No. 18-966

IN THE
Supreme Court of the United States

DEPARTMENT OF COMMERCE, ET AL.,
Petitioners,

v.

STATE OF NEW YORK, ET AL.,
Respondents.

On Writ of Certiorari Before Judgment to the United States Court of Appeals for the Second Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND TWENTY-THREE LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF RESPONDENTS

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
JOHN DAVISSON
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

April 1, 2019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues, to promote government transparency, and to protect privacy, the First Amendment, and other constitutional values.

EPIC has filed many amicus briefs before this Court and other federal courts concerning the protection of privacy. *See, e.g.*, Brief of *Amicus Curiae* EPIC et al., *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402) (arguing that technological changes since the era of analog phones justify departing from the third party doctrine); Brief of *Amici Curiae* EPIC et. al, *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (No. 13-1339) (arguing that the violation of a consumer's privacy rights under federal law constitutes an injury-in-fact sufficient to confer Article III standing); Brief of *Amici Curiae* EPIC et. al, *NASA v. Nelson*, 562 U.S. 134 (2011) (No. 09-530) (arguing that the Court should recognize the right to informational privacy).

EPIC filed an *amicus* brief in the present case in the Southern District of New York. *See* Brief of *Amicus Curiae* EPIC, *New York, et al. v. Dep't of Commerce, et al.*, 351 F.Supp.3d 502 (S.D.N.Y. 2019), *cert. granted sub. nom. Dep't of Commerce, et al. v. New York, et al.*, No. 18-966 (U.S. Feb. 15, 2019). EPIC has also filed

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

suit to block the citizenship question in the 2020 Census, alleging that the Bureau failed to complete privacy impact assessments required under the E-Government Act before initiating the collection of personally identifiable information. *EPIC v. Dep't of Commerce*, 356 F.Supp.3d 85 (D.D.C. 2019), *appeal docketed*, No. 19-5031 (D.C. Cir. Feb. 21, 2019).

EPIC has a long-standing interest in the privacy of census data. EPIC contributed directly to the revisions of the Census Bureau's "sensitive data" policy, Lynette Clemetson, *Census Policy on Providing Sensitive Data Is Revised*, N.Y. Times, (Aug. 31, 2004),[2] following an EPIC Freedom of Information Act ("FOIA") lawsuit which revealed that the DHS had improperly acquired data on Arab Americans from the Census Bureau after 9-11. EPIC, *Department of Homeland Security Obtained Data on Arab Americans From Census Bureau*;[3] Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*, N.Y. Times (July 30, 2004).[4] More recently, as a result of an EPIC FOIA request, EPIC uncovered emails from former Kansas State Secretary Kris Kobach to Commerce Secretary Wilbur Ross, recommending the addition of the citizenship question to the 2020 Census. EPIC also pursued a FOIA request to obtain the Census Bureau's analysis of the likely public response to the 2020 census if the Bureau chose to collect personal data regarding citizenship status. EPIC, *EPIC FOIA: EPIC Obtains Documents About Decision to Add Census*

---

[2] http://www.nytimes.com/2004/08/31/us/census-policy-on-providing-sensitive-data-is-revised.html.

[3] https://epic.org/privacy/census/foia.

[4] http://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html.

Citizenship Question (June 11, 2018).[5] In formal comments to the Census Bureau, EPIC opposed the decision to add a citizenship question to the 2020 census. *See* EPIC, Comment Letter on Proposed Information Collection; Comment Request; 2020 Census (Aug. 7, 2018).[6] In a formal statement to Congress, EPIC also urged that the Census Bureau remove the proposed citizenship question from the 2020 Census. *2020 Decennial Census: Hearing Before the H. Comm. on Oversight & Reform*, 116th Cong. (Mar. 14, 2019) (letter for the record submitted by EPIC).[7]

EPIC's brief is joined by the following distinguished experts in law, technology, and public policy.

Legal Scholars and Technical Experts

Anita L. Allen
Henry R. Silverman Professor of Law and Philosophy, Vice Provost, University of Pennsylvania Law School

James Bamford
Author and Journalist

Ann M. Bartow
Director, Franklin Pierce Center for Intellectual Property and Professor of Law, University of New Hampshire School of Law

Simon Davies
Publisher, the Privacy Surgeon, Fellow of the University of Amsterdam,

---

[5] https://epic.org/2018/06/epic-foia-epic-obtains-documen.html.

