NO. 18-17356

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

THE CENTER FOR INVESTIGATIVE REPORTING,

PLAINTIFF-APPELLANT,

V.

UNITED STATES DEPARTMENT OF JUSTICE,

DEFENDANT-APPELLEE.

On Appeal from the U.S. District Court for Northern California
No. 3:17-cv-06557-JSC
The Honorable Jacqueline Scott Corley

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFF-APPELLANT

Aaron Mackey
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: amackey@eff.org
Telephone: (415) 436-9333

Counsel for Amicus Curiae
Electronic Frontier Foundation

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Legislative Materials

Other Authorities

STATEMENT OF INTEREST[1]

Amicus curiae Electronic Frontier Foundation (EFF) is a non-profit civil liberties organization with more than 36,000 members that works to protect rights in the digital world. EFF relies on Freedom of Information Act (FOIA) requests to learn about government practices that target the speech and privacy interests of people in the United States and abroad.

EFF has used FOIA to free digital government data and bring much-needed awareness to secretive government surveillance programs, most recently concerning the massive telephone surveillance partnership between law enforcement agencies and AT&T, known as "Hemisphere." *See EFF v. DOJ*, No. 15-cv-03186-TSH (N.D. Cal. Nov. 2, 2018).[2] EFF and ACLU of Southern California have also fought to obtain automated license plate reader data withheld under the California Public Records Act, which revealed the overwhelming amount of location data gathered through this surveillance in Los Angeles, how law enforcement can glean intimate profiles of people's activities from this data over time, and the frequency with which

[1] No party's counsel authored this brief in whole or in part. Neither any party nor any party's counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amicus*, its members, or its counsel contributed money that was intended to fund preparing or submitting this brief. All parties consent to the filing of this brief.

[2] *See Hemisphere: Law Enforcement's Secret Call Records Deal With AT&T*, EFF, https://www.eff.org/cases/hemisphere (last visited March 12, 2019).

agencies have shared this information. *See ACLU Found. of Southern California v. Superior Court*, 3 Cal. 5th 1032 (2017).

INTRODUCTION

Construing the release of statistical aggregate data as the creation of a new record is out of step with the realities of data storage, and it fails to comport with FOIA's mandate to broadly interpret statutory disclosure requirements to further the people's right of access. The district court's holding not only imperils the Center for Investigative Reporting's efforts to obtain aggregate data in this case, it also potentially frustrates the broader public's ability to use FOIA to obtain aggregate data that can uncover government abuses and permit better public oversight. This Court should thus reverse the district court's holding to ensure that FOIA stays relevant in the age of databases and digital records.

Releasing statistical aggregate data from government databases is a vital—and sometimes the only—way to comply with FOIA's mandate while properly balancing the public's and the government's interests in safeguarding sensitive information. Because the government continues to collect massive amounts of personally identifying information on the public, implicating both privacy and free speech rights, the public's right to access such non-exempt information through FOIA is essential to ensure government accountability and to expose impropriety. As explained below, there are countless examples of government data collection that

pose acute risks to individual privacy and free expression. For example, the Department of Homeland Security (DHS) is collecting comprehensive biometric and biographic profiles of travelers, as well as obtaining biometrics on sponsors of unaccompanied children for possible arrest and deportation. DHS and the Federal Emergency Management Agency (FEMA) are also monitoring people's social media activity on a large scale. Additionally, as the Executive Branch makes government data less publicly accessible, FOIA is often the only way for the public to access statistical aggregate data that the government previously proactively disclosed. Having access to aggregate data in these situations would help the public understand the scope of the government's actions without intruding on the privacy of individuals whose data is found in those systems or compromising law enforcement or other government interests.

