ORAL ARGUMENT NOT YET SCHEDULED

No. 19-5031

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

ELECTRONIC PRIVACY INFORMATION CENTER,
Plaintiff-Appellant,

v.

UNITED STATES DEPARTMENT OF COMMERCE, et al.,
Defendants-Appellees.

On Appeal from an Order of the
U.S. District Court for the District of Columbia
Case No. 18-cv-2711-DLF

BRIEF FOR APPELLANT

MARC ROTENBERG
ALAN BUTLER
JOHN DAVISSON
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Plaintiff-Appellant

CERTIFICATE AS TO PARTIES, RULINGS & RELATED CASES AND CORPORATE DISCLOSURE STATEMENT

Pursuant to D.C. Circuit Rules 28(a)(1) and 26.1 and Fed. R. App. P. 26.1, the Electronic Privacy Information Center ("EPIC") submits the following Certificate as to Parties, Rulings, and Related Cases and Corporate Disclosure Statement:

I. PARTIES AND *AMICI* APPEARING BELOW

The parties to this case are Appellant EPIC, which was the Plaintiff in the district court, and Appellees United States Department of Commerce and Bureau of the Census, which were the Defendants in the district court.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues; to protect privacy, the First Amendment, and other constitutional values; and to promote open government.

The United States Department of Commerce is a federal agency subject to the Administrative Procedure Act and the E-Government Act, Pub. L. No. 107-347, 116 Stat. 2899 (Dec. 17, 2002) (codified at 44 U.S.C. § 3501 note).

The Bureau of the Census is a federal agency subject to the Administrative Procedure Act and the E-Government Act, Pub. L. No. 107-347, 116 Stat. 2899.

There were no amici or intervenors appearing before the district court, and no amici or intervenors have appeared before this Court.

II. RULINGS UNDER REVIEW

The ruling under review in this appeal is the February 8, 2019 Order and Memorandum Opinion by the U.S. District Court for District of Columbia (Hon. Dabney L. Friedrich) denying EPIC's motion for a preliminary injunction.

III. RELATED CASES

This case has not been before this Court or any other court, with the exception of the district court below. EPIC is aware of the following related cases under D.C. Circuit Rule 28(a)(1)(C) that are currently pending or on appeal:

- *New York v. U.S. Dep't of Commerce*, No. 18-2921 (S.D.N.Y. filed Apr. 3, 2018)
- *New York Immigration Coal. v. Dep't of Commerce*, No. 18-5025 (S.D.N.Y. filed June 6, 2018)
- *New York v. U.S. Dep't Commerce*, No. 19-212 (2d Cir. appeal docketed Jan 22, 2019)
- *Department of Commerce v. New York*, No. 18-966 (U.S. cert before judgment granted Feb. 15, 2019)
- *Kravitz v. Dep't of Commerce*, No. 18-1041 (D. Md. filed Apr. 22, 2018)
- *La Union del Pueblo Entero v. Ross*, No. 18-1570 (D. Md. filed May 31, 2018)
- *California v. Ross*, No. 18-1865 (N.D. Cal. filed Mar. 26, 2018)

- *City of San Jose v. Ross*, No. 18-2279 (N.D. Cal. filed Apr. 17, 2018)

IV. CORPORATE DISCLOSURE STATEMENT

EPIC is a 501(c)(3) non-profit corporation. EPIC has no parent, subsidiary, or affiliate. EPIC has never issued shares or debt securities to the public, and no publicly-held company has any ownership interest in EPIC.

Respectfully Submitted,

Dated: March 1, 2019

/s/ John L. Davisson
JOHN L. DAVISSON
EPIC Counsel

TABLE OF CONTENTS

TABLE OF AUTHORITIES*

Cases

---

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

Statutes

Rules

Regulations

Constitutional Provisions

Other Authorities

GLOSSARY

ADD	Citation to the Addendum
APA	Administrative Procedure Act
E-Government Act	E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899
EPIC	Electronic Privacy Information Center
JA ___	Citation to the Joint Appendix
NEPA	National Environmental Policy Act, 42 U.S.C. § 4321 *et seq*.
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PRA	Paperwork Reduction Act

INTRODUCTION

Unique among federal agencies, the U.S. 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.

EPIC has repeatedly warned the Census Bureau of the need to comply with E-Government Act—a point the agency does not dispute—yet the agency

continues to move forward with its unlawful agency action. Key deadlines are fast approaching, and major privacy risks have not been addressed by the agency. And nowhere is the duty to assess privacy risks under section 208 more important than the decennial census, a "unique" and compulsory collection of data that "reaches every population group, from America's long-time residents to its most recent immigrants." Presidential Proclamation No. 7,286, 65 Fed. Reg. 17,985, 17,985 (Apr. 1, 2000).

The Court should reverse the judgment of the district court denying EPIC's motion for a preliminary injunction and enter an injunction halting the Census Bureau's implementation of the citizenship question pending the adjudication of EPIC's claims.

JURISDICTIONAL STATEMENT

Appellant EPIC filed a motion for a preliminary injunction in the U.S. District Court for the District of Columbia pursuant to Fed. R. Civ. P. 65. The lower court had jurisdiction under 28 U.S.C. § 1331, 5 U.S.C. § 702, and 5 U.S.C. § 704. EPIC filed a timely notice of appeal on February 12, 2019. The Court has jurisdiction over this appeal under 28 U.S.C. § 1291.

PERTINENT STATUTORY PROVISIONS

The text of pertinent federal statutory provisions and regulations is reproduced in the addendum to this brief.

STATEMENT OF ISSUES FOR REVIEW

1. Whether the lower court wrongly denied EPIC's motion for a preliminary injunction blocking the Census Bureau's collection of citizenship status information via the 2020 Census?
2. Whether the Census Bureau has violated the E-Government Act by failing to conduct, review, and publish privacy impact assessments that evaluate the privacy risks of collecting citizenship status information?
3. Whether EPIC will suffer irreparable harm absent a preliminary injunction blocking the collection of citizenship status information via the 2020 Census?

STATEMENT OF THE CASE

I. Section 208 of the E-Government Act

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:

> 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*"), ADD 30. 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, ADD 29. 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." 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"), ADD 34.

