] actions"). These purposes would be completely undermined if an agency were allowed to conduct a privacy

impact assessment after the final decision and after a potentially "irretrievable commitment of resources." *Id.* (quoting *Lathan v. Volpe*, 455 F.2d 1111, 1121 (9th Cir. 1971)).

For precisely this reason, OMB regulations require an agency to conduct a privacy impact assessment when the agency is *considering* whether to collect personal data:

> 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.*

OMB Circular, app. II at 10 (emphases added). The OMB's definition of "privacy impact assessment" makes clear than an assessment must "examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns"—information that is of little use when a final decision to collect information has already been made. *Id.* at 34.

Moreover, a comprehensive privacy impact assessment may well have led the Bureau to substantially modify or abandon the collection of citizenship status information, given the evidence in the record that the agency may use the data gathered for purposes unrelated to the tabulation of the census. *E.g.*, Compl. ¶¶ 38–39. In 2006, for example, U.S. Customs and Border Protection substantially modified a collection of personally identifiable information obtained from trucking companies in response to a privacy impact assessment. U.S. Dep't of Homeland Sec., *Privacy Impact Assessment for Automated Commercial Environment (ACE) e-Manifest: Trucks (ACE Release 4) and International Trade Data System (ITDS)* 1, 3, 15 (2006).[12] The results of the assessment prompted CBP to change course and "strongly encourage" affected truck carriers to "inform their employees of any personal information reported to [CBP]." *Id.* at 13.

[12] https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_aceitds.pdf.

Construing the E-Government Act in the way that the Bureau urges would contravene the plain text of section 208, undermine the express purposes of the statute, and render the privacy impact requirement a functional nullity. EPIC respectfully urges the Court to reject the Bureau's reading and to conclude, on the basis of the Bureau's failure to publish required privacy impact assessments, that EPIC has stated valid claims for relief.

B. EPIC's suit satisfies the requirements for an action under the APA.

EPIC is entitled to bring this suit under the Administrative Procedure Act because EPIC has been "adversely affected or aggrieved" by the Census Bureau's violations of the E-Government Act, 5 U.S.C. § 702, which this Court has the power to review. 5 U.S.C. §§ 704, 706. In ruling on EPIC's Motion for a Preliminary Injunction, this Court correctly concluded that EPIC's suit satisfies the preconditions for an APA action. Mem Op. 18 n.10 (noting that the Bureau's APA arguments—which the Bureau recycles in its Motion to Dismiss—"would only be relevant if EPIC sought to challenge, prospectively, the agencies' failure to conduct or release adequate PIAs in the future").

Because EPIC is a membership organization, Compl. ¶ 10, it is aggrieved to the same extent that EPIC's Members are. *See Pharm. Research & Mfrs. of Am. v. Thompson*, 259 F. Supp. 2d 39, 56 (D.D.C. 2003), *aff'd*, 362 F.3d 817 (D.C. Cir. 2004) (finding membership organization that "represent[ed] the interests of urban Indian Centers" therefore "ha[d] prudential standing to assert" an APA claim on behalf of those centers).

First, EPIC is aggrieved by the Census Bureau's unlawful initiation of a new collection of information without first completing the required privacy impact assessments. Compl. ¶¶ 64–70. By "directing the Census Bureau to place the citizenship question . . . on the decennial census form," Compl. ¶ 30, Secretary Ross took "final agency action" on behalf of the Bureau. § 704.

"There is no dispute the Secretary Ross's decision constitutes 'final agency action' reviewable under the APA." *New York*, 351 F. Supp. 3d at 627; *see also* Mem. Op. 7 (noting the parties' agreement that Secretary Ross's letter "constitutes final agency action"). This action was final because it "mark[ed] the consummation of the agency's decisionmaking process" and is a decision "by which rights or obligations have been determined, or from which legal consequences will flow[.]" *Ipsen Biopharmaceuticals, Inc. v. Hargan*, 334 F. Supp. 3d 274, 277 (D.D.C. 2018) (quoting *U.S. Army Corps of Eng'rs v. Hawkes Co.*, 136 S. Ct. 1807, 1813 (2016)); *see also* 13 U.S.C. § 221(a)–(b) (requiring all persons over 18 to respond to census questions).

Moreover, the Bureau's final agency action violated section 208 of the E-Government Act, a provision whose purpose is to "is to ensure sufficient protections for the privacy of personal information[.]" § 208(a); *see also EPIC v. PACEI II*, 878 F.3d at 378 (explaining that section 208 of the E-Government Act "protect[s] *individuals* . . . by requiring an agency to fully consider their privacy before collecting their personal information" (emphasis in original)). EPIC is thus aggrieved by the Bureau's action, which unlawfully imperils the privacy of EPIC's Members and has denied them information to which they are legally entitled. Compl. ¶¶ 52–62, 68–69. Finally, this Court has the power to "hold unlawful and set aside" the Bureau's action because it is "not in accordance with law" and was carried out "without observance of procedure required by law[.]" § 706(2); *see also* § 704.

Second, EPIC is "aggrieved" by the Census Bureau's unlawful failure to complete the required privacy impact assessments for the collection of citizenship status information. Compl. ¶¶ 71–76. An agency "unlawfully with[olds]" action under § 706 the APA when it fails to take a "discrete action that the agency has a duty to perform." *W. Org. of Res. Councils v. Zinke*, 892

F.3d 1234, 1241 (D.C. Cir. 2018) (citing *Norton v. Southern Utah Wilderness Alliance* (*SUWA*), 542 U.S. 55, 62–63 (2004)). Here, the Bureau failed to take the discrete actions of conducting, reviewing, and publishing required privacy impact assessments before "initiating a new collection of information," as mandated by section § 208(b) of the E-Government Act. These duties are "nondiscretionary" and amount to "specific, unequivocal command[s]." *W. Org. of Res. Councils*, 892 F.3d at 1241 (quoting *SUWA*, 542 U.S. at 63–64); *see also* E-Government Act § 208(b)(1)(A) ("An agency shall take actions described under subparagraph (B)[.]").

By failing to conduct or publish PIAs for the collection of citizenship status information, the Bureau has failed to "ensure sufficient protections for the privacy of personal information," § 208(a), and failed to "fully consider the[ ] privacy" of individuals whose personal data would be collected. *EPIC v. PACEI II*, 878 F.3d at 378. EPIC is thus aggrieved by the Bureau's inaction, which unlawfully imperils the privacy of EPIC's Members and has denied them information to which they are legally entitled. Compl. ¶¶ 52–62; 74–75. Finally, this Court has the power to "compel agency action unlawfully withheld or unreasonably delayed" under 5 U.S.C. § 706(1). As the D.C. Circuit recently explained, "the court can undertake review [under § 706(1)] as though the agency had denied the requested relief and can order an agency to either act or provide a reasoned explanation for its failure to act." *Friedman v. FAA*, 841 F.3d 537, 545 (D.C. Cir. 2016) (quoting *Sierra Club v. Thomas*, 828 F.2d 783, 793 (D.C. Cir. 1987)).

Because EPIC has plausibly alleged that it is aggrieved by the Census Bureau's violations of the E-Government Act and the APA, and because this Court has the power to review and remedy those violations, EPIC has stated claims for relief under the APA.

CONCLUSION

For the foregoing reasons, the Court should deny Defendants' Motion to Dismiss EPIC's Complaint.

Respectfully Submitted,

MARC ROTENBERG, D.C. Bar #422825
EPIC President and Executive Director

ALAN BUTLER, D.C. Bar #1012128
EPIC Senior Counsel

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

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Attorneys for Plaintiff EPIC

Dated: April 1, 2019