[6] https://epic.org/apa/comments/EPIC-Census-2020-August2018.pdf.

[7] *Available at* https://epic.org/testimony/congress/EPIC-HCOGR-Census-Mar2019.pdf.

Founder of Privacy International and EPIC Senior Fellow

Woodrow Hartzog
Professor of Law and Computer Science, Northeastern University School of Law

Jerry Kang
Korea Times—Hankook Ilbo Chair in Korean Am. Studies and Law, UCLA

Lorraine G. Kisselburgh
Lecturer and Fellow, Discovery Park, Purdue University

Chris Larsen
Executive Chairman, Ripple Inc.

Harry R. Lewis
Gordon McKay Professor of Computer Science, Harvard University

Gary T. Marx
Professor Emeritus of Sociology, MIT

Mary Minow
Library Law Consultant

Dr. Pablo Garcia Molina
Adjunct Professor, Georgetown University

Dr. Peter G. Neumann
Chief Scientist, SRI International Computer Science Lab

Helen Nissenbaum
Professor, Cornell Tech Information Science

Frank Pasquale
Professor of Law, University of Maryland Francis King Carey School of Law

Deborah C. Peel, M.D.
President of Patient Privacy Rights

Dr. Stephanie Perrin
President, Digital Discretion, Inc.

Bilyana Petkova
EPIC Scholar-in-Residence; Assistant Professor, Maastricht University

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School

Dr. Barbara Simons
IBM Research (retired)

Edward G. Viltz
President and Chairman, Internet Collaboration Coalition

Jim Waldo
Gordon McKay Professor of the Practice of Computer Science, John A. Paulson School of Engineering and Applied Sciences, Harvard University

Christopher Wolf
Board Chair, Future of Privacy Forum

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

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 Section 208 of the E-Government Act, which requires the Bureau to conduct and publish a privacy impact assessment before initiating a new collection of personal data.

The Bureau's addition of the citizenship question to the 2020 Census—a step taken without any evaluation of the resulting privacy risks—works a clear violation of Section 208. Collecting citizenship status information from hundreds of millions of U.S. residents presents enormous privacy and security concerns. As the history of the census reveals, response data pertaining to national origin is particularly susceptible to abuse. Nevertheless, the Bureau failed to conduct a privacy impact assessment before finalizing the citizenship question in March 2018. As a result, 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. This unscrutinized data collection by a federal agency

is precisely what the privacy impact assessment requirement of Section 208 is designed to prevent.

The Court should affirm the decision of the lower court enjoining the addition of the citizenship question to the 2020 Census.

ARGUMENT

EPIC recognizes the importance of the decennial census and encourages the use of aggregate data, derived from the census, in policymaking.[8] The census promotes evidence-based policy decisions, and census data is the source of much political and economic planning in the United States. However, the accuracy and integrity of the census depends on the assurance that the personal information collected by the Census Bureau will be used only by the Bureau and for purposes consistent with the census.

The importance of record confidentiality for census data is widely known. Many of the strictest privacy laws in the United States limit the collection, use, and disclosure of census data. *See* 13 U.S.C. § 9 ("Information as confidential"); 44 U.S.C. § 2108(b) ("Responsibility for custody, use, and withdrawal of records").[9]

---

[8] EPIC testified before the Commission on Evidence-Based Policymaking and called for the Commission to adopt innovative privacy safeguards to protect personal data and make informed public policy decisions. Marc Rotenberg, Commission on Evidence-Based Policymaking: Privacy Perspectives, before the National Academies of Science, Sept. 9, 2016, https://epic.org/privacy/wiretap/RotenbergCEBP-9-16.pdf.

[9] The Census Bureau cannot disclose "personally identifiable information about an individual to any other

These laws "are key to respondent trust and ultimately the credibility of the statistical indicators the agencies produce." Nat'l Acads. of Scis., Eng'g & Med., Innovations in Federal Statistics: Combining Data Sources While Protecting Privacy 20 (Robert M. Groves & Brian A. Harris-Kojetin eds., 2017). But the collection of personal data regarding citizenship status in the 2020 census raises substantial privacy concerns and threatens to undermine the accuracy and integrity of the census. Of particular concern to EPIC, the Census Bureau failed to complete the necessary privacy impact assessments, required by Section 208 of the E-Government Act of 2002, prior to the decision to collect this sensitive personal information. The agency's disregard of this core responsibility for the management of information systems in the federal government is all the more egregious because there is no dispute that the data associated with citizenship is the most consequential collection activity in the 2020 census.

