UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF ALABAMA
EASTERN DIVISION

THE STATE OF ALABAMA, *et al.*

Plaintiffs,

v.

UNITED STATES DEPARTMENT OF COMMERCE, *et al.*

Defendants.

No. 3:21–cv–00211–RAH–ECM–KCN

BRIEF OF AMICUS CURIAE ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF DEFENDANTS' RESPONSE IN OPPOSITION TO PLAINTIFFS' MOTION FOR PRELIMINARY INJUNCTION AND PETITION FOR WRIT OF MANDAMUS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy issues. EPIC routinely participates as amicus in federal and state courts, including in cases regarding the collection, use, and disclosure of personal data by government agencies. *See, e.g.*, Brief of Amicus Curiae EPIC, *Bozzi v. Jersey City*, No. 084392 (N.J. argued Mar. 15, 2021) (arguing that disclosure of personal information in a government record presents a colorable privacy claim); Brief of Amici Curiae EPIC et al., *In re OPM Data Sec. Breach Litig.*, 928 F.3d 42 (D.C. Cir. 2019) (No. 17-5217) (arguing that the right to informational privacy safeguards the personal data held by federal agencies); Brief of Amici Curiae EPIC et al., *NASA v. Nelson*, 562 U.S. 134 (2011) (No. 09-530) (arguing that the right to informational privacy is well established); Brief of Amicus Curiae EPIC, *Doe v. Luzerne Cty.*, 660 F.3d 169 (3d Cir. 2011) (No. 10-3921) (arguing that plaintiff had a constitutional interest in preventing disclosure of a compromising image improperly obtained by a state actor).

EPIC has a strong interest in the protecting the confidentiality of census data. In 2004, the Census Bureau revised its "sensitive data" policy after an EPIC Freedom of Information lawsuit revealed that the Department of Homeland Security had improperly acquired data on Arab Americans from the Census Bureau following 9/11. Lynette Clemetson, *Census Policy on Providing Sensitive Data Is Revised*, N.Y. Times, (Aug. 31, 2004);[1] Lynette Clemetson, *Homeland Security Given Data on Arab-Americans*, N.Y. Times (July 30, 2004).[2] In 2018, EPIC

[1] https://www.nytimes.com/2004/08/31/us/census-policy-on-providing-sensitive-data-is-revised.html.
[2] https://www.nytimes.com/2004/07/30/us/homeland-security-given-data-on-arab-americans.html.

filed suit against the Department of Commerce to block the introduction of the citizenship question to the 2020 Census, alleging that the Bureau failed to complete several privacy impact assessments required under the E-Government Act of 2002. *EPIC v. Dep't of Commerce*, 928 F.3d 95 (D.C. Cir. 2019). EPIC also filed an amicus brief before the U.S. Supreme Court in *Department of Commerce v. New York* concerning the Bureau's unlawful failure to publish privacy impact assessments. Brief of Amici Curiae EPIC et al., *Dep't of Commerce v. New York*, 139 S. Ct. 2551 (2019) (No. 18- 966); *see also* Brief of Amicus Curiae EPIC, *New York, et al. v. Dep't of Commerce*, 351 F. Supp. 3d 502 (S.D.N.Y. 2019). Of particular relevance to this case, EPIC's Advisory Board includes leading experts in the field of differential privacy. EPIC, *EPIC Advisory Board* (2021).[3]

SUMMARY OF ARGUMENT

Unique among federal agencies, the U.S. Census Bureau is authorized by law to compel sensitive personal information from every person in the United States, 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. It is therefore vital, and required by law, that the Bureau protect the confidentiality of census responses across every data product it publishes. But in recent years, increasingly sophisticated reidentification methods have rendered traditional confidentiality protection measures obsolete. Accordingly, the Bureau has turned to a new disclosure avoidance system for the 2020 Census based on differential privacy—one which ensures both useful statistics and a mathematical guarantee of confidentiality. That

[3] https://epic.org/epic/advisory_board.html.

decision is the right one, and Plaintiffs' efforts to undo it should be rejected for at least three reasons.

