IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

STATE OF NEW YORK, *ET AL.*, Plaintiffs, v. UNITED STATES DEPARTMENT OF COMMERCE, *ET AL.*, Defendants.	Case No. 1:18-cv-2921 (JMF)

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFFS' POSITION AT TRIAL

Respectfully Submitted,

Marc Rotenberg
EPIC President and Executive Director
Alan Butler (pro hac vice)
EPIC Senior Counsel
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140
Counsel for the Electronic Privacy Information Center

TABLE OF CONTENTS

TABLE OF AUTHORITIES

INTEREST OF THE AMICUS

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC frequently participates as *amicus curiae* in federal and state court cases that implicate emerging privacy issues. EPIC was directly involved in the 2004 effort to revise the Census Bureau "sensitive data" policy after an EPIC Freedom of Information Act lawsuit revealed that the DHS had acquired data on Arab Americans from the Census Bureau after 9-11. In formal comments to the Census Bureau this year, EPIC has 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).[1] Through a FOIA request earlier this year, EPIC also uncovered emails from Kris Kobach urging Secretary Ross, on the direction of Steven Bannon, to add the citizenship question, and the Census Bureau's analysis of the impact of asking about citizenship. EPIC, *EPIC FOIA: EPIC Obtains Documents About Decision to Add Census Citizenship Question* (2018).[2]

The U.S. Census Bureau's collection of personal data implicates numerous privacy issues. *See* EPIC, *The Census and Privacy* (2018).[3] History has shown that personal data, collected by the government through the census, can threaten individual rights. In some countries, the misuse of census data has produced

[1] https://epic.org/apa/comments/EPIC-Census-2020-August2018.pdf.
[2] https://epic.org/2018/06/epic-foia-epic-obtains-documen.html.
[3] https://epic.org/privacy/census/.

horrific outcomes. The decision to add a citizenship question to the 2020 census should be suspended pending the completion of an updated Privacy Impact Assessment. The Bureau has failed to demonstrate that the collection of citizenship data will not undermine the rights of those who respond to the census.

ARGUMENT

EPIC supports the work of the Census Bureau and the use of aggregate data, derived from the census, in policymaking.[4] The census helps ensure 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 for purposes consistent with the census.

EPIC knows that the Census Bureau is committed to record confidentiality, Ron Jarmin, *The U.S. Census Bureau's Commitment to Confidentiality*, Census Blog (May 7, 2018),[5] and that some of the strictest privacy laws in the United States apply to census data. *See* 44 U.S.C. § 2108.[6] But the addition of the citizenship question to the 2020 census raises substantial privacy concerns and threatens to

[4] 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, Sep. 9, 2016, https://epic.org/privacy/wiretap/RotenbergCEBP-9-16.pdf.

[5] https://census.gov/newsroom/blogs/director/2018/05/the_u_s_census_bure.html.

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

undermine the accuracy and integrity of the census. And the Census Bureau has failed to satisfy its privacy obligations including, in particular, its obligations under the E-Government Act of 2002. The Bureau simply failed to assess the privacy risks of the citizenship question, perhaps the single most controversial change in the 2020 census.

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

As the Supreme Court has recognized, "[a]lthough Congress has broad power to require individuals to submit responses, an accurate census depends in large part on public cooperation. To stimulate that cooperation Congress has provided assurances that information furnished . . . by individuals is to be treated as confidential." *Baldrige v. Shapiro*, 455 U.S. 345, 354 (1982). But as technology and the format of the census evolve, so too do the privacy risks. The history of the census shows that it is essential to protect privacy in order to conduct an accurate census.

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 (Sep. 2002).[7] 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

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

(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 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 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, 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 Jun. 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).[8] 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).

The digital era presented new challenges for federal recordkeeping, including the census, and animated Congress to pass the Privacy Act in 1974. The Privacy Act

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

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 and databases. One of the most influential studies to which the Congress looked when drafting the Privacy Act was the 1973 "HEW Report." 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).[9] 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 and 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*;[10] Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*,

[9] *Available at* https://www.epic.org/privacy/hew1973report/.
[10] https://epic.org/privacy/census/foia.

N.Y. Times (Jul. 30, 2004).[11] While the Census Bureau and Customs and Border Protection revised their data request policies following EPIC's FOIA case, 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. U.S. Customs and Border Protection, *Policy for Requesting Information of a Sensitive Nature from the Census Bureau* (Aug. 9, 2004);[12] Census Bureau News, *U.S. Census Bureau Announces Policy Regarding Sensitive Data*, press release CB04-145, August 30, 2004; Lynette Clemetson, *Census Policy On Providing Sensitive Data Is Revised*, N.Y. Times, (Aug. 31, 2004);[13] 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).[14]

Given EPIC's earlier monitoring of 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 answers to questions about citizenship for purposes unrelated to the census. The Department of Justice intends to use the citizenship data in enforcing Section 2 of the Voting Rights Act. Letter from Arthur E. Gary, Gen. Counsel, Justice Mgmt.