I. Privacy protection ensures the accuracy, integrity, and reliability of the census.

As the Supreme Court has recognized, "Congress has broad power to require individuals to submit responses, an accurate census depends in large part on

---

individual or agency until 72 years after it was collected for the decennial census" pursuant to a 1952 agreement between the Archivist of the United States and the Census Bureau Director, which was subsequently codified by Congress in 1978, Pub. L. 94-416, 92 Stat. 915 (Oct. 5, 1978). *See* U.S. Dep't of Commerce, U.S. Census Bureau, *The "72-Year Rule"* (2018), https://www.census.gov/history/www/genealogy/decennial_census_records/the_72_year_rule_1.html.

public cooperation." *Baldrige*, 455 U.S. at 354 But the Court has also made clear, "to stimulate that cooperation Congress has provided assurances that information furnished . . . by individuals is to be treated as confidential." *Id*. The long history of the U.S. Census makes clear the importance of privacy protection and the risks to individuals when confidentiality is not preserved.

The first census in 1790 consisted of just six questions: the name of the head of the household and the number of inhabitants who were free white males 16 years and older, free white males under 16 years, free white females, free persons of any other color, and enslaved persons. U.S. Dep't of Commerce, U.S. Census Bureau, *Measuring America: The Decennial Censuses from 1790 to 2000* 5 (Sept. 2002).[10] From 1790 through 1840, no individual-level data was collected through the census. *Id*. at 6–7. During this period, a copy of the census schedule was posted in "two of the most public places" in each division for anyone to inspect. Act of Mar. 1, 1790 (for the enumeration of the inhabitants of the United States), ch. 2, § 7, 1 Stat. 101, 103; Act of Feb. 28, 1800 (to provide for the Second Census or enumeration of the inhabitants of the United States), ch. 13, § 7, 2 Stat. 11, 13; Act of Mar. 26, 1810 (providing for the Third Census or enumeration of the inhabitants of the United States), ch. 17, § 7, 2 Stat. 564, 568; Act of Mar. 14, 1820 (to provide for taking the Fourth Census, or enumeration of the inhabitants of the United States, and for other purposes), ch. 24, § 7, 3 Stat. 548, 552; Act of Mar. 23, 1830 (to provide for taking the Fifth Census or enumeration

---

[10] *Available at* https://www.census.gov/history/pdf/measuringamerica.pdf.

of the inhabitants of the United States), ch. 40, § 7, 4 Stat. 383, 387; Act of Mar. 3, 1839 (to provide for taking the Sixth Census or enumeration of the inhabitants of the United States), ch. 78, § 7, 5 Stat. 331, 335.

The scope of the census greatly expanded in 1850, as did concerns over privacy. Congress established a central processing office for census statistics, the Census Board, which was also delegated responsibility to design the 1850 census questions. Act of Mar. 3, 1849 (to make arrangements for taking the Seventh Census), ch. 115, 9 Stat. 402; *see also* Margo Anderson, *The American Census: A Social History* 42 (2015). After lobbying from a group of scholars and statisticians, the Board restructured the census to collect individual-level data. Anderson, *supra*, at 43. For the first time, the census required the names of every individual in a household, along with their age, sex, race, profession, place of birth, and whether the individual was "deaf and dumb, blind, insane, idiotic, [a] pauper, or [a] convict." *Measuring America*, *supra*, at 9–11. Census workers were no longer to post the completed schedules in public; instead, they were instructed about the importance of confidentiality. Carroll D. Wright & William C. Hunt, *History and Growth of the United States Census: 1790-1890*, S. Doc. No. 56-194, at 148–50 (1900). The Census Board informed its marshals and assistants:

> Information has been received at this office that in some cases unnecessary exposure has been made by the assistant marshals with reference to the business and pursuits, and other facts relating to individuals, merely to gratify curiosity, or the facts applied to the private use or pecuniary advantage of the assistant, to the

> injury of others. Such a use of the returns was neither contemplated by the act itself nor justified by the intentions and designs of those who enacted the law. No individual employed under sanction of the Government to obtain these facts has a right to promulgate or expose them without authority.