Moreover, Congress has repeatedly affirmed that the public should have access to aggregate data precisely because of FOIA's salutary purpose: exposing government use and abuse of the data it collects. In the 1996 Electronic FOIA Amendments (E-FOIA Amendments), Congress explicitly updated FOIA to require the government to "use new technology to enhance public access to agency records and information."[3] And late in 2018, Congress required federal agencies to make

[3] Pub. L. No. 104-231, 110 Stat. 3048 (1996).

much of digital government data open, usable, and machine-readable by default. Open, Public, Electronic, and Necessary Government Data Act (OPEN Government Data Act).[4] Courts have consistently held that FOIA requires the extraction and reformatting of components of records in response to FOIA requests, and that such responses do not amount to the creation of new records or impose undue burden on the agency.

The district court's cramped interpretation of FOIA goes against these mandates. Its decision also has the potential to frustrate access to vast amounts of government digital data in which the public has a legitimate interest. This Court should reverse the district court's decision to correct these errors.

ARGUMENT

I. As the Government Creates Massive Databases, Releasing Statistical Aggregate Data Through FOIA Is Crucial to Ensure Transparency and Oversight While Balancing Other Interests.

As data and data-driven algorithms increasingly become an integral part of how government agencies function, robust public access to electronically stored data through FOIA, especially in the form of statistical aggregate data, is essential to

[4] Foundations for Evidence-Based Policymaking Act, Pub. L. No. 115-435, Title II, ___ Stat. ___ (2019) (Open, Public, Electronic, and Necessary Government Data Act).

ensure government accountability and oversight while balancing competing interests such as individual privacy and legitimate needs for government secrecy.

A. Disclosing Statistical Aggregate Data Provides an Important Check on Government Databases that Collect Sensitive Information.

The federal government is collecting and centralizing extensive swaths of personally identifying data on members of the public, including extremely sensitive information like biometrics and expressive activity on social media. Stated justifications for these databases range from national security to child welfare. The public has an undeniable interest in learning how these databases are actually being implemented and whether they are being misused or disproportionately targeting specific groups.

The public must have a viable way to obtain this non-exempt information through FOIA, and statistical aggregate data makes transparency and oversight possible without disclosing exempt information. For instance, statistical aggregate data can provide the public with meaningful information about a recently announced, expansive DHS biometric and biographic database called Homeland Advanced Recognition Technology (HART), without disclosing sensitive and personally identifying information.[5] This statistical data could reveal whether people belonging

[5] Jennifer Lynch, *HART: Homeland Security's Massive New Database Will Include Facial Recognition and Peoples' "Non-Obvious Relationships*," EFF Deeplinks

to particular demographic groups appear in the database more frequently than others, whether the data was shared with particular third parties, or whether it was shared for particular purposes. Having access to that type of aggregate data could be invaluable to expose racial, religious, or other profiling, as well as to learn whether the agency is sharing sensitive information with other federal or state agencies without authorization or oversight.

The HART database is of paramount public concern because it raises acute privacy and free speech concerns and likely contains inaccuracies that may have damaging legal effect for those who end up in the database. For one, biometric data is often collected in suspect circumstances, and often contains errors.[6] HART will also contain "records related to the analysis of relationship patterns among individuals," including "non-obvious relationships."[7] This will inevitably intrude upon the First Amendment right to privacy in expressive associations by potentially exposing individuals' political, social, or religious relationships. *See, e.g.*, *NAACP v. Alabama*, 357 U.S. 449 (1958). Additionally, HART's data will be disseminated to other federal government agencies, the intelligence community, state and local

---

Blog (June 7, 2018), https://www.eff.org/deeplinks/2018/06/hart-homeland-securitys-massive-new-database-will-include-face-recognition-dna-and.

[6] *Id*.

[7] *DHS Reveals Details of RFP for HART*, Planet Biometrics (Mar. 9, 2017), http://www.planetbiometrics.com/article-details/i/5614/desc/dhs-reveals-details-of-rfp-for-hart.

law enforcement, and foreign governments.[8] Relative to its predecessor, the Automated Biometric Identification (IDENT) system, HART's system will offer a "broader range of service" to these third parties.[9]

Similarly, statistical aggregate data would be essential to illuminate potential legal problems associated with a federal social media "extreme vetting" program that will harvest, preserve, and scrutinize immigrants' social media information for purposes of determining eligibility to enter the United States.[10] While this "extreme vetting" program ostensibly targets foreign visitors, it will inevitably sweep up the many Americans who use social media to communicate with these foreigners—and these Americans are disproportionately people of color. The captured information will be stored in an immigrant's A-file, which contains the complete immigration and travel records of all VISA applicants, asylum seekers, lawful permanent residents, and even naturalized citizens. The program thus raises the very real possibility of targeting individuals by their race and religion, as well as increasing the surveillance and data collection of vulnerable populations.

