[ORAL ARGUMENT NOT YET SCHEDULED]

Appeal No. 18-5276

UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA

JASON LEOPOLD AND
REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS,

Appellants,

v.

UNITED STATES OF AMERICA

Appellee.

Appeal from the United States District Court for the District of Columbia,
Hon. Beryl A. Howell, Case No. 1:13-mc-00712-BAH

AMICUS BRIEF OF ELECTRONIC FRONTIER FOUNDATION AND RIANA PFEFFERKORN IN SUPPORT OF PETITIONERS-APPELLANTS

Aaron Mackey, Bar No. 55223
Camille Fischer
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
amackey@eff.org

Attorneys for Amici Curiae

January 25, 2019

CERTIFICATE AS TO PARTIES, RULINGS, RELATED CASES, AND STATUTES

Pursuant to D.C. Circuit Rules 26.1 and 28(a)(1), and Fed. R. App. P. 26.1, the undersigned counsel certifies as follows:

A. Parties and *Amici*

All parties, intervenors, and *amici* appearing in the proceedings below and in this Court are listed in the Brief of Appellants.

B. Rulings Under Review

References to the rulings at issue appear in the Brief of Appellants.

C. Related Cases

This case has not previously been before this Court or any other court. Counsel are not aware of any related cases currently pending in this Court or any other court within the meaning of Circuit Rule 28(a)(1)(c).

D. Statutes and Regulations

All applicable statutes, etc., are contained in the Brief Appellants.

January 25, 2019 /s/ *Aaron Mackey*

CORPORATE DISCLOSURE STATEMENT

Pursuant to D.C. Circuit Rule 26.1 and Federal Rule of Appellate Procedure 26.1, *amicus* submits the following corporate disclosure statement:

Amicus Electronic Frontier Foundation ("EFF") is a donor-funded, non-profit civil liberties organization. EFF has no parent corporation, and does not issue stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

* Authorities upon which we chiefly rely are marked with asterisks.

Statutes

Legislative Materials

Other Authorities

INTEREST OF *AMICI*[1]

Amicus curiae Electronic Frontier Foundation (EFF) is a non-profit civil liberties organization with more than 39,000 members that works to protect rights in the digital world. Based in San Francisco and founded in 1990, EFF regularly advocates in courts and broader policy debates on behalf of users and creators of technology in support of free expression, privacy, and innovation. As part of its work, EFF advocates for restrictions on law enforcement's ability to obtain sensitive and private information about Internet users. Brief for Electronic Frontier Foundation *et. al.* as *Amici Curiae* supporting Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402). EFF also pushes private companies that collect and maintain user data to zealously guard their users' data, including by disclosing it only when required by law and giving users notice and an opportunity to challenge disclosure. *Who Has Your Back?*, EFF (2017).[2]

EFF has also represented *The Stranger*, a Pulitzer Prize-winning alternative newsweekly, which petitioned the U.S. District Court for the Western District of Washington in 2017 to unseal judicial records documenting law enforcement

[1] No party's counsel authored this brief in whole or in part. No party or party's counsel, nor any person besides *amici*, members of *amicus* Electronic Frontier Foundation, or *amici*'s counsel contributed money toward this brief. Counsel for all parties have consented to the filing of this brief.

[2] https://www.eff.org/who-has-your-back-2017.

requests for information similar to the materials sought by Petitioners-Appellants in this case. *In re Index Newspapers, LLC*, No. 17-mc-00145 (W.D. Wash. 2017). As a result of this petition, the court and U.S. district attorney's office have agreed to begin docketing applications and orders sought under the Stored Communications Act, 18 U.S.C. § 2703(d), and Pen Register Act, 18 U.S.C. § 3122-23, and in 2020 will start issuing reports every six months tracking those cases.

Amica Riana Pfefferkorn is the Associate Director of Surveillance and Cybersecurity at the Center for Internet and Society ("CIS"), a public interest technology law and policy program at Stanford Law School. She appears in her personal capacity only and does not represent CIS, Stanford Law School, or Stanford University. Much of Pfefferkorn's role at CIS involves researching government surveillance and encryption law and policy. As a key part of her work at CIS, Pfefferkorn researches and analyzes judicially-authorized government surveillance activities. She investigates and analyzes the policies and practices of the U.S. and foreign governments for forcing decryption and/or influencing cryptography or security-related design of online platforms and services, devices, and products through the courts and legislatures.