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, ADD 34. 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;
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, ADD 34. 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, ADD 34.

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), ADD 32. 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, ADD 32–33. 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, ADD 33; "agencies work[ing] together on shared functions involving significant new uses or exchanges of information in identifiable form," *Id.* § II.B.2.g, ADD 33; and "changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form." *Id.* § II.B.4, ADD 33.

II. The Department of Commerce order initiating the collection of citizenship status information

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, "the 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." Letter from Wilbur Ross, Secretary of Commerce, to Karen Dunn Kelley, Under Secretary for Economic Affairs, at 8 (Mar. 26, 2018), JA 60. No such question appeared on the 2010 Census, U.S. Dep't of Commerce, *United States Census 2010* (2009), JA 221, nor has the Bureau posed a citizenship question to all census respondents

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

since the 1950 Census. *See* JA 53. 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. JA 53. Secretary Ross's explanation for his decision is at odds with the extensive evidence uncovered in litigation over the citizenship question. *See New York v. U.S. Department of Commerce*, No. 18-CV-2921 (JMF), 2019 WL 190285, at *4 (S.D.N.Y. Jan. 15, 2019).

On March 28, 2018, the Bureau officially reported to Congress its intention to add a citizenship question to the 2020 Census. U.S. Census Bureau, *Questions Planned for the 2020 Census and American Community Survey* 7 (March 2018), JA 61. The version of the question presented to Congress asked: "Is this person a citizen of the United States?" *Id.* 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 release of respondents' citizenship status (and potentially immigration status), 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," JA 53, 60—data that is susceptible to reidentification. Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000), JA 63. 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." 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), JA 153, 155, 157. 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." Tara Bahrampour, *Trump Administration Officials Suggested Sharing Census Responses with Law Enforcement, Court Documents*

Show, Wash. Post (Nov. 19, 2018);[3] *see also* Decl. of Andrew Case in Supp. of Pls.' Opp'n to Defs.' Mot. Summ. J. at Ex. B, *City of San Jose v. Ross*, 18-2279 (N.D. Cal. Filed Nov. 16, 2018).

Historically, the misuse of census data has caused considerable harm, particularly to vulnerable populations. 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

---

[3] https://www.washingtonpost.com/local/social-issues/trump-administration-officials-suggested-sharing-census-responses-with-law-enforcement-court-documents-show/2018/11/19/41679018-ec46-11e8-8679-934a2b33be52_story.html.

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).[4]

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. EPIC, *Department of Homeland Security Obtained Data on Arab Americans From Census Bureau* (2004);[5] *see also* Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*, N.Y. Times (Jul.

[4] https://www.archives.gov/files/research/japanese-americans/justice-denied/chapter-3.pdf.
[5] https://epic.org/privacy/census/foia/.

30, 2004).[6] The Census Bureau and Customs and Border Protection revised their data request policies following EPIC's FOIA case. *See* Lynette Clemetson, *Census Policy On Providing Sensitive Data Is Revised*, N.Y. Times, (Aug. 31, 2004);[7] U.S. Customs and Border Protection, *Policy for Requesting Information of a Sensitive Nature from the Census Bureau* (Aug. 9, 2004).[8]

Many Americans remain fearful that their census responses will be "used against them or their loved ones" by federal agencies. *New York v. U.S. Department of Commerce*, No. 18-CV-2921 (JMF), 2019 WL 190285, at *9 (S.D.N.Y. Jan. 15, 2019). 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 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 administrative sources." Memorandum from John M. Abowd, Chief Scientist, U.S. Census

---

[6] https://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html.
[7] https://www.nytimes.com/2004/08/31/us/census-policy-on-providing-sensitive-data-is-revised.html.
[8] https://epic.org/privacy/census/foia/policy.pdf.

Bureau, to Wilbur L. Ross, Sec'y of Commerce, at 1 (Jan. 19, 2018), JA 96; *see also 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 the district court made clear, the defendants concede they must "prepare PIAs that adequately address the collection of citizenship data in the 2020 Census." Mem. Op. 6 (citing Defs.' Opp'n, ECF No. 12, at 1, 12), JA 9. 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.

When the Census Bureau produces a privacy impact assessment concerning Bureau activities, the assessment is published on the Bureau's privacy impact assessment webpage. 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).[9] 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.*

[9] 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. *See* U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN05 Field Systems Major Application System* at 1 (approved June 22, 2018), JA 133; JA 149, 153; 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), JA 165, 168; U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN13 Center for Economic Studies (CES)* at 1 (approved June 26, 2018), JA 178; U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN18 Enterprise Applications* at 1 (approved June 26, 2018), JA 190.

EPIC, on its own behalf and on behalf of its members, sought out the most recent privacy impact assessment for these five CEN systems. *See* Declaration of Christopher Wolf ¶ 13 (Nov. 29, 2018), JA 204; Declaration of Bruce Schneier ¶ 13 (Nov. 29, 2018), JA 207; Declaration of Harry R. Lewis ¶ 13 (Dec. 3, 2018), JA 210. 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/or dissemination of citizenship data would affect the privacy of census respondents.

See JA 136–37 (failing to list "citizenship" among the information collected); JA 180–81 (same); JA 192–93 (same); JA 148–63 (failing to analyze the privacy implications of collecting citizenship status information); JA 164–76 (same).

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. JA 132; *see also* JA 204, 207, 210. 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." JA 133; *see also* Declaration of Robin J. Bachman, Chief Privacy Officer, United States Census Bureau ¶ 14 ("Bachman Decl."), JA 249. 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. *See generally* JA 132–47.

EPIC, on its own behalf and on behalf of its members, sought out the privacy impact assessment for "CEN08 Decennial Information Technology Division (DITD)" by visiting the Census Bureau privacy impact assessment webpage. JA 148; *see also* JA 204, 207, 210. 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[.]" JA 158; *see also* JA 246. Although the most recent privacy impact assessment for CEN08 acknowledges the existence of the citizenship question through a single word ("Citizenship"), JA 153, the assessment contains no specific analysis of the impact of collecting citizenship status information. *See generally* JA 148–63.