---

[11] http://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html.
[12] https://epic.org/privacy/census/foia/policy.pdf.
[13] http://www.nytimes.com/2004/08/31/us/census-policy-on-providing-sensitive-data-is-revised.html.
[14] https://www2.census.gov/cac/nac/meetings/2017-11/Meyers-NAC-Confidentiality-Presentation.pdf.

Div., Dep't of Justice, to Ron Jamin, U.S. Census Bureau, at 1 (Dec. 12, 2017).[15] Through a FOIA request earlier this year, EPIC obtained emails that revealed that Kris Kobach, former Vice Chair of the now-defunct Presidential Advisory Commission on Election Integrity, urged Secretary Ross to add the citizenship question "on the direction of Steven Bannon," which indicates that interest in the citizenship question was not confined to the Department of Justice. Email from Kris Kobach, Sec'y, Kan. Dep't of State, to Wilbur Ross, Sec'y, Dep't of Commerce (Jul. 21, 2017).[16]

EPIC's FOIA request also revealed a Census Bureau analysis of the impact of asking the citizenship question. 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).[17] 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.

[15] https://www.documentcloud.org/documents/4340651-Text-of-Dec-2017-DOJ-letter-to-Census.html.
[16] https://epic.org/foia/censusbureau/EPIC-18-03-22-Census-Bureau-FOIA-20180611-Production-Kobach-Emails.pdf.
[17] https://epic.org/foia/censusbureau/EPIC-18-03-22-Census-Bureau-FOIA-20180611-Production-Technical-Review-Memo.pdf.

II. The Census Bureau did not conduct a Privacy Impact Assessment that assessed 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 failed to conduct an adequate Privacy Impact Assessment ("PIA") as mandated by the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899. The Bureau issued a cursory PIA for the division that maintains and processes census response data, but the Bureau entirely failed to address the security risks posed by collecting citizenship information or the possibility that such data could be transferred to other agencies and used for purposes unrelated to the census.

A. Agencies must conduct and publish a comprehensive Privacy Impact Assessment before collecting personally identifiable information or imposing new privacy risks.

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."[18] E-Government Act § 208(b)(1)(A)–(B). A PIA, as defined by the Office of Budget and Management ("OMB"), is

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

[18] 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).

Joshua B. Bolten, Dir., Office of Mgmt. & Budget, Executive Office of the President, M03-22, Memorandum for Heads of Executive Departments and Agencies, Attachment A § II.A.6 (Sept. 26, 2003) ("OMB Guidance"). Section 208, in mandating that a PIA be conducted and published before an agency collects personally identifiable information, serves Congress's dual objectives under the E-Government Act of "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)(9), 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"; "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 PIA 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 Protectio*n (2000).[19]

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); *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 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 a PIA "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 PIA 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*

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

(Wright & Hert eds.), *supra*, at 161–62; *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.").

Accordingly, an agency's privacy obligations under the E-Government Act do not end with the initial publication of a Privacy Impact Assessment. Rather, a PIA must be revised continually "to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form." OMB Guidance § II.B.d; *accord* U.S. Dep't of Commerce, Office of Privacy & Open Gov't, *Privacy Compliance* (July 9, 2018);[20] U.S. Dep't of Commerce, U.S. Census Bureau, *Policy on Conducting Privacy Impact Assessments* (Nov. 11, 2005).[21] 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[.]" OMB Guidance § II.B.2.g–i; *accord* Office of Privacy & Open Gov't, *Privacy Compliance*, *supra*.

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

In failing to assess the risks that would result from the collection of

[20] http://www.osec.doc.gov/opog/privacy/compliance.html.
[21] https://www2.census.gov/foia/ds_policies/ds019.pdf.

citizenship data, the Census Bureau has violated its obligations under the E-Government Act. On June 26, 2018, the Bureau issued a revised Privacy Impact Assessment for the collection, maintenance, and dissemination of census response data. U.S. Dep't of Commerce, U.S. Census Bureau, *Privacy Impact Assessment for the CEN08 Decennial Information Technology Division (DITD)* (Jun. 26, 2018), Ex. 1. The June 28 PIA marked the first time the Bureau had evaluated the privacy implications of census data collection since August 2014. *See* U.S. Dep't of Commerce, Office of Privacy & Open Gov't, *U.S. Census Bureau Privacy Impact Assessments (PIAs) and Privacy Threshold Analysis (PTA)* (Apr. 24, 2017).[22] Although the June 28 PIA acknowledges that the Bureau would be collecting citizenship data, the Bureau devotes exactly *one word* to this far-reaching change:

b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address	X	o. Medical Information	
d. Gender	X	j. Telephone Number	X	p. Military Service	
e. Age	X	k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity	X	l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): Citizenship					

Ex. 1 at 3. Remarkably, the Bureau stated that change is merely for "an existing information system without changes that create new privacy risks." *Id.* at 2.[23] The decision to add the citizenship question to the 2020 census is arguably the most consequential decision of the Bureau in recent history. As the Pew Research Center

[22] https://web.archive.org/web/20170505015624/http://www.osec.doc.gov/opog/privacy/Census-pias.html.