Pfefferkorn is a *pro se* petitioner in a matter similar to the instant case that is currently pending in the Northern District of California, *In re Petition of Jennifer Granick and Riana Pfefferkorn*, No. 16-mc-80206 (N.D. Cal. petition filed Sept. 28,

2016). That case, like this one, seeks to unseal certain sealed court records in the court's surveillance docket as well as prospective changes to the court's docketing and unsealing practices for surveillance matters.

INTRODUCTION AND SUMMARY OF ARGUMENT

Our personal interactions, daily activities, and business efforts are conducted and recorded electronically, generating an enormous volume of digital data. Usually that electronic information is transmitted and held by third-party entities that we rely on to provide us with email communications, calling, messaging and text, cloud storage, and many other services. This data is a valuable resource for law enforcement to gather evidence in criminal investigations, and they frequently obtain it using the legal authorities at issue in this case: search and seizure warrants under the Stored Communications Act ("SCA"), Title II of the Electronic Communications Protection Act ("ECPA"), 18 U.S.C. §§ 2701–2712; court orders under Section 2703(d) of the SCA; and court orders authorizing the use of a pen register and/or trap-and-trace ("PR/TT") device under the Pen Register Act ("PRA"), Title III of the ECPA, 18 U.S.C. §§ 3121–3127.

In district courts around the country, these warrants and court orders, along with related court filings (applications, supporting affidavits, etc.) and even the case docket sheets themselves, largely remain under seal indefinitely. Although sealing these court records initially may be justified to protect the secrecy of an active

investigation, the records typically stay sealed well after the underlying investigation is over, long past any need for continued secrecy.

This *de facto* indefinite sealing violates the public's First Amendment and common law rights to access court records, as Petitioners-Appellants ably demonstrate. *Amici* write separately to highlight two important salutary effects that will result from public access to the court records at issue in this case.

First, disclosure of the records Petitioners-Appellants seek will inform the public how law enforcement uses its statutory authorities to obtain personal data. As recent cases show, law enforcement frequently develops novel legal theories to access the data created by the digital devices and services everyone relies on daily. Often, these developments occur in secret and do not require law enforcement to obtain a warrant for people's data. The current, endemic secrecy surrounding this law enforcement activity is thus incompatible with the public's rights of access and its ability to advocate for policy changes or new laws that protect individual privacy. Disclosure would provide the public with the information we need to have an informed debate about the limits society should place on law enforcement's ability to comb through our digital data, as that data often reflects the most intimate details of our lives.

Second, public disclosure of the records sought will allow the public to learn more about when and how frequently the services we rely on provide our personal

data to law enforcement, and under what circumstances. In recent years the public has become increasingly focused on understanding how well communications and other service providers protect our data. Users deserve to know whether their providers will push back against overreaching government demands for their data. Knowing how providers respond to law enforcement requests impacts consumer decisions. With the right information, users can exercise their consumer power to push an overly cooperative provider to stand up for its users, encourage a provider to "walk the talk" by living up to its public statements about protecting users, reward a truly user-protective provider with more business, or switch their allegiance to the provider that most zealously defends user privacy.

Accordingly, this Court should reverse the district court's decision.

I. DISCLOSURE OF THE JUDICIAL RECORDS PETITIONERS-APPELLANTS SEEK WOULD ALLOW THE PUBLIC TO LEARN HOW THE GOVERNMENT OBTAINS INFORMATION FROM COMMUNICATION PROVIDERS THAT REVEAL INTENSELY PRIVATE DETAILS OF OUR LIVES.

At a time when nearly everyone relies on private service providers for nearly everything—from talking to friends, to organizing events, storing photographs, shopping, and running businesses—it is essential that the public know when and how the government accesses our personal information held by those providers. Before the development of electronic communication and digital services, the majority of our communications and other interactions left few to no records. And

even when those communications or interactions did leave records, the volume paled in comparison to the vast digital ocean of data created today. As the Supreme Court observed in *Riley v. California*, "a photograph or two of loved ones tucked into a wallet" says something about a person, but they reveal nothing close to "[t]he sum of an individual's private life [that] can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions" that are recorded and stored digitally. 134 S. Ct. 2473, 2489 (2014).