EPIC, on its own behalf and on behalf of its members, sought out the privacy impact assessment for "CEN11 Demographic Census, Surveys, and Special Processing" by visiting the Census Bureau privacy impact assessment webpage. JA 164; *see also* JA 204, 207, 210. 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." JA 165; *see also* JA 249. Although the most recent privacy impact assessment for CEN11 acknowledges the existence of the citizenship question through a single word ("Citizenship"), JA 168, the assessment contains no specific analysis of the impact of collecting citizenship status information. *See generally* JA 164–76.

EPIC, on its own behalf and on behalf of its members, sought out the privacy impact assessment for "CEN13 Center for Economic Studies (CES)" by visiting the Census Bureau privacy impact assessment webpage. JA 177; *see also*

JA 204, 207, 210. 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[.]" JA 178; *see also* JA 249. 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. *See generally* JA 177–88.

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. JA 189; *see also* JA 204, 207, 210. CEN18 is an information system "used to deliver applications to end users of the U.S. Census Bureau network." JA 190. 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.*; *see also* JA 249. 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. *See generally* JA 189–201.

V. EPIC's prior warnings to the Census Bureau of E-Government Act noncompliance

Prior to filing a motion for a preliminary injunction in this case, EPIC notified the U.S. Census Bureau on four occasions that the Bureau was in violation of section 208 of the E-Government Act.

On August 7, 2018, EPIC filed comments with the Bureau about the proposed questions for the 2020 Census. EPIC, *Comments of EPIC to the U.S. Census Bureau* (Aug. 7, 2018), JA 211–16; *see also Proposed Information Collection; Comment Request; 2020 Census*, 83 Fed. Reg. 26,643 (June 8, 2018). EPIC stated that the Bureau had violated its privacy impact assessment obligations under section 208 and that the Bureau had "not undertaken an appropriate analysis of the privacy risks of the citizenship question." JA 215.

On October 2, 2018, EPIC published a statement to the Senate Committee on Homeland Security and Government Affairs concerning the nomination of Steven D. Dillingham to be Director of the Census. Statement from EPIC to Ron Johnson, Chairman, Senate Comm. on Homeland Sec. & Gov't Affairs, et al. at 4 (Oct. 2, 2018), JA 217–20. EPIC told the Committee (and the Bureau) that the Bureau was in violation of section 208 and "should conduct a new PIA dealing specifically with the issues raised by the citizenship question." JA 220.

On October 29, 2018, EPIC filed an amicus brief in *New York*, No. 18-CV-2921 (JMF), 2019 WL 190285, a case challenging the addition of the citizenship

question to the 2020 Census. EPIC explained the Bureau's privacy impact assessment obligations in detail and warned that "the Bureau has not adequately justified the collection of citizenship information or shown that it has implemented the safeguards necessary to protect the data that it collects." Br. of EPIC as Amicus Curiae in Supp. Pls.' Position at Trial at 20, *New York*, No. 18-CV-2921 (JMF), 2019 WL 190285 (S.D.N.Y. Jan. 15, 2019).

Finally, on November 20, 2018, EPIC filed the complaint in this case alleging that the agency had "failed to conduct *any* of the privacy analysis required by the E-Government Act for a major collection of personally identifiable information." Complaint ¶ 63 (Nov. 2, 2018) (emphasis in original), JA 47. EPIC charged that the Defendants violated the E-Government Act and Administrative Procedure Act ("APA") in two respects. First, EPIC alleged that the 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. JA 48–49 (Count I). Second, EPIC alleged that the Defendants unlawfully withheld production of required privacy impact assessments in violation of 5 U.S.C. § 706(1) and E-Government Act § 208(b). JA 49–50 (Count II). EPIC also brought a claim under the Declaratory Judgment Act, 28 U.S.C. § 2201(a). JA 50–51 (Count III). As relief, EPIC sought, *inter alia*, the

suspension and revocation of the citizenship question until the Bureau's completion and publication of the required privacy impact assessments. JA 51.

To date, the Census Bureau has not updated the privacy impact assessments for CEN05, CEN08, CEN11, CEN13, or CEN18 to include an analysis of how a citizenship question would impact privacy. The Department of Commerce recently reiterated, in a filing with the OMB, that the Bureau intends to collect citizenship status information through the 2020 Census. *See Submission for OMB Review*, 84 Fed. Reg. 3,748, 3,751 (Feb. 13, 2019). The Bureau has also stated that the "printing, addressing, and mailing of Internet invitations, reminder cards or letters, and paper questionnaire packages" for the 2020 Census will begin by June 2019. JA 11 (quoting U.S. Census Bureau, *2020 Census Operational Plan: A New Design for the 21st Century* at 89 (Sept. 2017)).

VI. The ruling of the court in New York v. U.S. Department of Commerce

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*, No. 18-CV-2921 (JMF), 2019 WL 190285, a case in which the plaintiffs challenged 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 *4, *89. 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 *125. On February 15, 2019, the Supreme Court granted the Government's petition for certiorari before judgment in *New York* and scheduled oral argument for "the second week of the April argument session." *Dep't of Commerce v. New York*, No. 18-966, 2019 WL 331100 (U.S. Feb. 15, 2019).

VII. EPIC's motion for a preliminary injunction

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, the district court (Hon. Dabney L. Friedrich) denied EPIC's motion for a preliminary injunction. JA 4–23; Order, JA 24. 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," JA 9 (citing Defs.' Opp'n at 1, 12), and the court acknowledged the "negative policy consequences" that can result "if an agency drags its feet in performing its PIA obligations." JA 20. The court also rejected the Bureau's arguments that EPIC's APA claims suffered from a "lack of ripeness or final agency action," JA 21 n.10. However, the court concluded that EPIC had failed to demonstrate a likelihood of success on the merits. Even though Secretary Ross's March 26, 2018 letter announcing the citizenship question "constitutes final agency action," JA 10, the court reasoned that the Bureau's duty to conduct, review, and publish the requisite privacy impact assessments will not come due "until the Bureau mails its first set of [census] questionnaires to the public in January 2020," JA 9–10—*i.e.*, after decision has been made to add the question to the census form, design the census form, print the census form, and deliver the census form, addressed to millions of American households, to the U.S. Postal Service. The court thus concluded that EPIC had failed to satisfy the four-part test for a preliminary injunction.