[23] On September 27, 2018, the Census Bureau issued a further revision to the CEN08 PIA to address the collection and use of fingerprinting data collected from census workers. U.S. Census Bureau, *Privacy Impact Assessment for the CEN08 Decennial Information Technology Division (DITD)* (Sep. 27, 2018), http://www.osec.doc.gov/opog/privacy/Census%20PIAs/CEN08_PIA_SAOP_Approved.pdf. However, this PIA contained no new information concerning the Bureau's collection of citizenship data.

stated plainly, "[f]or the first time since 1950, the U.S. Census Bureau is planning to ask everyone living in the United States whether they are citizens when it conducts its next decennial census in 2020." D'Vera Cohen, *What to Know About the Citizenship Question the Census Bureau is Planning to Ask in 2020*, Pew Research Center (Mar. 30, 2018).[24]

The Bureau's one-word privacy "assessment" of the proposed citizenship question is utterly inadequate to satisfy section 208 of the E-Government Act. First, it plainly violates the Bureau's obligation to produce a PIA 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 be posed to an estimated 325 million people and would elicit intensely private information concerning respondents' citizenship and immigration status. U.S. Dep't of Commerce, U.S. Census Bureau, *QuickFacts* (2017).[25] Second, the revised PIA wrongly ignores 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; *see* Ex. 1 at 2. Census responses about citizenship status—compelled by law—could easily be used for deportation or other purposes, interfering wholesale with "the right to be let alone." Samuel D. Warren & Louis D. Brandeis, *The Right*

[24] http://www.pewresearch.org/fact-tank/2018/03/30/what-to-know-about-the-citizenship-question-the-census-bureau-is-planning-to-ask-in-2020/.
[25] https://www.census.gov/quickfacts/fact/table/US/AGE775217.

to Privacy, 4 Harv. L. Rev. 193 (1890).

Moreover, the PIA completely fails to address that citizenship data could (and likely would) be transferred to agencies and persons outside of the Census Bureau, creating 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 on 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 DOJ has also called on the Bureau to publicly "release this new data regarding citizenship at the same time it releases the other redistricting data[.]" *Id.* at 3.

It is not apparent whether the DOJ expects the Census Bureau to disaggregate citizenship data from the names, addresses, and other personal information of respondents before transferring or publishing that data. But even if citizenship data were "deidentified," there is a 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]

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

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.* More recent work by the National Academies of Sciences suggests that privacy-preserving techniques and privacy enhancing techniques may provide more robust approaches for deidentification. *See* Nat'l Academies of Sciences, Engineering, & Medicine, *Federal Statistics, Multiple Data Sources, and Privacy Protection: Next Steps* (2017).

In ignoring this serious threat to the privacy of census respondents, the Census Bureau has flouted its obligation to conduct a comprehensive Privacy Impact Assessment under the E-Government Act.

C. The Bureau did not consider the data security risks posed by collecting additional sensitive information on such a large scale.

The Census Bureau's pro forma Privacy Impact Assessment fails to consider uses of the sensitive citizenship information that the agency proposes to collect, and does not address the data security risks of the proposal. Each year individuals face an increasing threat of data breach, which even the most well-established companies and government agencies have fallen victim too. *See* Peter Neumann, *Every Computer System Can Be Compromised*, N.Y. Times (Oct. 6, 2014);[27] Bruce Schneier, *Internet Hacking Is About to Get Much Worse*, N.Y. Times (Oct. 11,

[27] https://www.nytimes.com/roomfordebate/2014/10/04/keeping-credit-cards-and-bank-account-data-from-hackers/every-computer-system-can-be-compromised.

2018).[28] U.S. Government databases have been no exception to external cyberattacks, as illustrated by increasingly serious agency data breaches over the past ten years. The Bureau's assessment fails to address risks of data breach, improper access to census response data, and reidentification of individuals based on block-level data. The Bureau also failed to address the systematic risks posed by conducting the census entirely online. These are serious concerns that deserve serious attention by the Bureau, and absent a thorough consideration of these risks the census should not be modified as the agency has proposed.

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) [hereinafter August 2018 GAO Report].[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*. So far, the GAO reported, the Census Bureau has failed to meet its own schedule for recruiting key personnel necessary to secure the system and for "incorporate lessons from the 2018 End-to-End Test," and the Bureau had not (as of August) "identified a specific time frame for completing these efforts." *Id*. at 11. The GAO had previously warned that the "tight time frames" involved in the 2020 census changes "could exacerbate" the

[28] https://www.schneier.com/essays/archives/2018/10/internet_hacking_is_.html.
[29] https://www.gao.gov/assets/700/694169.pdf.

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

Given the risk that sensitive census data will be exposed to breach or improper access, 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 foregoing reasons, the Court should sustain the Plaintiffs' challenge to the Census Bureau's inclusion of a citizenship question in the 2020 Census.

Dated: October 29, 2018

Respectfully Submitted,

Marc Rotenberg
EPIC President and Executive Director

/s/ Alan Butler
Alan Butler (pro hac vice)
EPIC Senior Counsel
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140
Counsel for the Electronic Privacy Information Center