Our digital communications generate so much data about whom we speak with, when, for how long, and from where, that law enforcement is operating in a golden age of surveillance. Peter Swire, *The Golden Age of Surveillance*, Slate (July 15, 2015).[3] And law enforcement can obtain much of this data, which reveals the "privacies of life," without a warrant. *See Riley*, 134 S. Ct. at 2494 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

Law enforcement's reliance on the Stored Communications Act and Pen Register Act to obtain much of this information is problematic precisely because the data that law enforcement can collect without a warrant today is "qualitatively different" in volume, detail, and comprehensiveness than the more limited kinds of information Congress envisioned would be collected when the ECPA became law

[3] https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html.

in 1986. *See Carpenter v. United States*, 138 S. Ct. 2206, 2216–17 (2018). Law enforcement's use of these statutory authorities thus implicates not just the privacy interests of those targeted, but the broader public interest in knowing how the government is using investigatory powers created during a different era of electronic communications to capture personal data generated by new digital technologies.

And as discussed further below, because these matters remain sealed by default, often indefinitely, public disclosure of the materials sought by Petitioners-Appellants is all the more necessary for the public to gain a full understanding of the government's activities.

A. The Public Has a Right to Learn How Law Enforcement Is Adapting Its Surveillance Authority to Obtain Information About People that New Digital Technologies Create and Collect.

As new technologies become ever more embedded into people's everyday lives, providing users with innovative ways to communicate and making their lives easier, they generate massive amounts of data. Law enforcement understands this and often seeks that data under the Stored Communications Act or Pen Register Act. By default, that law enforcement activity is secret, as are the court records that give them the authority to collect the data. As this case proves, that secrecy persists long after law enforcement begins criminal proceedings against people or closes its investigations.

To counter that secrecy, the public's rights of access under the First Amendment and common law provide the best avenue for users to understand the evolution of how the government is using its powers to obtain personal information. *See* Brief of Petitioners-Appellants at 36–40. This public access should at minimum allow for disclosure of basic docketing information and historic materials in which any law enforcement or privacy concerns can be addressed via redactions, rather than wholesale sealing.

While the contents of communications have long been protected by the Fourth Amendment's warrant requirement, *see, e.g.*, *Ex parte Jackson*, 96 U.S. 727, 733 (1877), courts have traditionally subjected non-content information to less protection. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 744–46 (1979). But that distinction is becoming increasingly fraught as technologies blur the line between content and non-content information. *See generally* Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1 (2016) (arguing against outdated content/non-content distinction in light of the complex architecture of the Internet). Moreover, the Supreme Court has recognized that even non-content data can disclose incredibly personal details. *Carpenter*, 138 S. Ct. at 2220 (holding that historic records about an individual's location "implicate[] privacy concerns far

beyond those considered" in earlier cases involving data collected by more primitive technologies).

Public access is thus important to allow for greater oversight of law enforcement. This is particularly true of the government's use of court orders under Section 2703(d) of the Stored Communications Act (SCA), 18 U.S.C. § 2703(d) ("D Orders"), which authorize the government to obtain records of users' wire or electronic communications as well as the contents of older wire or electronic communications held in storage. *See* 18 U.S.C. § 2703(a)–(c). Notably, to apply for D Orders, the government need not demonstrate probable cause as it would to obtain a warrant. Instead, it must only "offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id*. at § 2703(d). The standard for the application of a PR/TT order is even less robust, requiring the government to certify that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1).

The Supreme Court has recently curbed the use of D Orders to obtain detailed location records, finding that historic cell-site location information is protected by the warrant requirement because it is "detailed, encyclopedic, and effortlessly

compiled." *Carpenter*, 138 S. Ct. at 2216.[4] Similarly, the Sixth Circuit held in 2010 that D Orders cannot be used to obtain the contents of stored email communications, a holding that service providers across the country rely on to require law enforcement to obtain search warrants before they will disclose the contents of users' messages. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010).[5]

Law enforcement agencies have similarly used the Pen Register Act to seek access to data that is different than the traditional dialing and routing information the statute envisions, such as trying to obtain information about changes to a particular mobile device's subscriber information, including advance notice of termination of the account or a change in number. *In re Application of the United States of America for an Order Authorizing the Installation and Use of Pen Registers and Trap and Trace Devices*, 2018 WL 6442661, at *1 (S.D. Fla. Nov. 30, 2018).