Although the district court found it "unnecessary to weight the remaining preliminary injunction factors," JA 15 (quoting *Doe v. Hammond*, 502 F. Supp. 2d 94, 102 (D.D.C. 2007), the court "[n]onetheless" went on to "address the plaintiff's three theories of irreparable harm[.]" *Id.* The court concluded, in dicta, that EPIC

had "not demonstrated a 'certain' injury 'of such imminence that there is a clear and present need for equitable relief to prevent irreparable harm.'" JA 17 (quoting *Wisconsin Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985)).

EPIC filed a notice of appeal from the district court's order on February 12, 2019.

SUMMARY OF THE ARGUMENT

The Court should reverse the judgment of the district court and enter a preliminary injunction to preserve the status quo and allow a full adjudication of EPIC's claims on the merits. EPIC has shown that it is entitled to such an injunction.

In taking final agency action to add a citizenship question to the 2020 Census, the Census Bureau initiated a new collection of personal information. Yet prior to this "consummation of the agency's decisionmaking process," *Bennett v. Spear,* 520 U.S. 154, 117 (1997), the Bureau failed to conduct, review, and publish the requisite privacy impact assessments addressing the privacy consequences of collecting the citizenship status of every person in the country. As a result, when the Bureau introduced the citizenship question, neither the Bureau nor the public had an informed understanding of the extraordinary privacy risks involved, the allowable uses of the data gathered, the less-invasive alternatives to the question, or any possible steps to mitigate the resulting privacy harms. Specifically, the

Census Bureau had failed to determine: what information would be collected; why the information was being collected; what the intended use of the information would be; with whom the information would be shared; what notice or opportunities for consent would be provided to individuals regarding the collection and sharing of the information; how the information would be secured; and whether a system of records was being created under the Privacy Act—the essential requirements of section 208. This uninformed data collection by a federal agency is precisely what the E-Government Act prohibits.

Because the Bureau has still failed to conduct and publish legally sufficient privacy impact assessments, EPIC and its members face ongoing, imminent, and irreparable harm. EPIC cannot evaluate the privacy impact of the citizenship question or scrutinize any privacy protections that might be put in place for the collection of their personal citizenship data. The privacy of EPIC's members is also unduly threatened by the Bureau's actions, which violate key privacy safeguards established by Congress.

Finally, the equities and public interest favor an injunction. EPIC and the public have a strong interest in avoiding the informational and privacy harms caused by the Bureau's conduct, while Bureau has no cognizable interest in unlawful agency action. And unless the Bureau is enjoined, the agency will soon

make an irretrievable commitment of resources toward an illegal collection of information. EPIC is entitled to a preliminary injunction.

STANDARD OF REVIEW

"This court reviews the district court's legal conclusions as to each of the four factors [of the preliminary injunction test] de novo, and its weighing of them"—if any—"for abuse of discretion." *League of Women Voters of United States v. Newby*, 838 F.3d 1, 6 (D.C. Cir. 2016). Moreover, "[t]his court can independently grant an injunction after considering the proper factors." *Id.* at 7 (citing *Chaplaincy of Full Gospel Churches v. England*, 454 F.3d 290, 305 (D.C. Cir. 2006)).

ARGUMENT

EPIC is entitled to a preliminary injunction because the Census Bureau's failure to conduct and publish legally required privacy impact assessments causes EPIC irreparable harm and conflicts with the public interest. A plaintiff is entitled to a preliminary injunction upon establishing "that [it] is likely to succeed on the merits, that [it] is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [its] favor, and that an injunction is in the public interest." *In re Navy Chaplaincy*, 697 F.3d 1171, 1178 (D.C. Cir. 2012) (quoting *Winter v. NRDC*, 555 U.S. 7, 20 (2008)).

Because EPIC readily satisfies each of these factors, the district court erred in denying EPIC's motion. Accordingly, this Court should reverse the district court's judgment and preliminarily enjoin the Defendants from taking any steps to collect—*i.e.*, "initiating the collection"—of citizenship information in the 2020 Census absent adequate privacy impact assessments. Such an order would "preserve the relative positions of the parties until a trial on the merits can be held." *Benisek v. Lamone*, 138 S. Ct. 1942, 1945 (2018) (quoting *University of Tex. v. Camenisch*, 451 U.S. 390, 395 (1981)).

I. EPIC IS LIKELY TO SUCCEED ON THE MERITS OF ITS CLAIMS.

EPIC is likely to prevail on its claims that the Census Bureau violated the E-Government Act and Administrative Procedure Act by failing to conduct and publish privacy impact assessments. Under section 208 of the E-Government Act, federal agencies must "conduct," "ensure the review of," and "make publicly available" a detailed privacy impact assessment "*before* . . . initiating a new collection of information that—"

> (I) will be collected, maintained, or disseminated using information technology; and
> (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

E-Government Act § 208(b)(1)(A) (emphasis added). Agencies must also "update[]" existing PIAs "where a system change creates new privacy risks." OMB Guidance § II.B.2, ADD 32.

The Census Bureau has failed to satisfy these obligations with respect to each of the five Bureau systems that will be used to collect, maintain, or disseminate citizenship status information.

A. The Census Bureau is required to complete and publish privacy impact assessments that address the privacy risks of collecting citizenship status information.

As the Census Bureau "concede[d]" below, the Bureau must "prepare PIAs that adequately address the collection of citizenship data in the 2020 Census." JA 9 (citing Defs.' Opp'n at 1, 12). Indeed, it is difficult to imagine a data collection activity more likely to trigger the obligations of section 208 than an effort by the Census Bureau to gather from every household in the United States sensitive personal information that could subject individuals to criminal prosecution.

The Census Bureau's collection of citizenship status information is a "new collection" of personally identifiable information that triggers the agencies' privacy impact assessment obligations. E-Government Act § 208(b)(1). An individual's citizenship status constitutes personally identifiable information because it "permit[s] the identity of [the] individual to whom the information applies to be reasonably inferred," E-Government Act § 208(d), when collected in

"combination [with] gender, race, birth date, geographic indicator, and other descriptors" demanded on the census. OMB Guidance § II.A.2, ADD 32. The Bureau admits as much. *See, e.g.*, JA 153 (listing "Citizenship" data among the "General Personal Data" handled by the CEN08 system).