First, the Census Bureau has an affirmative obligation to ensure that its publications do not permit the identification of individual census responses, even when those publications are combined with other datasets. Plaintiffs' attempt to draw the Bureau's confidentiality obligations narrowly fails. Second, differential privacy is the only reliable technique for defeating current and future reidentification attacks. The traditional disclosure avoidance methods favored by Plaintiffs are outdated and ineffective. Finally, differential privacy is essential to—not in conflict with—the accuracy of census data products. Protecting the confidentiality of census responses is vital to public participation in future surveys and does not endanger the usefulness of 2020 Census data. Accordingly, the Court should deny Plaintiffs' motion and petition.

ARGUMENT

I. The Census Bureau is legally obligated to ensure that its data products do not enable the identification of individual census responses.

If the Census Act makes one thing clear, it is that the Bureau must preserve the confidentiality of individual census responses as it fulfills its statistical mission. The Bureau is prohibited from making "any publication whereby the data furnished by any particular establishment or individual under this title can be identified" and may not use census responses "for any purpose other than the statistical purposes for which it is supplied[.]" 13 U.S.C. § 9 ("Information as confidential"). The Bureau may only "furnish copies of tabulations and other statistical materials which do not disclose the information reported by, or on behalf of, any particular respondent." 13 U.S.C. § 8(b). Congress enacted this restriction specifically to ensure "protection of privacy." S. Rep. No. 94–1256, at 3–4 (1976). The Act also commands that census responses may not be "used to the detriment of any respondent or other person to whom such

information relates." 13 U.S.C. § 8(c). And if the point were not already plain, any employee of the Bureau who "publishes or communicates any information, the disclosure of which is prohibited" by the Census Act "shall be fined not more than $5,000 or imprisoned not more than 5 years, or both." 13 U.S.C. § 214 ("Wrongful disclosure of information"); *see also Oath of Non-Disclosure*, U.S. Census Bureau (2021)[4] ("I will not disclose any information contained in the schedules, lists, or statements obtained for or prepared by the Census Bureau to any person or persons either during or after employment.").

These census privacy provisions serve three related purposes. First, they "guarantee the privacy of respondents." S. Rep. No. 94–1256, at 3–4. Second, they help secure the participation of respondents in Census Bureau surveys. As the Supreme Court has explained, "[A]n accurate census depends in large part on public cooperation. To stimulate that cooperation Congress has provided assurances that information furnished to the Secretary by individuals is to be treated as confidential." *Baldrige v. Shapiro*, 455 U.S. 345, 354 (1982). Finally, they ensure that census responses are only put to the legitimate statistical uses for which they are collected. *See id.* at 356.

Plaintiffs' narrow view of the Census Bureau's confidentiality obligations would undermine each of these purposes. In attacking the Bureau's adoption of differential privacy, Plaintiffs suggest that the Census Act only prohibits the publication of a data product that "*by itself* . . . lead[s] to the disclosure of confidential information[.]" Pls.' Mot., Dkt. No. 3, at 31 (emphasis in original). Under this theory, the Bureau's disclosure avoidance methods need not (indeed, cannot) account for the ways that a data product might be used by third parties, now or in the future, even if that data product could permit reidentification of individual responses when

[4] https://www.census.gov/about/policies/privacy/data_stewardship/oath_of_non-disclosure.html.

combined with other datasets. The Plaintiffs essentially contend that as, long as the Bureau uses a lock, it does not matter if someone already has (or might later obtain) the key.

This is a deeply flawed reading of the Census Act's confidentiality mandate. First, as a textual matter, the words "by itself" do not appear in 13 U.S.C. § 9. The provision broadly prohibits "*any* publication whereby the data furnished by *any* particular establishment or individual . . . can be identified." *Id.* (emphases added). It is well established that the disclosure avoidance methods favored by Plaintiffs can no longer prevent the data of individual census respondents from "be[ing] identified." *Id.*; *see also, e.g.*, JASON, *Formal Privacy Methods for the 2020 Census* 89 (Apr. 2020).[5] And that is exactly the result that § 9 aims, on its face, to avoid. If a given data product is one "whereby"—*i.e.*, "through which"—reidentification may be achieved, *Whereby*, Black's Law Dictionary (11th ed. 2019), section 9 prohibits the publication of that data product, even if a successful reidentification attack is only possible with the assistance of extrinsic data. The "assurances" Congress has given to the public "that information furnished to the Secretary by individuals is to be treated as confidential" would be meaningless if the Census Bureau were permitted (or even required) to publish data products that effectively guaranteed widespread breaches of confidentiality and facilitated nonstatistical uses of census responses. *Baldrige*, 455 U.S. at 355.