---

[4] Even after *Carpenter*, law enforcement is still trying to access this information in novel ways and at least one district court after *Carpenter* has upheld "hybrid" PR/TT and SCA § 2703(d) orders for cell-site location information, saying that the hybrid orders are the "functional equivalent" of a search warrant. *United States v. Evans*, 2018 WL 7051095, at *3–4 (E.D.N.C. Dec. 20, 2018).

[5] Despite the fact that DOJ has adopted a policy requiring federal law enforcement to obtain a warrant when seeking the contents of email messages and other stored digital communications, *see* H.R. Rep. No. 114-528, at 9 (2016), the Stored Communications Act still allows for the collection of some older email messages with a D Order, a privacy loophole that Congress has tried, and so far failed, to close. *See* David Ruiz, *Email Privacy Act Comes Back, Hopefully to Stay*, EFF Deeplinks Blog (May 29, 2018), https://www.eff.org/deeplinks/2018/05/email-privacy-act-comes-back-hopefully-stay.

Similarly, in another case involving the Lavabit encrypted email service, investigators attempted to force disclosure of encryption keys pursuant to an SCA seizure warrant.[6] *See In re Under Seal*, 749 F.3d 276, 282–83, 285 (4th Cir. 2014). However, it is not clear that the SCA authorizes the seizure of encryption keys, and the Fourth Circuit declined to reach that issue. *See id.* at 293 (holding issue waived because not challenged below).

The examples above show that law enforcement regularly seeks novel or uncommon court authorizations to enable new or unusual investigatory techniques that may later be found to be unlawful. Yet there is often a long delay between the initial government attempt to access private data in new ways and the public disclosure and appellate scrutiny (if any) of law enforcement's activities. *See Carpenter*, 138 S. Ct. at 2212 (ruling in 2018 that law enforcement's use of a D

[6] Although outside the scope of this brief, *amici* support a finding that the lower court erred in its conclusion that warrants under the Stored Communications Act "are functionally unlike traditional search warrants and more akin to subpoenas." *In re Application of Jason Leopold to Unseal Certain Electronic Surveillance Applications and Orders*, 300 F. Supp. 3d 61, 88 (D.D.C. 2018); *see* Brief of Petitioners-Appellants at 26–29. This issue was before the Supreme Court last year in *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018), but the case was mooted by federal legislation. *See* Clarifying Lawful Overseas Use of Data ("CLOUD") Act, Pub. L. 115-141, Div. V, § 103, 132 Stat. 348 (2018). However, the Second Circuit's now-vacated decision analyzes the congressional record of the Stored Communications Act and determines that an SCA warrant is a warrant. *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197, 212-13 (2d Cir. 2016), *aff'ed* en banc, 855 F.3d 53 (2017), *vacated as moot*, 138 S. Ct. 1186 (2018).

Order in 2011 to collect historic cell-site location information was unconstitutional). Thanks to that delay, there may be numerous cases in which law enforcement successfully requests or accesses private data with less than a warrant, resulting in serious privacy invasions of an untold number of individuals.

Further, because D Orders and PR/TT orders do not meet the Fourth Amendment's standard for the issuance of warrants, it is a matter of public concern when the government uses them to obtain a range of sensitive and revealing information. Access to dockets and orders creates opportunities for public oversight and potentially even policy intervention. As retired magistrate judge Stephen Smith has noted, "the exercise of judicial power is an inherently *public* act." Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177, 21 (2009). *See also* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 331 (2012) ("Greater transparency" of the federal courts' secret surveillance dockets "would enable meaningful oversight not only by appellate courts but also by Congress and the general public.").

Disclosure of these materials reasonably soon after the needs for secrecy are no longer justified would in turn allow the public and lawmakers to determine whether the government's legal theories are correct and whether new laws or policies should be created to limit access to the data or to at least require a search warrant.

Unsealing these closed matters would thus ensure that the public's understanding of the government's activities remains up to date, allowing everyone to intelligently debate them.