The Census Bureau's collection of personal data concerning citizenship status is also "new." The Bureau did not collect citizenship status information through the 2010 Census, JA 221, which is the only other decennial census conducted since the E-Government Act was enacted in 2002. Secretary Ross himself acknowledged that the Bureau was undertaking a "reinstatement of a citizenship question" that had not been asked on "census surveys of the entire United States population" since 1950. JA 54, 60.

Finally, in deciding to collect citizenship status information from every person in the United States, the Bureau has imposed "identical reporting requirements" on "10 or more persons." E-Government Act § 208(b)(1)(A)(ii)(II); *see also* 13 U.S.C. § 221(a)–(b) (requiring all persons over 18 to respond to census questions). The Bureau is thus required to conduct and publish a fully compliant privacy impact assessment for each IT system that it will use to collect, maintain, or disseminate citizenship status information. *See* E-Government Act § 208(b)(1); JA 133; JA 149, 153; JA 165, 168; JA 178; JA 190.

Similarly, the Census Bureau's order initiating the collection of citizenship status information triggers the agencies' obligation to update and republish existing privacy impact assessments because "new information in identifiable form [is being] added to a collection" that "raises the risks to personal privacy[.]" OMB Guidance § II.B.2, ADD 32. On March 26, 2018—the day that the Bureau initiated a new collection of citizenship status information—each of the five IT systems slated to collect, maintain, or disseminate citizenship information was covered by a prior privacy impact assessment. JA 226–27. But none of those prior assessments addressed the extraordinary privacy implications of collecting and processing citizenship status information from every person in the United States. The Bureau was simply not engaged in such data collection prior to the March 26, 2018 order. By initiating the addition of "new information in identifiable form" to multiple Census Bureau IT systems, the Bureau therefore triggered its obligation to fully update the existing privacy impact assessments for those systems. OMB Guidance §§ II.B.2, II.B.2.i, ADD 32–33.

B. The Census Bureau has not yet completed and published privacy impact assessments that address the privacy risks of collecting citizenship status information.

The Census Bureau, in "conced[ing]" that it must still "prepare PIAs that adequately address the collection of citizenship data in the 2020 Census," also concedes that it has not yet completed and published the requisite assessments. JA

9 (citing Defs.' Opp'n at 1, 12) (emphasis added). The Bureau therefore failed to produce valid privacy impact assessments before Secretary Ross's March 26, 2018 order—and continues not to do so despite EPIC's repeated warnings and the initiation of this lawsuit.

To satisfy section 208 of the E-Government Act, an agency must publish a privacy impact assessment specifying, *inter alia*, "what information is to be collected"; "why the information is being collected"; "the intended use of the agency of the information"; "with whom the information will be shared"; and "how the information will be secured[.]" E-Government Act § 208(b)(2)(B)(ii). An assessment also "must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA." OMB Guidance § II.C.1.b, ADD 34.

The Census Bureau has not published a new or updated privacy impact assessment for any of the five systems that the Bureau proposes to use for the collection, maintenance, or dissemination of citizenship status information. With respect to three systems (CEN05, CEN13, and CEN18), the Bureau's failure is total. Although these systems would be used to maintain or process response data from the 2020 Census, the most recent privacy impact assessment for each system does not even acknowledge that citizenship status information is among the data "to be collected." E-Govermment Act § 208(b)(2)(B)(ii); *see also* JA 133, 136–

138; JA 178, 180–81; JA 190, 192–93. Consequently, the Bureau has entirely failed to assess the privacy impact of maintaining and processing personal data concerning citizenship status with these systems.

The current privacy impact assessments for two other Census Bureau systems (CEN08 and CEN11) acknowledge, with a single word, that citizenship status information will be collected. *See* JA 153 ("Citizenship"); JA 168 ("Citizenship"). Yet neither assessment includes any analysis—let alone a "commensurate" analysis, § 208(b)(2)(B)(i)—of how the collection of this new information will impact privacy. For example, neither assessment explains "why [citizenship] information is being collected" via the census for the first time in 70 years or what "the intended use of the agency of [citizenship] information" is. § 208(b)(2)(B)(ii); *see also* JA 148–63; JA 164–76.

The privacy impact assessments conducted and published by the Census Bureau to date do not permit the Bureau to "initiati[e] a new collection" of citizenship status information. E-Government Act § 208(b)(1)(A).

C. The Census Bureau was obligated to publish the required privacy impact assessments by March 26, 2018.

The deadline for the Census Bureau to conduct and publish the privacy impact assessments required by the E-Government Act was 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. In

holding otherwise, the district court misconstrued—and effectively gutted—section 208.

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 district court noted, JA 10, 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);[10] "to cause or facilitate the beginning of: set going," *Initiate*, Merriam-Webster (2019);[11] 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." JA 10 (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 continuous process or course of action—not a discrete, one-off action. *See, e.g.*, *Doe v. Bridgeport Police Dep't*, 434 F.

---

[10] http://www.oed.com/view/Entry/96066?rskey=wxG1jD&result=2&isAdvanced=false#eid.

[11] https://www.merriam-webster.com/dictionary/initiate.

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 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, the 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. 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*, 520 U.S. at 177–78) (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 district court—after acknowledging the expansive definitions of "initiate" and "collection of information"—adopted an artificially narrow construction of the combined phrase. Without explanation, the district court limited its analysis to just one possible meaning of "initiate" (*i.e.*, "begin"). JA 10. The court also elided the word "the" from the definition of "collection of information," converting 44 U.S.C. § 3502(3)(A) into a series verb phrases rather than gerunds. JA 10. Based on this construction, the district court concluded that the Bureau could postpone publication of the required privacy impact assessments until it *solicits* citizenship information—that is, "until the Bureau mails its first set of [census] questionnaires to the public in January 2020." *Id. Contra* 44 U.S.C. § 3902(a) (distinguishing between the "initiating" and "carrying out" of a process). This arbitrary temporal line cannot be squared with the plain text of the E-Government Act and PRA, the implementing OMB regulations, or the 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 ("NEPA"), 42 U.S.C. § 4321 *et seq*. *See Oglala Sioux Tribe v. U.S. Nuclear Regulatory Comm'n*,

896 F.3d 520, 532 (D.C. Cir. 2018) (quoting *Robertson v. Methow Valley Citizens Council*, 490 U.S. 332, 349 (1989)).

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 significant. *Knight v. Comm'r*, 552 U.S. 181, 188 (2008). Instead, Congress

recognized the "collection of information"—like the introduction of a new IT system—as a process that is initiated before any personal data is actually collected.