---

[8] *Id*.

[9] *Id.*

[10] Aleksander Danielyan, EFF Urges DHS to Abandon Social Media Surveillance and Automated "Extreme Vetting" of Immigrants, EFF Deeplinks Blog (Nov. 16, 2017), https://www.eff.org/deeplinks/2017/11/eff-urges-dhs-abandon-social-media-surveillance-and-automated-extreme-vetting.

Even though the government has abandoned for now its ill-conceived plans to use computer algorithms to mine this data and determine which visitors are most likely to be violent, public oversight is needed to prevent future expansion of the controversial program.[11] It is thus crucial that the public have the ability to access statistical aggregate data about this program that also maintains the privacy of individuals who are caught up in the program. Indeed, the Knight First Amendment Institute at Columbia University has filed a FOIA lawsuit seeking records about this program, including, "statistical data or reports regarding the application or waiver of the endorse or espouse provisions to exclude or remove individuals from the United States based on 'beliefs, statements or associations.'"[12]

Statistical aggregate data would also help the public understand how a new information-sharing database between DHS and the Department of Health and

[11] Drew Harwell and Nick Miroff, ICE Just Abandoned Its Dream of Extreme Vetting Software that Could Predict Whether a Foreign Visitor Would Become a Terrorist, Wash. Post (May 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/17/ice-just-abandoned-its-dream-of-extreme-vetting-software-that-could-predict-whether-a-foreign-visitor-would-become-a-terrorist/?utm_term=.40cb6aaa3361; see Manar Waheed, New Documents Underscore Problems of 'Social Media Vetting' of Immigrants, ACLU (Jan. 3, 2018), https://www.aclu.org/blog/privacy-technology/internet-privacy/new-documents-underscore-problems-social-media-vetting.

[12] First Amended Complaint at Ex. B, *Knight Institute v. DHS*, No. 1:17-cv-07572-ALC (S.D.N.Y. Mar. 12, 2018), available athttps://knightcolumbia.org/content/knight-institute-v-dhs-foia-suit-records-ideological-exclusion-and-social-media-monitoring.

Human Services (HHS) concerning the sponsors of unaccompanied immigrant children and the children themselves could be misused. The aggregate data would allow for greater scrutiny without invading individuals' privacy or compromising government investigations. The agencies' agreement, formalized in mid-2018, requires the collection of biometrics of sponsors of unaccompanied immigrant children, including their household members. Memorandum of Agreement Between ORR-HHS, ICE, and CBP, 4–5 (Apr. 13, 2018) (MOA).[13] The stated purpose is to determine sponsorship eligibility and ensure the welfare of the children, *see id.*, but the federal register notice allows ICE to use this information for enforcement and deportation purposes. DHS/ICE-007 Criminal History and Immigrant Verification (CHIVe) System of Records, 83 Fed. Reg. 20,844 (May 7, 2018). Thus, important statistical aggregate data on the DHS-HHS database would include the number of sponsor arrests or deportations that have resulted from this database, the number of arrests or deportations that are associated with particular countries of origin, and the number of children that only had one such sponsor.