B. Public Disclosure of These Judicial Materials Is Critical Because Endemic Secrecy Surrounding Law Enforcement's Use of Its Surveillance Authority Has Stifled Public Debate.

The current practice of wholesale, indefinite sealing of the judicial materials sought by Petitioners-Appellants also frustrates the public's ability to fully understand how law enforcement uses legal provisions to prevent service providers from disclosing the fact that they have received demands for their users' data. Unsealing would thus help the public understand whether the government is misusing those legal provisions, which often implicate due process and free speech rights of the service providers and their users.

The Stored Communications Act permits law enforcement to prohibit service providers who receive SCA orders from providing notice to the users targeted by the request. 18 U.S.C. § 2705(b). The provision allows the government to effectively gag providers indefinitely, as until recently the government would seek extensions of delayed-notice orders for extended periods of time.

Courts have expressed concern about the government's use of Section 2705(b) orders, including finding that their indefinite duration implicates providers' First

Amendment rights. *Microsoft v. DOJ*, 233 F. Supp. 3d 887 (W.D. Wash. 2017).[7] After the court allowed Microsoft's suit to proceed, the DOJ publicly stated that it would change its policy seeking indefinite orders under Section 2705(b), and Microsoft dropped the case. *See* Deputy Attorney General Rod Rosenstein, *Memorandum for Heads of Department Law Enforcement Components* (Oct. 19, 2017).[8] Instead of gag orders for an indefinite duration, DOJ's new policy stated that "[b]arring exceptional circumstances," prosecutors "may only seek to delay notice for one year or less." *Id.* at 2.

The public attention that Microsoft drew to the DOJ's practice was instrumental in prompting the DOJ's policy change. But, just one week after the DOJ's policy change in October 2017, it came to light that federal prosecutors were requesting the new one-year delayed-notice maximum by default, without providing any justification commensurate with such a long delay. *In re Grand Jury Subpoena to Google Inc.*, 2017 WL 4862780, at *1 (E.D.N.Y. Oct. 26, 2017) ("[T]he government's request for a one-year non-disclosure period appears to reflect a new policy of the Department of Justice, but in a way that conforms to its letter rather than its rationale"). This practice only came to light because the magistrate judge

[7] EFF filed an *amicus* brief in the case advocating for user notice. Brief of the Electronic Frontier Foundation as *Amici Curiae* in Support of Plaintiff, *Microsoft Corp. v. DOJ*, 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. 16-cv-00538).

[8] https://www.justice.gov/criminal-ccips/page/file/1005791/download.

who received the government's application decided to publicly issue his order denying it. *Id*. Public disclosure of surveillance applications (including gag requests) and courts' orders on those applications is thus necessary for the public to understand the government's interpretation of both statutory surveillance authorities and its own policies for using those authorities, as well as to understand whether judges are independently scrutinizing every request.

Further, knowing how service providers respond to information requests, and specifically which providers are willing to challenge government requests, helps consumers determine which service providers to use to communicate and store sensitive information. Unsealing would thus allow the public to learn how frequently the government requests delayed notification under Section 2705(b); for how many days, and on what basis; whether courts grant or reject the request; how often authorized delays are extended, and for how long; whether service providers push back against orders not to notify their users; and whether users are eventually notified.

II. PUBLIC DISCLOSURE OF THE JUDICIAL RECORDS SOUGHT BY PETITIONERS-APPELLANTS WOULD ENABLE THE PUBLIC TO BETTER UNDERSTAND HOW WELL PRIVATE COMPANIES PROTECT OUR DATA.

Users of electronic communication services benefit and can make more informed choices about which digital tools and services they use when they are given meaningful disclosures about how the government requests user information and

how service providers collect, use, and share user information. Public access to the records sought by Petitioners-Appellants would provide a more comprehensive picture that would enable consumers to make more informed choices. It would also provide more accountability by allowing the public to compare service providers' responses to law enforcement with their stated policies regarding how they protect user data.

A. Disclosure of the Judicial Records Sought Here Would Help Fill Gaps in Current Transparency Efforts, Which Are Piecemeal and Make it Difficult for the Public to Make Meaningful Choices About Technology Use.