Id. at 150. The Census Office established other similar prohibitions in the years to come. In 1870, census takers were warned that "[n]o graver offense can be committed by assistant marshals than to divulge information acquired in the discharge of their duty. All disclosure should be treated as strictly confidential." *Id*. at 156. For the 1880 census, Congress added a confidentiality clause to the oath of office for enumerators, requiring them to swear that they would "not disclose any information contained in the schedules, lists, or statements obtained by [them] to any person or persons, except to [their] superior officers." Act of Mar. 3, 1879 (to provide for taking the tenth and subsequent censuses), ch. 195, § 7, 20 Stat. 473, 475. Breaking this oath, or communicating "any statistics of property or business" to a person not authorized to receive that information, was a misdemeanor carrying a fine up to $500. *Id*. at § 12. The 1890 census law removed "of property or business," forbidding communication of any information without authorization. Act of Mar. 1, 1889 (to provide for taking the eleventh and subsequent censuses), ch. 319, §13, 25 Stat. 760, 764.

Census privacy concerns continued into the early twentieth century. President Taft's proclamation on the 1910 census reveals a general fear not only that census takers would disclose individuals' responses,

but also that the federal government would use census data for law enforcement purposes:

> The sole purpose of the census is to secure general statistical information regarding the population and resources of the country, and replies are required from individuals only in order to permit the compilation of such general statistics. The census has nothing to do with taxation, with army or jury service, with the compulsion of school attendance, with the regulation of immigration, or with the enforcement of any national, state, or local law or ordinance, nor can any person be harmed in any way by furnishing the information required. There need be no fear that any disclosure will be made regarding any individual person or his affairs. For the due protection of the rights and interest of the persons furnishing information, every employee of the Census Bureau is prohibited, under heavy penalty, from disclosing any information which may thus come to his knowledge.

Proclamation of Mar. 15, 1910, 36 Stat. 2599. Subsequent presidents, including Woodrow Wilson in 1920, Herbert Hoover in 1930 and Franklin Roosevelt in 1940, would use almost the exact same language in their proclamations, indicating that the federal government continued to believe that assurances of privacy were integral to an accurate census. Proclamation No. 1540, 41 Stat. 1772 (Nov. 10, 1919); Proclamation No. 1898, 46 Stat. 3011, 3012 (Nov. 22, 1929);

Proclamation No. 2385, 5 Fed. Reg. 653 (Feb. 13, 1940).

Nevertheless, census data was used during this period for non-census purposes. The 1910 census law 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 July 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, during World War I, the Census Bureau did in fact disclose census records to the Department of Justice and local draft boards to help enforce the draft. 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 law that would become known as Title 13, which prohibited the Census 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. However, the Second War Powers Act weakened this restriction and permitted the Census 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)* 16 (Mar. 29-31, 2007)

(unpublished manuscript).[11] The Census 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).

Congress in 1962 established strict confidentiality rules for reports submitted to the Census Bureau. Pub. L. 87-813, 68 Stat. 1013 (1962) (codified as amended at 13 U.S.C. § 9). The confidentiality provision has been amended numerous times since then, and now reads:

> (a) Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, or local government census liaison, may, except as provided in [certain subsections]
>
> > (1) use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or
> >
> > (2) make any publication whereby the data furnished by any particular establishment or individual under this title can be identified; or
> >
> > (3) permit anyone other than the sworn officers and employees of the Department or bureau or

[11] *Available at* http://studylib.net/doc/7742798/census-confidentiality-under-the-second-war-powers.

> agency thereof to examine the individual reports.
>
> No department, bureau, agency, officer, or employee of the Government, except the Secretary in carrying out the purposes of this title, shall require, for any reason, copies of census reports which have been retained by any such establishment or individual. Copies of census reports which have been so retained shall be immune from legal process, and shall not, without the consent of the individual or establishment concerned, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding.