Disclosing that statistical aggregate data could either assuage or increase many public interest groups' concerns that the government is using the information for enforcement purposes rather than the limited sponsorship eligibility and youth

[13] *Available at* https://www.texasmonthly.com/wp-content/uploads/2018/06/Read-the-Memo-of-Agreement.pdf.

protection purposes that justified collecting the information in the first instance.[14] Indeed, by deporting potential sponsors or even introducing the specter of deportation, advocacy groups have noted the database may actually undermine the children's welfare, as children will "remain in detention for longer rather than being placed with family members," another concern that statistical aggregate data might help to address.[15]

FOIA's right of access to aggregate data must extend to allow the public to audit less-controversial databases that collect sensitive information as well. The FEMA database that monitors social media does so to enable situational awareness during emergencies, but the public should be able to access statistical aggregate data through FOIA to assess the extent of the data collected, how often FEMA actually responds to flagged content, whether the data is in practice used for any other purposes, and how long the data is retained.[16] As described in other examples above, the aggregate data could disclose valuable information showing how FEMA uses its database while still protecting the rights of individuals who are swept in the program.

---

[14] See DHS-HSS Information Sharing and ICE Enforcement Against Potential Sponsors of Detained Children: A Resource Page, Brennan Center for Justice (Dec. 6, 2018), https://www.brennancenter.org/analysis/dhs-hhs-information-sharing-and-ice-enforcement-against-potential-sponsors-detained.

[15] *Id.*

[16] DHS/FEMA-013 Operational Use of Publicly Available Social Media Internet Sources for Situational Awareness, 81 Fed. Reg. 23,503 (Apr. 21, 2016).

B. Ensuring FOIA Provides Access to Aggregate Government Data Is Essential After the Executive Branch Stopped Proactively Disclosing Important Data.

FOIA must continue to permit robust access to aggregate government data because agencies do not always proactively disclose important data and in some cases have taken steps to remove data that was previously accessible. In 2016, federal agencies started taking down government data that was previously accessible to the public via their websites.[17] Some agencies removed data entirely, others later restored the data after facing public opposition, and other agencies made the data more difficult to find or to use.[18]

Although federal agencies have some discretion to proactively disclose data, when agencies determine that they will no longer provide public access via their websites, FOIA's statutory right of access to the same becomes all the more important. Because FOIA is the public's only recourse when federal government data is no longer publicly accessible, narrowing FOIA's reach to exclude statistical

---

[17] Juliet Eilperin, *Under Trump, Inconvenient Data Is Being Sidelined*, Washington Post (May 14, 2017), https://www.washingtonpost.com/politics/under-trump-inconvenient-data-is-being-sidelined/2017/05/14/3ae22c28-3106-11e7-8674-437ddb6e813e_story.html?utm_term=.69a5d3756281.

[18] Eric Lipton, *White House Backs Down on Keeping Ethics Waivers Secret*, N.Y. Times (May 26, 2017), https://www.nytimes.com/2017/05/26/us/politics/administration-lobbyists-ethics-waivers.html; Coral Davenport, *How Much Has 'Climate Change' Been Scrubbed from Federal Websites? A Lot.*, N.Y. Times (Jan. 10, 2018), https://www.nytimes.com/2018/01/10/climate/climate-change-trump.html.

aggregate data would severely undermine the public's right of access at precisely the moment when it is needed the most.

In one salient example, the U.S. Department of Agriculture (USDA) removed an animal welfare database from its website, leaving FOIA as the public's only mechanism to obtain the same statistical aggregate data it could compile without restriction before.[19] Indeed, the move "eliminated tens of thousands of reports detailing how many animals are kept by research labs, companies, zoos, and circuses, and whether those animals are being treated humanely under the Animal Welfare Act."[20]

The USDA slowly returned some of the information to its website in March 2018, but the agency's redactions made the data much less useful than what had previously been public.[21] Even Congress objected to the agency's backtracking, requiring the agency to restore the previously removed content as part of appropriations to USDA in 2018. H.R. Rep. No. 115-232 (2018), at 28.[22] A directive

[19] Amanda Carrozza, USDA Urged by Congress to Reinstate Access to Inspection Reports, American Veterinarian (Apr. 12, 2018), https://www.americanveterinarian.com/news/usda-urged-by-congress-to-reinstate-access-to-inspection-reports.

[20] *Id*.

[21] *Animal Welfare Enforcement Actions*, Dep't of Agriculture (last modified Aug. 10, 2018), https://www.aphis.usda.gov/aphis/ourfocus/animalwelfare/enforcementactions.