Moreover, courts have repeatedly confirmed the breadth and rigor of § 9's "strongly worded prohibition against disclosure[.]" *Seymour v. Barabba*, 559 F.2d 806, 807 (D.C. Cir. 1977). In *Baldrige v. Shapiro*, the Supreme Court rejected the argument that § 9 only protects the "*identities* of individuals who provide raw census data," explaining that the provision is not drawn

[5] https://www2.census.gov/programs-surveys/decennial/2020/program-management/planning-docs/privacy-methods-2020-census.pdf.

so narrowly: "The unambiguous language of the confidentiality provisions, as well as the legislative history of the Act . . . indicates that Congress plainly contemplated that raw data reported by or on behalf of individuals was to be held confidential[.]" *Baldrige*, 455 U.S. at 355 (emphasis added); *see also Franklin v. Massachusetts*, 505 U.S. 788, 818 n.18 (1992) (citing *Baldrige*, 455 U.S. at 356–58) ("The confidentiality of individual responses has long been assured by statute.").

The Court's ruling in *Baldrige* followed decades of federal court decisions emphasizing the Census Bureau's affirmative duty to *protect the privacy* of census respondents—not merely to avoid direct, unfiltered publication of census responses. *McNichols v. Klutznick*, 644 F.2d 844, 845 (10th Cir. 1981) ("[B]oth the history of the Census Act and the broad language of the confidentiality provisions of [§] 9 make abundantly clear that Congress intended both a rigid immunity from publication or discovery and a liberal construction of that immunity that would assure confidentiality."); *United States v. IBM Corp.*, No. 69 Civ. 200, 1975 WL 905, at *9 (S.D.N.Y. 1975) (explaining that § 9 "protects the privacy of members of the public who are required by law to submit information, often of a confidential nature, to the Department of Commerce"); *United States v. Bethlehem Steel Corp.*, 21 F.R.D. 568, 570 (S.D.N.Y. 1958) ("One need not probe far to understand that when Congress imposed upon citizens the duty of disclosing information of a confidential and intimate nature, its purpose was to protect those who complied with the command of the statute."); *see also FTC v. Orton*, 175 F. Supp. 77, 79 (S.D.N.Y. 1959) (explaining, in reference to § 9, that confidentiality is essential "where the Government needs information for the conduct of its functions, and the persons possessing the information need the encouragement of privacy in order to be induced freely to make full disclosure").

As the Census Bureau explained in a bulletin to 2020 Census respondents: "The law is clear—no personal information can be shared." *The 2020 Census and Confidentiality* 1, U.S. Census Bureau (Mar. 2019);[6] *see also* Br. for Dep't of Commerce et al. at 18, *EPIC v. Dep't of Commerce*, 928 F.3d 95 (D.C. Cir. 2019) (No. 19-5031) (arguing that "the threat to any privacy interest" from the then-planned addition of a census citizenship question was "wholly speculative because . . . the Census Act severely restricts the government's use and disclosure of census-derived information"). Plaintiffs' construction of the Census Act's confidentiality provisions would ensure the opposite, stripping the Bureau of its power to prevent the dissemination of personal information furnished by census respondents. The Court should reject this reading.

II. Differential privacy is the only technique known to effectively protect against reidentification attacks.

The Census Bureau's decision to adopt differential privacy for the 2020 Census was both necessary and correct. The threat that reidentification and reconstruction attacks pose to census confidentiality is real; the resulting harms are numerous and material; and differential privacy is the only credible technique to protect against such attacks, including those that may be developed in the future.

The susceptibility of census responses to reidentification and reconstruction is well established. The Census Bureau has shown that prior census data is alarmingly vulnerable to such attacks, revealing that the sex, age, race, and ethnicity of 142 million individuals could be inferred from publicly available 2010 Census data and that 52 million census respondents could be reidentified with the added use of commercial datasets. Michael Hawes, U.S. Census Bureau,

---

[6] https://2020census.gov/content/dam/2020census/materials/partners/2019-03/2020-confidentiality-factsheet.pdf.