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 the district court is correct, and 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 "facts or opinions" for the 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. Presidential Advisory Comm'n on Election Integrity*, 878 F.3d 371, 380 (D.C. Cir. 2017) (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).[12] ("[T]he adoption dossier submitted by prospective adoptive parents . . . to initiate an adoption, will need to include the PAIR letter issued by 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 extensive 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 "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 §§ 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

---

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

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 (emphasis 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, it is likely that a comprehensive privacy impact assessment would lead (or would 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. *See* JA 53, 60; JA 153, 155, 157. 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).[13] 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.

Reading the E-Government Act in the way that the Bureau urges would contravene the plain text of 208, undermine the express purposes of the statute, and render the privacy impact requirement a functional nullity. The Court should decline to do so and should instead conclude that EPIC "is likely to succeed on the merits" of its claims. *Winter*, 555 U.S. at 22.

---

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

II. EPIC WILL SUFFER IRREPARABLE HARM ABSENT AN INJUNCTION.

This Court has never had the opportunity to apply the irreparable harm standard in a case concerning the timing of an agency's privacy impact assessment obligation under the E-Government Act. EPIC and its members are "likely to suffer irreparable harm" in several ways. *Doe v. Mattis*, 889 F.3d 745, 751 (D.C. Cir. 2018) (citing *Winter*, 555 U.S. at 20).

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.), *aff'd on other grounds*, 878 F.3d 371. EPIC and its members will also be irreparably harmed by "the failure of decision-makers" to take privacy "factors into account in the way that" the E-Government Act mandates. *Jones v. D.C. Redevelopment Land Agency*, 499 F.2d 502, 512 (D.C. Cir. 1974) (finding that the irreparable harm caused by failure to comply with NEPA's environmental assessment obligations is "imminent" when the agency has failed to comply with the statutory deadline). Finally, EPIC and its members will be irreparably harmed if the Bureau is permitted invade the privacy of EPIC's members by unlawfully compelling disclosure of their citizenship status.

First, the Census Bureau's failure to publish valid privacy impact assessments irreparably harms EPIC by denying EPIC's members information vital

to the national debate over the inclusion of the citizenship question on the 2020 Census. As the D.C. Circuit has emphasized, "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)); *see also Byrd v. EPA*, 174 F.3d 239, 244 (D.C. Cir. 1999) ("Byrd's injury, however, resulted from EPA's failure to furnish him with the documents until long after they would have been of any use to him."). Thus, "the non-disclosure of information to which a plaintiff is entitled, under certain circumstances itself constitutes an irreparable harm; specifically, where the information is highly relevant to an ongoing and highly public matter." *EPIC*, 266 F. Supp. 3d at 319; *see also EPIC v. DOJ*, 416 F. Supp. 2d 30, 41 (D.D.C. 2006) ("EPIC will also be precluded, absent a preliminary injunction, from obtaining in a timely fashion information vital to the current and ongoing debate surrounding the legality of the Administration's warrantless surveillance program."); *Washington Post v. DHS*, 459 F. Supp. 2d 61, 75 (D.D.C. 2006) ("Because the urgency with which the plaintiff makes its FOIA request is predicated on a matter of current national debate, due to the impending election, a likelihood for irreparable harm exists if the plaintiff's FOIA request does not receive expedited treatment.").

The collection of citizenship status information through the 2020 Census is inarguably "an ongoing and highly public matter." *EPIC*, 266 F. Supp. 3d at 319.

The Census Bureau has resolved to collect the citizenship status of hundreds of millions of persons nationwide, a controversial decision that has been the subject of tens of thousands of articles of interest to the public. *See "Census" and "Citizenship"*, Google News (Feb. 28, 2019)[14] (identifying more than 127,000 news articles containing the words "Census" and "Citizenship"). The Bureau's decision to initiate the collection of citizenship status information is the subject of numerous federal lawsuits,[15] one of which was significant enough to warrant a Supreme Court grant of certiorari before judgment. And the window for public debate is rapidly closing: the Bureau has stated that the "printing, addressing, and mailing of Internet invitations, reminder cards or letters, and paper questionnaire packages" for the 2020 Census must begin by June 2019. JA 11.

Moreover, the privacy impact assessments that the Census Bureau has unlawfully withheld are "highly relevant" to the ongoing debate over the planned citizenship question. *EPIC*, 266 F. Supp. 3d at 319. In failing to publish valid assessments, the Bureau has denied EPIC and its members critical details about the privacy risks of adding the citizenship question, leaving EPIC "little if any

---

[14] https://www.google.com/search?q=%22Census%22+and+%22Citizenship%22&tbm=nws.

[15] *See New York et al. v. U.S. Dep't of Commerce*, 351 F. Supp. 3d 502 (S.D.N.Y. 2019); *Kravitz v. U.S. Dep't of Commerce*, No. GJH-18-1041, 2018 WL 6830226; *La Union del Pueblo Entero v. Ross*, No. GJH-18-1570, 2018 WL 5885528 (D. Md. Nov. 9, 2018); *California et al. v. Ross*, Nos. 18-1865, 18-2279, 2018 WL 7142097 (N.D. Cal. Dec. 14, 2018).

information about prospective [] harms and potential mitigating measures." *Winter*, 555 U.S. at 23. The Bureau has thus irreparably harmed—and will continue to harm—the ability of EPIC's members to learn about and assess the privacy implications of collecting citizenship status information through the census. *See* JA 204; JA 207; JA 210.

The harms suffered by EPIC's members are also analogous to the harms at issue in cases under the National Environmental Policy Act. 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*, 896 F.3d at 523 (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 the assessment "combined with" the "concrete injury" of (1) the violation of EPIC and its members' right to information in the privacy impact assessment and (2) the imminent, unauthorized collection of EPIC's 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*, 490 U.S. at 349). 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*, 555 U.S. at 23. 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).