[22] *Available at* https://www.congress.gov/115/crpt/hrpt232/CRPT-115hrpt232.pdf.

from Congress stated that "USDA is now posting heavily redacted inspection reports that make it difficult in certain cases for the public to understand the subject of the inspection, assess USDA's subsequent actions, and to evaluate the effectiveness of its enforcement."[23] It further stated that "the online searchable database should allow analysis and comparison of data and include all inspection reports, annual reports, and other documents related to enforcement of animal welfare laws."[24] In short, Congress recognized the value that statistical aggregate USDA data provided to the public. But rather than make the data proactively available once more, the USDA website directs the public to seek that information through FOIA requests.[25] The agency's behavior demonstrates why FOIA must require the disclosure of aggregate data.

[23] Congressional Directive: Division A – Agriculture, Rural Development, Food and Drug Administration, and Related Agencies Appropriations Act (2018) at 4, https://docs.house.gov/billsthisweek/20180319/DIV%20A%20AG%20SOM%20FY18%20OMNI.OCR.pdf; *see Tracking U.S. Government Data Removed from the Internet During the Trump Administration*, Sunlight Foundation, https://sunlightfoundation.com/tracking-u-s-government-data-removed-from-the-internet-during-the-trump-administration/ (last visited March 20, 2019).

[24] *Id.*

[25] *Animal Welfare Enforcement Actions*, *supra* note 21.

II. This Court Should Reverse the District Court's Erroneous Decision that Releasing Statistical Aggregate Data Results in the Creation of New Records.

Although FOIA was enacted before electronic records were as prevalent as they are today, Congress has updated the law to ensure that it allows access to electronic records and data sets. This evolution mirrors the government's own digital revolution, which has redefined how it collects, compiles, and maintains information. Congress has thus given courts the tools to ensure FOIA provides robust public access to otherwise non-exempt government records that are of great interest to the public. One such tool Congress readily provided in FOIA: providing that agencies can release statistical aggregate data, which allows for the disclosure of information while protecting other interests, and that extracting this information neither constitutes the creation of a new record nor imposes an unreasonable burden on agencies.

The district court erred in holding that releasing statistical aggregate data requires the creation of new records and therefore violates FOIA. Its position ignores the requirements of the E-FOIA Amendments and the OPEN Government Data Act, as well as case law that has validated that extraction of data from government databases does not create a record under FOIA.

Congress enacted the E-FOIA Amendments to encourage government agencies to "use new technology to enhance public access to agency records and

information" and "maximize the usefulness of agency records and information collected, maintained, used, retained, and disseminated by the Federal Government." Pub. L. No. 104-231, § 2, 110 Stat at 3028. The key provision of the E-FOIA Amendments requires that "an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format." Pub. L. No. 104-231, § 5, 110 Stat. at 3050.

Congress' passage of the OPEN Government Data Act in 2018 provides further insight about how this Court should interpret the requirements of the E-FOIA Amendments as electronic government data has proliferated. Congress asserted that "[m]anaging Federal Government data to make it open, available, discoverable, and usable to the general public, businesses, journalists, academics, and advocates promotes efficiency and effectiveness in government . . . and more importantly, strengthens our democracy." OPEN Government Data Act at § 2(a)(1). The law requires the federal government to make data "open by default" and "machine-readable." *Id*. at §§ 202(b)-(c). The OPEN Government Data Act's provisions complement the E-FOIA Amendments' requirements that agencies provide robust access to government data, including aggregate statistical data that would shed light on government operations.