Differential Privacy and the 2020 Decennial Census 13 (Mar. 5, 2020).[7] Other experts have highlighted and validated the privacy risks illustrated by the Bureau's experiments. *See* JASON, *supra*, at 89; Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 2 (Carnegie Mellon Univ., Data Privacy Working Paper No. 3, 2000) (explaining that the "practice of de-identifying data and of ad hoc generalization" previously used by the Bureau is "not sufficient to render data anonymous because combinations of attributes often combine uniquely to re-identify individuals").[8]

Reidentification and reconstruction are not distant or hypothetical problems; they are real and growing threats to the privacy of census respondents. Reidentification attacks have proven effective at identifying individuals through nominally deidentified datasets of AOL search queries, Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. Times (Aug. 9, 2006);[9] Netflix movie ratings, Arvind Narayanan & Vitaly Shmatikov, *Robust De-Anonymization of Large Sparse Datasets*, 2008 Proc. of IEEE Symp. on Security & Privacy 111; and medical records, Latanya Sweeney, *Only You, Your Doctor, and Many Others May Know*, Tech. Sci. (Sept. 29, 2015);[10] among other data sets. Reconstruction attacks based on census tables have been shown to pose a similar risk. *See* Irit Dinur & Kobbi Nissim, *Revealing Information While Preserving Privacy*, *in* 22 Proc. ACM SIGMOD-SIGACT-SIGAI Symp. on Principles of Database Sys. (June 2003) (demonstrating how collections of summary tables can be used to deduce information about individuals). And there is every reason to believe that the sophistication of reidentification and reidentification attacks will grow in the future. Absent

---

[7] https://www2.census.gov/about/policies/2020-03-05-differential-privacy.pdf.
[8] https://dataprivacylab.org/projects/identifiability/paper1.pdf.
[9] https://www.nytimes.com/2006/08/09/technology/09aol.html.
[10] https://techscience.org/a/2015092903.

privacy protections that are durable against such attacks, many 2020 Census respondents will fall victim. The potential harms are significant:

> Anyone could construct a linkage attack by purchasing commercial data[.] . . . Most people do not view the characteristics in the decennial census as particularly sensitive, but those who are most at risk to having their data abused (and are typically also the hardest to count) do. People who are living in housing units with more people than are permitted on the lease are nervous about listing everyone living there, unless they can be guaranteed confidentiality. Same-sex couples are nervous about marking their relationship status accurately if they feel as though they could face discrimination. Yet, the greatest risks people face often stem from how census data can be used to match more sensitive data (e.g., income, health records, etc.).

danah boyd, *Balancing Data Utility and Confidentiality in the 2020 US Census* 15–16 (Apr. 27, 2020);[11] Daniel L. Oberski & Frauke Kreuter, *Differential Privacy and Social Science: An Urgent Puzzle*, Harv. Data Sci. Rev. (Jan. 31, 2020)[12] ("[O]ne should assume that the probability of a linkage attack is 100% and the harm substantial."); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1705 (2010) ("[T]he power of reidentification will create and amplify privacy harms. . . . Accretive reidentification makes all of our secrets fundamentally easier to discover and reveal. Our enemies will find it easier to connect us to facts that they can use to blackmail, harass, defame, frame, or discriminate against us.").

Differential privacy is the best—indeed, the only known—method for preserving the privacy of census respondents against reidentification attacks. Protecting survey participants from harm is the organizing principle of differential privacy. "'Differential privacy' describes a promise, made by a data holder, or curator, to a data subject: 'You will not be affected, adversely

---

[11] https://datasociety.net/wp-content/uploads/2019/12/Differential-Privacy-04_27_20.pdf.
[12] https://hdsr.mitpress.mit.edu/pub/g9o4z8au/release/3.