13 U.S.C. § 9.

The era of automated record-keeping presented new challenges for federal agencies, including the Census Bureau, and animated Congress to pass the Privacy Act in 1974. The Privacy Act was the legislative culmination of extensive research into the many threats to individual privacy and autonomy posed by the use of increasingly powerful computing systems across the federal government. One of the most influential studies to which the Congress looked when drafting the Privacy Act was the 1973 "HEW Report," chaired by RAND computer scientist Willis Ware. U.S. Dep't. of Health, Educ. & Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*

(1973).[12] The federal advisory committee that produced the report sought to determine the limitations that should be placed on the application of computer technology to record keeping about citizens. *Id.* at 33. The advisory committee foresaw that sensitive personal information could be compromised when compiled into vast databases that lacked regulatory oversight. *Id.* at 28. Ultimately, the HEW Report outlined a series of recommendations that became the basis of the Privacy Act of 1974.

While federal privacy protections have expanded since World War II, there continues to be a risk of misuse of census data. A 2004 EPIC Freedom of Information Act lawsuit 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 as well as 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* (2019);[13] Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*, N.Y. Times (July 30, 2004).[14] While the Census Bureau and Customs and Border Protection revised their data request policies following EPIC's FOIA case, Lynette Clemetson, *Census Policy on Providing Sensitive Data Is Revised*, N.Y. Times, (Aug.

---

[12] *Available at* https://www.epic.org/privacy/hew1973report/.

[13] https://epic.org/privacy/census/foia.

[14] http://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html.

31, 2004),[15] many Americans are justifiably fearful that their census responses will be used against them by other federal agencies, which can lead individuals to provide false or incomplete information. Mikelyn Meyers, Center for Survey Management, *U.S. Census Bureau, Presentation on Respondent Confidentiality Concerns and Possible Effects on Response Rates and Data Quality for the 2020 Census*, presented at National Advisory Committee on Racial, Ethnic, and Other Populations Fall Meeting (Nov. 2, 2017).[16]

Given the misuse of census data after 9/11, it is not difficult to see the risk in the decision to add the citizenship question to the 2020 census. Communications between the Department of Commerce, the Department of Justice, and the White House indicate that the Government plans to use personal data obtained from the citizenship question for purposes unrelated to the census and by agencies other than the Census Bureau. The Department of Justice purportedly intends to use the citizenship data in enforcing section 2 of the Voting Rights Act. Letter from Arthur E. Gary, Gen. Counsel, Justice Mgmt. Div., Dep't of Justice, to Ron Jamin, U.S. Census Bureau, at 1 (Dec. 12, 2017).[17] Through a 2018 FOIA request, EPIC obtained emails that revealed that Kris Kobach, former Vice Chair of the now-defunct Presidential Advisory Commission on Election Integrity, urged Secretary of

---

[15] http://www.nytimes.com/2004/08/31/us/census-policy-on-providing-sensitive-data-is-revised.html.

[16] https://www2.census.gov/cac/nac/meetings/2017-11/Meyers-NAC-Confidentiality-Presentation.pdf.

[17] https://www.documentcloud.org/documents/4340651-Text-of-Dec-2017-DOJ-letter-to-Census.html.

Commerce Wilbur Ross to add the citizenship question. Email from Kris Kobach, Sec'y, Kan. Dep't of State, to Wilbur Ross, Sec'y, Dep't of Commerce (July 21, 2017).[18]

EPIC's FOIA request also revealed a Census Bureau analysis of the impact of collecting personal data about citizenship status. U.S. Dep't of Commerce, U.S. Census Bureau, *Technical Review of the Dep't of Justice Request to Add Citizenship Question to the 2020 Census* (Jan. 19, 2018).[19] The Bureau concluded that adding a citizenship question is "very costly, harms the quality of the census count, and would use substantially less accurate citizenship status data than are available" from other government sources. *Id.* at 1. While the nine-page report shows that the Census Bureau considered, on some level, the consequences for accuracy in adding a census question, the Bureau has not given the same consideration to the privacy risks associated with the addition.

II. The Census Bureau failed to conduct a privacy impact assessment to evaluate the addition of the citizenship question as required by the E-Government Act of 2002.

The Census Bureau cannot lawfully collect citizenship information because it has failed to conduct an adequate Privacy Impact Assessment ("PIA") as mandated by the E-Government Act of 2002, Pub. L.

---

[18] https://epic.org/foia/censusbureau/EPIC-18-03-22-Census-Bureau-FOIA-20180611-Production-Kobach-Emails.pdf.