As the Supreme Court explained in *Winter*, "[p]art of the harm NEPA attempts to prevent in requiring an EIS is that, without one, there may be little if any information about prospective environmental harms and potential mitigating measures." 555 U.S. at 23. The same is true of privacy impact assessments conducted pursuant to the E-Government Act. The failure of the Bureau to take privacy risks into account when reviewing its proposed collection, as mandated by the E-Government Act, works an irreparable harm to those whose citizenship status information will be collected (including EPIC's members). That harm has already "mature[d]," in that the Bureau was "obliged to file the impact statement and fail[ed] to do so." *Jones*, 499 F.2d at 512.

Moreover, a preliminary injunction will ensure that compliance with the E-Government Act "take[s] place before there has been an 'irretrievable commitment of resources,'" *Jones*, 499 F.2d at 512 (quoting *Lathan*, 455 F.2d at 1121), such as the "printing, addressing, and mailing of Internet invitations, reminder cards or letters, and paper questionnaire packages" in June 2019. U.S. Census Bureau, *2020 Census Operational Plan: A New Design for the 21st Century*, *supra*, at 89. As the D.C. Circuit has explained regarding environmental impact statements:

> The purpose of equitable intervention in cases in which federal agencies have failed to comply with NEPA's requirements is to ensure that such compliance will take place before there has been an 'irretrievable commitment of resources.' It may be that preparation of the statement will, in the end, not move the agency from adherence to decisions it has already made. But it is not for the courts to prejudge. So long as the status quo is maintained, so long as the environmental impact statement is not merely a justification for a fait accompli, there is a possibility that the statement will lead the agency to change its plans in ways of benefit to the environment. It is this possibility that the courts should seek to preserve.

Jones, 499 F.2d at 512–13 (quoting *Lathan*, 455 F.2d at 1121); *cf. Pub. Employees for Envtl. Responsibility v. U.S. Fish & Wildlife Serv.*, 189 F. Supp. 3d 1, 2 (D.D.C. 2016) (quoting *Realty Income Tr. v. Eckerd*, 564 F.2d 447, 456 (D.C. Cir. 1977)) ("[W]hen an action is being undertaken in violation of NEPA, there is a presumption that injunctive relief should be granted against continuation of the action until the agency brings itself into compliance."). For the same reasons, the Court should issue a preliminary injunction here to preserve the possibility that the

Census Bureau will "change its plans in ways of benefit to" privacy. *Jones*, 499 F.2d at 512–13.

Finally, EPIC and its members will be irreparably harmed if the Census Bureau unlawfully acquires personal data concerning citizenship status from EPIC's members. The nonconsensual or compelled disclosure of one's personal information to a party who is not legally entitled to it constitutes irreparable harm. *United States v. Hubbard*, 650 F.2d 293, 314 n.73 (D.C. Cir. 1980) (finding a "serious threat of irreparable harm to the property and the privacy interests advanced" where the government seized documents from a church containing personal information of the church's members); *see also Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000) ("The harm at issue here—disclosure of confidential information—is the quintessential type of irreparable harm that cannot be compensated or undone by money damages."); *Nat'l Fed'n of Fed. Emps. v. Greenberg*, 789 F. Supp. 430, 438 (D.D.C. 1992) ("[I]rreparable injury flows not only from the employee's failure to complete the form or to complete it in a manner that the Department deems unacceptable; the intrusive nature of the compelled disclosure itself also constitutes such injury."), *vacated on other grounds*, 983 F.2d 286 (D.C. Cir. 1993). In the NEPA context, courts have found that much more indirect and intangible harms can be sufficient to satisfy the irreparable injury test. For example, in *Committee of 100 on Federal City*, the court

found that the potential removal of "approximately 200 trees, most of which are on public property," in an area near where one of the plaintiff's members lived, was sufficient to satisfy the irreparable injury prong in a challenge to the adequacy of a NEPA assessment related to a transit project. 87 F. Supp. 3d at 205.

III. THE EQUITIES AND THE PUBLIC INTEREST WEIGH IN FAVOR OF AN INJUNCTION.

The Court should enter a preliminary injunction as an equitable matter because "the balance of equities tips in [EPIC's] favor" and "an injunction is in the public interest." *Winter*, 555 U.S. at 22. These final two factors of the four-factor test "merge when the Government is the opposing party." *Nken v. Holder*, 556 U.S. 418, 435 (2009).

EPIC has a powerful equitable interest in avoiding the irreparable harms that will result if the Census Bureau continues its unlawful collection of citizenship status information without first conducting and publishing valid privacy impact assessments. For example, the equities favor enabling EPIC to review to the agency's assessment of privacy risks *before* the citizenship question is fully implemented. *See EPIC*, 266 F. Supp. 3d at 319 (holding that a denial of "information [that] is highly relevant to an ongoing and highly public matter" works an irreparable harm). Indeed, EPIC's informational interest in this matter is uniquely strong. EPIC is the premiere organization in the country working to enforce agencies' E-Government Act obligations, JA 26–28 (collecting EPIC PIA

cases), and EPIC has been a leading advocate of census privacy protections for nearly two decades, JA 28. As a membership organization dedicated to both privacy and open government, EPIC is uniquely equipped to evaluate the Bureau's PIAs and to inform EPIC's members and the public about the Bureau's compliance with the E-Government Act. *See* JA 26; EPIC, *EPIC FOIA Cases* (Sep. 17, 2018)[16] (collecting dozens of EPIC Freedom of Information Act cases resulting in the disclosure of thousands of privacy-related records). EPIC also has a strong equity in ensuring E-Government Act compliance "before there has been an 'irretrievable commitment of resources'" by the Bureau, *Jones*, 499 F.2d at 512 (quoting *Lathan*, 455 F.2d at 1121), and EPIC's members have an urgent need to avoid the unlawful collection of their citizenship status information. *See* JA 204, 207, 210.