or otherwise, by allowing your data to be used in any study or analysis, no matter what other studies, data sets, or information sources, are available.'" Cynthia Dwork & Aaron Roth, *The Algorithmic Foundations of Differential Privacy* 5 (2014).[13] By "introduc[ing] a controlled quantity of noise," differential privacy can preserve statistical calculations while also "provid[ing] robust and measurable guarantees of confidentiality." Jae June Lee & Cara Brumfield, *Differential Privacy in the 2020 Census* 1–2 (Nov. 2019).[14] Professor Cynthia Dwork, one of the pioneers of differential privacy, succinctly explained the features that make it the optimal approach to census disclosure avoidance:

> Differential privacy is a mathematically rigorous definition of privacy tailored to statistical analysis of large datasets. Differentially private systems simultaneously provide useful statistics to the well-intentioned data analyst and strong protection against arbitrarily powerful adversarial system users—without needing to distinguish between the two. Differentially private systems "don't care" what the adversary knows, now or in the future. Finally, differentially private systems can rigorously bound and control the cumulative privacy loss that accrues over many interactions with the confidential data.

Cynthia Dwork, *Differential Privacy and the U.S. Census*, *in* 38 Proc. ACM SIGMOD-SIGACT-SIGAI Symp. on Principles of Database Sys. (June 2019);[15] *see also* Dwork & Roth, *supra* at 1 ("At their best, differentially private database mechanisms can make confidential data widely available for accurate data analysis, without resorting to data clean rooms, data usage agreements, data protection plans, or restricted views."). These advantages have led to broad commercial deployment of differential privacy techniques, including by major companies like Apple and Google. Apple, *Differential Privacy* (2017);[16] Lily Hay Newman, *Google Wants to Help Tech*

---

[13] https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf.
[14] https://www.georgetownpoverty.org/wp-content/uploads/2019/11/GCPI-ESOI-Differential-Privacy-in-the-2020-Census-20191107.pdf.
[15] https://dl.acm.org/doi/abs/10.1145/3294052.3322188 (full keynote presentation available at https://www.youtube.com/watch?v=NNTBQ_K4h7c).
[16] https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf.

Companies Know Less About You, Wired (Sept. 5, 2019).[17] And contrary to Plaintiffs' suggestion that the Census Bureau's use of differential privacy is responsible for the delay in the release of redistricting data, Pls.' Mot. 31, the record reflects that differential privacy can be implemented in *less* time than traditional disclosure avoidance techniques. Abowd Decl. ¶ 72, Dkt. No. 41-1; Thieme Decl. ¶ 71, Dkt. No. 41-2.

For all of these reasons, the Census Bureau was right to institute differential privacy for the 2020 Census. If the Court reaches the merits of Plaintiffs' differential privacy claims, it should determine that the Bureau's adoption of differential privacy was both well-founded and consistent with the Census Act.

III. Differential privacy is essential to, not at odds with, the accuracy of Census Bureau data products.

Differential privacy is not the enemy of statistical accuracy in Census Bureau data products, as Plaintiffs suggest. Congress and the courts have long understood that protecting the confidentiality of census responses is vital to securing robust public participation in Census Bureau surveys, which is in turn is critical to ensuring their accuracy. "Congress's purpose in barring disclosure was to promote the success and accuracy of the census by assuring the public that responses would be kept confidential[.]" *In re England*, 375 F.3d 1169, 1179 (D.C. Cir. 2004) (citing *Baldrige*, 455 U.S. at 361); *see also Baldrige*, 455 U.S. at 355 (explaining that "assurances" of privacy are necessary to secure "public cooperation" in the census); *IBM Corp.,* No. 69 Civ. 200, 1975 WL 905, at *5 ("Maintenance of confidentiality facilitates the functioning of Government by encouraging the submission of full and free census data, data upon which the Government relies for a variety of purposes."); *Bethlehem Steel Corp.*, 21 F.R.D. at 570

[17] https://www.wired.com/story/google-differential-privacy-open-source/.

(explaining that one purpose of 13 U.S.C. § 9 "was to encourage citizens to submit freely all data desired in recognition of its importance in the enactment of laws and other purposes in the national interests").

This point was recently underscored by a coalition of organizations concerned with the sound administration of the 2020 Census. Noting that the Census "can only succeed if all households participate by completing accurately the census questionnaire," the coalition wrote:

> In 21st century America, households must be confident that information provided to the Census Bureau as part of the Census is confidential and will not be used for any purpose other than producing anonymous statistics. They must be assured that the Census Bureau will not share any data pertaining to a specific individual or household with any other government agency, court of law, or private entity for any purpose, or release any dat[a] that could undermine the confidentiality of personal information.