[19] https://epic.org/foia/censusbureau/EPIC-18-03-22-Census-Bureau-FOIA-20180611-Production-Technical-Review-Memo.pdf.

No. 107-347, 116 Stat. 2899. Although the Secretary of Commerce has ordered the Census Bureau to collect personal data about citizenship status, the Bureau has neither completed nor published an evaluation of the privacy and security risks posed by such data collection. Moreover, neither the Commerce Department or the Census Bureau disputes this point. *See EPIC v. U.S. Dep't of Commerce*, 356 F. Supp. 3d 85, 89 (D.D.C. 2019) (noting the defendants' "conce[ssion]" that they must "prepare PIAs that adequately address the collection of citizenship data in the 2020 Census"), *appeal docketed*, No. 19-5031 (D.C. Cir. Feb. 21, 2019). This matter is now pending before the U.S. Court of Appeals for the District of Columbia Circuit.

A. Agencies must conduct and publish a comprehensive privacy impact assessment before collecting personal data.

Under Section 208 of the E-Government Act, federal agencies (including the Census Bureau) must conduct, ensure the review of, and publish a privacy impact assessment *before* "initiating a new collection of information" that will be digitally stored or transmitted "in an identifiable form."[20] E-Government Act § 208(b)(1)(A)–(B). A privacy impact assessment, as defined by the Office of Budget and Management ("OMB"), is

> [A]n analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy

[20] Agencies must also conduct and publish a PIA before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form[.]" E-Government Act § 208(b)(1)(A)(i).

> 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.

Office of Mgmt. & Budget, OMB Circular A-130, Managing Information as a Strategic Resource 34 (2016) ("OMB Circular").[21] Section 208, in mandating that a privacy impact assessment be conducted and published before an agency begins the process of collecting personally identifiable information, serves Congress's objectives under the E-Government Act of "promot[ing] better informed decisionmaking by policy makers"; "provid[ing] enhanced access to Government information"; "mak[ing] the Federal Government more transparent and accountable"; and "ensur[ing] sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government." E-Government Act §§ 2(b)(7), 2(b)(9), 2(b)(11), 208(a).

To satisfy Section 208, a privacy impact assessment must disclose, *inter alia*, "what information is to be collected"; "why the information is being collected"; "the intended use [by] the agency of the information";

---

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

"with whom the information will be shared"; "what notice or opportunities for consent would be provided"; and "how the information will be secured." E-Government Act § 208(b)(2)(B)(ii). Crucially, the 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[.]" E-Government Act § 208(b)(2)(B)(i). "Simply put, a privacy impact assessment seeks to set forth, in as much detail as required to promote necessary understanding, the essential components of any personal information system or any system that contains significant amounts of personal information." David Flaherty, *Privacy Impact Assessments: An Essential Tool for Data Protection* (2000).[22]

Far from a simple box-checking exercise, a privacy impact assessment is the "the most comprehensive tool yet available for policy-makers to evaluate new personal data information technologies before they are introduced." Gary T. Marx, *Foreword*, in *Privacy Impact Assessment*, at v (David Wright & Paul De Hert, eds., 1st ed. 2012). As OMB regulations explain:

> 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

[22] http://www2.austlii.edu.au/privacy/secure/PLPR/2000/45.html.

> stages of the agency activity and throughout the information life cycle.

OMB Circular app. II at 10; *see also* Anita Ramasastry, *Lost in Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 Santa Clara Computer & High Tech. L.J. 757, 794 (2006) ("[P]erhaps the best way to begin to imagine how we can safeguard privacy in the wake of data mining is to require the government to provide robust data-mining privacy impact assessments.").

The privacy impact assessments required by the E-Government Act "are crafted to bring attention to privacy problems" and to enable agencies to correct those problems. Marc Rotenberg, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11*, at 19–20 (SSRN, Working Paper No. 933690, 2006). When agency officials conduct an assessment "that shows a program does not strictly comply or that adequate protections are not in place, the [agency's] Privacy Office should require that the program be revised to protect privacy rights." *Id.* at 31–32. In this way, a privacy impact assessment is a foundation for a federal agency "to develop better policy, to save money, to develop a culture of privacy protection, to prevent adverse publicity and to mitigate risks in advance of resource allocation." Robin M. Bayley & Colin J. Bennett, *Privacy Impact Assessments in Canada*, in *Privacy Impact Assessment* 161–62 (David Wright & Paul De Hert, eds., 1st ed. 2012); *see also* Marx, *supra*, at xi ("Privacy protection is not like a vaccination that occurs once and is over. Rather it is part of an enduring process involving a series of separate actions.").