The equities similarly favor an injunction because the Census Bureau has ignored four prior warnings from EPIC, including the filing of the Complaint in this matter, concerning the Bureau's noncompliance with section 208. First, on August 7, 2018, EPIC explained in comments to the Census Bureau that the Bureau had "not undertaken an appropriate analysis of the privacy risks of the citizenship question." JA 215. Second, on October 2, 2018, EPIC published a statement to the Senate Committee on Homeland Security & Government Affairs urging—in advance of a hearing on the Census—that the Bureau "should conduct a

[16] https://www.epic.org/foia/.

new PIA dealing specifically with the issues raised by the citizenship question." JA 220. Third, on Oct. 29, 2018, EPIC filed an amicus brief in *New York v. Department of Commerce* arguing that "the Bureau has not adequately justified the collection of citizenship information or shown that it has implemented the safeguards necessary to protect the data that it collects." Br. of EPIC as Amicus Curiae in Supp. Pls.' Position at Trial at 20, *New York*, No. 18-CV-2921 (JMF), 2019 WL 190285. Finally, on Nov. 20, 2018, EPIC filed a complaint in this case alerting the Defendants that they had "failed to conduct any of the privacy analysis required by the E-Government Act for a major collection of personally identifiable information." JA 48. Despite these repeated warnings from EPIC over the past seven months, the Bureau has still failed to bring itself into compliance with section 208.

There are few, if any, equities "to overcome the much more substantial countervailing harms" to EPIC. *Newby*, 838 F.3d at 13. Although federal agencies and the public have an interest in the sound administration of federal law, "there is generally no public interest in the perpetuation of unlawful agency action." *Id.* at 12 (citing *Pursuing America's Greatness v. FEC*, 831 F.3d 500, 511-12 (D.C. Cir. 2016); *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013)). To the contrary: "there is a substantial public interest in having governmental agencies abide by the federal laws that govern their existence and operations." *Id*.

Neither the Census Bureau nor the public at large has a cognizable interest in the collection of citizenship status information absent the required assessments of privacy risks. Congress has already balanced the competing interests of privacy and data collection by enacting E-Government § 208(b), which prohibits collection without assessment. The Court should not hesitate to equitably enforce that Congressionally-struck balance. *Cf. Realty Income Tr.*, 564 F.2d at 456 ("[W]hen an action is being undertaken in violation of NEPA, there is a presumption that injunctive relief should be granted against continuation of the action until the agency brings itself into compliance."); *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 609–10 (1952) (Frankfurter, J., concurring). ("When Congress itself has struck the balance, has defined the weight to be given the competing interests, a court of equity is not justified in ignoring that pronouncement under the guise of exercising equitable discretion.").

Even if the Census Bureau were legally permitted to collect citizenship status information without first evaluating the attendant privacy risks, the public interest would strongly disfavor such a collection. Permitting federal agencies to collect personal data without first conducting a privacy impact assessment endangers privacy and curtails public understanding of government decisionmaking. That is why Congress imposed a government-wide privacy impact assessment requirement in the first place: "[t]o make the Federal Government more

transparent and accountable" and "to ensure sufficient protections for the privacy of personal information[.]" E-Government Act §§ 2(b)(9), 208(a). Nowhere is the duty to assess privacy risks more important than the decennial census, a "unique" and compulsory collection of data that "reaches every population group, from America's long-time residents to its most recent immigrants." Presidential Proclamation No. 7,286, 65 Fed. Reg. at 17,985. Moreover, the public interest leans heavily against the implementation of the citizenship question because—as the Census Bureau's chief scientist recently noted—adding the question would be "very costly, harms the quality of the census count, and would [result in] substantially less accurate citizenship status data than are available from administrative sources." JA 96.

The public interest also favors injunctive relief at this stage because there is likely to be an "irretrievable"—and potentially wasteful—"commitment of resources" by the Census Bureau absent a preliminary order halting the citizenship question. *Jones*, 499 F.2d at 512 (quoting *Lathan*, 455 F.2d at 1121). As the Bureau has argued, "finalizing the decennial census questionnaire is time-sensitive," and it is "important to resolve as soon as possible" the key legal issues concerning the 2020 Census. Petition for a Writ of Mandamus at 15, *In re Dep't of Commerce*, No. 18-557, 2018 WL 5458822 (U.S. Nov. 16, 2018). If no injunction issues prior to final judgment in this case, the Bureau will likely expend significant

resources in the meantime implementing the citizenship question—a question that this Court may later deem unlawful. *See, e.g.*, U.S. Census Bureau, *2020 Census Operational Plan: A New Design for the 21st Century*, *supra*, at 89 (noting that the "printing, addressing, and mailing of Internet invitations, reminder cards or letters, and paper questionnaire packages" for the 2020 Census will begin by June 2019).

Because the balance of the equities and the public interest strongly favor a halt to the Census Bureau's implementation of the citizenship question, the Court should grant EPIC's motion for a preliminary injunction. The requested injunction is carefully tailored to address the privacy implications of the citizenship question and poses no impediment to other census operations or questions.

CONCLUSION

For the foregoing reasons, this Court should reverse the judgment of the lower court and issue a preliminary injunction halting the implementation of the Defendants' March 26, 2018 decision to add a citizenship question to the 2020 Census.

Respectfully Submitted,

Dated: March 1, 2019

MARC ROTENBERG
EPIC President

ALAN BUTLER
EPIC Senior Counsel

/s/ John L. Davisson
JOHN L. DAVISSON
EPIC Counsel

Electronic Privacy Information Center
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

davisson@epic.org

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6). The brief is composed in a 14-point proportional typeface, Times New Roman, and complies with the word limit of Fed. R. App. P. 32(a)(7)(B)(iii) and D.C. Cir. R. 32(e), because it contains 12,945 words, excluding parts of the brief exempted under Fed. R. App. P. 32(a)(7)(B)(iii).

/s/ John L. Davisson
JOHN L. DAVISSON
EPIC Counsel

CERTIFICATE OF SERVICE

I, John Davisson, hereby certify that on March 1, 2019, I electronically filed the foregoing document with the Clerk of the Court for the United States Court of Appeals for the D.C. Circuit by using the CM/ECF system. The following participants in the case will be served by email and the CM/ECF system:

Mark B. Stern, Attorney
Email: mark.stern@usdoj.gov
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530

Sarah Carroll
Email: sarah.w.carroll@usdoj.gov
U.S. Department of Justice
(DOJ) Civil Division, Appellate Staff
Firm: 202-514-2000
950 Pennsylvania Avenue, NW
Washington, DC 20530

/s/ John L. Davisson
JOHN L. DAVISSON
EPIC Counsel