MALDEF et al., *The Census Confidentiality Protection Pledge* (Mar. 27, 2020).[18] The coalition explained that the "protection of census data confidentiality is essential to a successful Census and to a successful and healthy United States," pledging "to monitor for any breach of census data confidentiality" and "to use their collective power and influence to prevent, block, and/or bring an end to any breach of the currently-established guarantee and understanding of the confidentiality of data collected as part of the 2020 Census[.]" *Id.*

As established, the confidentiality of census responses cannot be reliably protected against reconstruction and reidentification attacks without the use of differential privacy. *See supra* Part II. An effective implementation of differential privacy is therefore critical not only to the privacy of 2020 Census respondents, but to the accuracy of future Census Bureau surveys as well.

Plaintiffs also rely on a second, related misconception about differential privacy: the notion that 2020 Census data will be "erroneous" or "faulty" in ways materially different from

---

[18] https://www.maldef.org/wp-content/uploads/2020/03/Final-Final-CensusPledge-03.27.20.pdf.

past censuses. Pls.' Mot. 3, 18. This overlooks a basic truth about the census: "No decennial census is, or can be, perfect[.]" Letter from JASON to Christa D. Jones, U.S. Census Bureau 3 (Feb. 8, 2021) (capitalization altered).[19] "Despite best efforts, the bureau has historically fallen short of counting each person once, only once, and in the right place." William P. O'Hare, Cara Brumfield, & Jae June Lee, Geo. Ctr. on Poverty & Inequality, *Evaluating the Accuracy of the Decennial Census* 3 (Nov. 2020). On top of routine omissions and erroneous enumerations (known as "coverage errors"), *id.*, the Census Bureau has long "introduce[d] errors into statistics in order to protect confidentiality." *Id.* at 35. Although the Bureau endeavors to minimize these errors, they are inevitable. *See, e.g.*, Thomas Mule, U.S. Census Bureau, *Census Coverage Measurement Estimation Report* (2012).[20] Census figures "may be as accurate as such immense undertakings can be, but they are inherently less than absolutely accurate[.]" *Gaffney v. Cummings*, 412 U.S. 735, 745 (1973).

Given this, Plaintiffs have failed to demonstrate that any errors in privacy-infused redistricting data will be meaningfully different than errors in past census data. Indeed, Plaintiffs could not possibly make this showing at present, as the Bureau has yet to finalize its disclosure-avoidance algorithms and privacy-loss budget. And it makes no sense to argue generically that differential privacy will introduce unacceptable error into redistricting data, as "Differential privacy is a *definition*, not an algorithm." Dwork & Roth, *supra* at 6 (emphasis in original). Plaintiffs' accuracy arguments are without merit.

---

[19] https://fas.org/irp/agency/dod/jason/census-data.pdf.
[20] https://www2.census.gov/programs-surveys/decennial/2010/technical-documentation/methodology/g-series/g01.pdf.

CONCLUSION

For the foregoing reasons, the Court should deny Plaintiffs' motion and petition.

Respectfully Submitted,

Dated: April 27, 2021

/s/ Adam W. Pittman
Adam W. Pittman (ASB-0146-A33P)
CORY WATSON, P.C.
2131 Magnolia Avenue, Suite 200
Birmingham, AL 35205
(205) 328-2200
(205) 324-7896, fax
apittman@corywatson.com

John L. Davisson (D.C. Bar #1531914)*
EPIC Senior Counsel
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)
davisson@epic.org

Attorneys for Amicus Curiae EPIC

* Admitted *pro hac vice*.

CERTIFICATE OF SERVICE

I hereby certify that on 27th day of April, 2021, I filed with the Court and served on all counsel through the CM/ECF system the foregoing document.

/s/ Adam W. Pittman
Adam W. Pittman (ASB-0146-A33P)
CORY WATSON, P.C.
2131 Magnolia Avenue, Suite 200
Birmingham, AL 35205
(205) 328-2200
(205) 324-7896, fax
apittman@corywatson.com