Thus, an agency's privacy obligations under the E-Government Act do not end with the initial publication of a privacy impact assessment. As the OMB instructs:

> [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 Circular app. II at 10; *accord* U.S. Dep't of Commerce, Office of Privacy & Open Gov't, *Privacy Compliance* (July 9, 2018);[23] U.S. Dep't of Commerce, U.S. Census Bureau, *Policy on Conducting Privacy Impact Assessments* (Nov. 11, 2005).[24] Specifically, a PIA must be "updated as necessary where a system change creates new privacy risks," including "when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)" and "when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form[.]" Joshua B. Bolten, Dir., Office of Mgmt. & Budget, Executive Office of the President, M03-22, Memorandum for Heads of Executive Departments

---

[23] http://www.osec.doc.gov/opog/privacy/compliance.html.

[24] https://www2.census.gov/foia/ds_policies/ds019.pdf.

and Agencies, Attachment A § II.B.2.g–i (Sept. 26, 2003) ("OMB Guidance").

B. The Census Bureau did not assess the risk that personal data collected for the census could be transferred to other agencies and used for purposes unrelated to the census.

In failing to assess the risks that would result from the collection of personal data regarding citizenship status, the Census Bureau has violated its obligations under the E-Government Act.

On September 27, 2018, the Bureau issued the most recent privacy impact assessment for CEN08, the primary system used to collect, maintain, and disseminate census response data. U.S. Dep't of Commerce, U.S. Census Bureau, *Privacy Impact Assessment for the CEN08 Decennial Information Technology Division (DITD)* (Sept. 27, 2018).[25] Although the CEN08 assessment acknowledges the Bureau's plan to collect citizenship data, the Bureau devotes exactly *one word* to this far-reaching change: "Citizenship." *Id.* at 5. Alarmingly, the CEN08 assessment indicates 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." *Id.* at 5, 7, 9.

The current privacy impact assessments for the four other Bureau systems implicated in the 2020 Census fare no better. Like the CEN08 assessment, these

---

[25] http://www.osec.doc.gov/opog/privacy/Census%20PIAs/CEN08_PIA_SAOP_Approved.pdf [https://web.archive.org/web/20190327172612/http://www.osec.doc.gov/opog/privacy/Census%20PIAs/CEN08_PIA_SAOP_Approved.pdf].

assessments acknowledge the collection of citizenship data with no more than a single word—if at all. *See* U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN05 Field Systems Major Application System* (June 22, 2018) (including no reference to citizenship data); U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN11 Demographic Census, Surveys, and Special Processing* (June 22, 2018) (including a one-word reference to "Citizenship" data); U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN13 Center for Economic Studies (CES)* (June 26, 2018) (including no reference to citizenship data); U.S. Dep't of Commerce, *Privacy Impact Assessment for the CEN18 Enterprise Applications* (June 26, 2018) (including no reference to citizenship data).

The Bureau's one-word privacy "assessments" of the proposed citizenship question are utterly inadequate to satisfy Section 208 of the E-Government Act. First, these bare references to citizenship data plainly fall short of the Bureau's obligation to produce a privacy impact assessment that is "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[.]" E-Government Act § 208(b)(2)(B)(i). The proposed citizenship question would reach hundreds of millions of Americans and would elicit intensely private information concerning respondents' citizenship and immigration status. Second, the existing privacy impact assessments wrongly ignore that, by posing a citizenship question on the census, the Bureau would be collecting "new information in identifiable form [which] raises the risks to personal privacy . . . ." OMB Guidance § II.B.2.i. Census responses about citizenship status—compelled

by law—could easily be used to carry out deportations or for other law enforcement purposes, interfering wholesale with "the right to be let alone." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