Since passage of the E-FOIA Amendments, courts have consistently held that using computer programs to select components of data from a larger whole and to

modify the records' format does not amount to creating a new record under FOIA. For example, in *Schladetsch v. Department of Housing and Urban Development*, the agency "conceded that it possesse[d] in its databases all the discrete pieces of information that [plaintiff] ha[d] requested, but it claim[ed] that it [did] not possess the information in the isolated compilation" that plaintiff sought. 2000 WL 33372125, at *2 (D.D.C. Apr. 4, 2000) (citations omitted). The court expressly held that compliance with plaintiff's request would not result in "creation" of a new record: "The fact that the agency may have to search numerous records to comply with the request and that the net result of complying with the request will be a document the agency did not previously possess is not unusual in FOIA cases, nor does this preclude the applicability of the Act." *Id*. at *3. It went on to hold that "[b]ecause an electronic search of computer databases does not amount to a creation of records, it follows that the programming necessary to instruct the computer to conduct the search does not involve the creation of a record." *Id.* (citations omitted). The court concluded that "[b]ecause HUD has conceded that it possesses in its databases the discrete pieces of information which [plaintiff] seeks, extracting and compiling that data does not amount to the creation of a new record." *Id.*

In *National Security Counselors v. CIA*, the court reiterated that "sorting a pre-existing database of information to make information intelligible does not involve the creation of a new record because, as Congress noted in the legislative

history to the E-FOIA Amendments, '[c]omputer records found in a database rather than a file cabinet may require the application of codes or some form of programming to retrieve the information.'" 898 F. Supp. 2d 233, 270 (D.D.C. 2012) (quoting H.R. Rep. No. 104-795, at 22 (1996)). Thus, a request that seeks "entire fields of data from particular electronic databases" is proper under FOIA, as long as the requester seeks "the contents of the database"—as opposed to an analysis of the data, or other information that does not otherwise exist. *Id.* at 271. *See also Schladetsch*, 2000 WL 33372125, at *3 ("The programming necessary to conduct the search is a search tool and not the creation of a new record.").

The above cases demonstrate that searching for and extracting particular information maintained in an agency's database does not constitute the "creation" of a new record. Indeed, "[t]he fact that the agency may have to search numerous records to comply with the request and that the net result of complying with the request will be a document the agency did not previously possess is not unusual in FOIA cases" and is not a legitimate reason for an agency to resist disclosure. *Id.* (quoting *Disabled Officer's Association v. Rumsfeld*, 428 F. Supp. 454, 456 (D.D.C. 1977), *aff'd*, 574 F.2d 635 (D.C. Cir. 1978)). To the extent that the disputed items can be provided to plaintiffs through a query to the agency's database, the agency is legally obligated to conduct such searches.

Even prior to the E-FOIA Amendments, courts have interpreted FOIA to require agencies to manipulate existing records and databases to extract information sought by a public records requestor, and that doing so does not create a new record. In *May v. Department of Air Force*, a federal appellate court addressed records maintained as handwritten forms that, if released, could reveal the identity of the author based on the distinctive style of the handwriting. 800 F.2d 1402 (5th Cir. 1986). The court held the Air Force could create a typewritten copy of the records or recreate them in a third-party's hand to protect the identity of the author. *Id*. at 1403. It furthermore concluded that "such disclosure would . . . ensure maximum disclosure under the [FOIA], and not unreasonably burden the agency." *Id*. The principle articulated in *May* applies to aggregate data: to the extent that an agency must protect the privacy of individuals identified in its data, it can take steps to modify the data or release portions that are not identifiable without creating a new record. *See also Yeager v. DEA*, 678 F.2d 315, 321 (D.C. Cir. 1982) ("Although accessing information from computers may involve a somewhat different process than locating and retrieving manually-stored records, these differences may not be used to circumvent the full disclosure policies of the FOIA.").

CONCLUSION

For the foregoing reasons, *amicus curiae* respectfully requests that this Court reverse the district court's decision and require the agency to provide statistical aggregate data to the Center for Investigative Reporting.

Dated: March 28, 2019

Respectfully Submitted,

/s/ Aaron Mackey
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: amackey@eff.org
Telephone: (415) 436-9333

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)(7)(C)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amici Curiae Electronic Frontier Foundation In Support of Plaintiffs-Appellants complies with the type-volume limitation, because this brief contains 3,875 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: March 28, 2019

/s/ Aaron Mackey
Aaron Mackey

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on March 28, 2019.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: March 28, 2019

/s/ Aaron Mackey
Aaron Mackey

Counsel for Amicus Curiae
Electronic Frontier Foundation