Moreover, the Bureau's existing privacy impact assessments completely fail to address that citizenship data could (and likely would) be transferred to agencies and persons outside of the Census Bureau, creating privacy risks for respondents and undermining the purpose and integrity of the census. *See* OMB Guidance § II.B.2.g. For example, the Department of Justice ("DOJ") has demanded access to citizenship information collected through the census with the purported aim of calculating "the citizen voting-age population in localities where voting rights violations are alleged or suspected." Letter from Arthur E. Gary, Gen. Counsel, Justice Mgmt. Div., Dep't of Justice, to Ron Jamin, U.S. Census Bureau, at 1 (Dec. 12, 2017). The Bureau has also promised that if state officials "indicate a need for tabulations of citizenship data" for redistricting purposes, "the Census Bureau will make a design change to include citizenship as part of" the census data given to the states. Submission for OMB Review, 84 Fed. Reg. 3,748, 3,756 (Feb. 13, 2019). And, as noted, the CEN08 assessment indicates that census response data may be transferred in "[b]ulk" to other federal agencies "[f]or criminal law enforcement activities." *Id.* at 7, 9.

Even if citizenship data were "deidentified" before dissemination beyond the Census Bureau, there is a material risk of reidentification. As Dr. Latanya Sweeney has demonstrated, the "practice of de-identifying data and of ad hoc generalization" used by the

Census Bureau is "not sufficient to render data anonymous because combinations of attributes often combine uniquely to re-identify individuals." Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000).[26] Using census summary data and information from other readily available sources at the time, Dr. Sweeney "found that 87% . . . of the population in the United States had reported characteristics that likely made them unique based only on {5-digit ZIP, gender, date of birth}." *Id.*

In ignoring this serious threat to the privacy of census respondents, the Census Bureau has flouted its obligation under the E-Government Act to conduct a comprehensive privacy impact assessment for the collection of citizenship data.

C. The Census Bureau did not consider the data security risks posed by collecting additional sensitive information from every American household.

The Census Bureau's pro forma privacy impact assessments also fail to address the data security risks posed by the collection of citizenship information. Each year individuals face an increasing threat of data breach—a threat to which even the largest companies and government agencies have fallen victim. *See, e.g.*, Peter Neumann, *Every Computer System Can Be Compromised*, N.Y. Times (Oct. 6, 2014);[27] Bruce Schneier,

---

[26] https://dataprivacylab.org/projects/identifiability/paper1.pdf.

[27] https://www.nytimes.com/roomfordebate/2014/10/04/keeping-credit-cards-and-bank-account-

Internet Hacking Is About to Get Much Worse, N.Y. Times (Oct. 11, 2018).[28] Yet the Bureau's privacy impact assessments fail to address the risk that citizenship information might be improperly accessed, both during and after the Bureau's collection of such data. These are serious concerns that deserve serious attention from the Bureau. Absent a thorough evaluation of these security and privacy risks, the Bureau should not be permitted to introduce the citizenship question.

In June 2018, the Government Accountability Office (GAO) reported that the Census Bureau had acknowledged "3,100 security weaknesses that will need to be addressed in the coming months." Gov't Accountability Office, GAO-18-655, 2020 Census: Continued Management Attention Needed to Address Challenges and Risks with Developing, Testing, and Securing IT Systems (Aug. 2018).[29] The GAO stated that "it will be important that the Bureau addresses system security weaknesses in a timely manner and ensures that risks are at an acceptable level before systems are deployed." *Id*. According to the GAO, the Census Bureau had failed—as of August—to meet its own schedule for recruiting key personnel necessary to secure the system and to "incorporate lessons learned to date from the 2018 End-to-End Test." *Id.* at 11. Moreover, the Bureau had not "identified a specific time frame for completing these efforts." *Id*. The GAO had previously warned that the "tight time frames" involved in the 2020 Census changes "could exacerbate"

---

data-from-hackers/every-computer-system-can-be-compromised.

[28] https://www.schneier.com/essays/archives/2018/10/internet_hacking_is_.html.

[29] https://www.gao.gov/assets/700/694169.pdf.

the "significant challenges" that the agency faces in ensuring adequate cybersecurity measures. *Id.* at 17.

Given the risk that sensitive census data will be improperly accessed or breached, 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.

CONCLUSION

For the above reasons, *amici* respectfully ask this Court to affirm the decision of the U.S. District Court for the Southern District of New York.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
JOHN DAVISSON
MEGAN IORIO
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
(202) 483-1248 (fax)
rotenberg@epic.org

April 1, 2019