Public access to information about law enforcement requests to service providers and service providers' responses to those requests matters because it enables users to make informed decisions about the best communication service for their needs. Consumers may change their communication habits based on their perception of providers' willingness to provide law enforcement warrantless access to users' information. After newspapers broke the story of domestic mass-surveillance programs in 2013, in which service providers were accused of some level of participation, 34% of U.S. consumers who had heard about the programs took at least one proactive step to hide their information from the government—often by changing privacy settings or enabling security tools. Abigail Geiger, *How*

Americans have viewed government surveillance and privacy since Snowden leaks, Pew Research Ctr. (June 4, 2018).[9]

Right now, the majority of the information the public knows about government requests for users' online information comes from companies themselves, normally in the form of transparency reports that reveal select pieces of information that companies choose to disclose, usually in the aggregate. This type of reporting first emerged in 2010 when Google published a global report on government requests for user data and for content takedowns, largely in response to growing online censorship practices by the People's Republic of China.[10] Now, several of the large Internet companies issue at least yearly transparency reports.[11]

---

[9] http://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/.

[10] Google's Transparency Report website includes a timeline of Google's transparency practices, including changing policy rationales as well as changing data points that the company has elected to report. For instance, the 2010 report details Google's traffic data to create a map of where content is removed and sites are blocked by governments, whereas in August 2018 Google elected to share information about political ad purchases and revenue. Google, Transparency Report, Requests for User Information, https://transparencyreport.google.com/user-data/overview?hl=en (last visited Jan. 25, 2018).

[11] *See, e.g.*, Facebook, Transparency, United States, https://transparency.facebook.com/government-data-requests/country/US/jan-jun-2018 (last visited Jan. 25, 2018); Microsoft, Law Enforcement Requests Report, https://www.microsoft.com/en-us/corporate-responsibility/lerr/ (last visited Jan. 25, 2018); AT&T, Transparency Report, https://about.att.com/csr/home/frequently-requested-info/governance/transparencyreport.html (last visited Jan. 25, 2018); Twitter, Transparency Report, United States of America, https://transparency.twitter.com/en/countries/us.html (last visited Jan. 25, 2018).

The information provided in these company transparency reports can be useful to identify larger trends in government requests for user information, but are often not granular or comprehensive enough for the public to understand what types of data are collected, what legal mechanisms and justification the government uses for these requests, and how many people the requested information concerns. For instance, Google's latest transparency report focuses on legal process. It breaks down how many subpoenas, search warrants, court orders, emergency disclosure requests, pen register orders, wiretap orders, and preservation requests the company received between January and June 2018.[12] In contrast, Apple's latest transparency report focuses on the data collected. It quantifies government requests by type of user information sought: devices, financial identifiers, and accounts.[13] These two reports tell very different stories, but each set of data is incomplete without the other, so each report paints only a partial picture of the user data requests received by the respective company.

[12] Google, Transparency Report, United States Jan2018–Jun2018, https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts,compliance;authority:US;time:Y2018H1&lu=user_requests_report_period&legal_process_breakdown=expanded:0 (last visited Jan. 25, 2018).

[13] Apple, Transparency Report, United States of America Jan2018–Jun2018, https://www.apple.com/legal/transparency/us.html (last visited Jan. 25, 2018).

Public interest organizations have been calling for standardized corporate reporting of law enforcement requests in order for consumers and researchers to directly compare corporate practices. Harvard University's Berkman Center for Internet and Society and New America's Open Technology Institute published best practices for corporate transparency reports on government requests for user data to end the fragmentation of practices that have made it impossible to meaningfully compare metrics across companies. THE TRANSPARENCY REPORTING TOOLKIT (March 2016).[14] The best practices discuss both the information and level of detail that consumers need for meaningful transparency. *Id.* They recommend that companies report government data requests in granular detail while also explaining their policies for complying with those requests. *Id.* at 18, 26.[15]

---

[14] https://static.newamerica.org/attachments/12935-the-transparency-reporting-toolkit/Transparency_Memo_Web.d0ecdb0e8c1a4dae9993e12ae61e5ef1.pdf.

[15] The recommendations include: 1) reporting the numbers of government requests for information by category of legal process (*i.e.*, number of subpoena, 18 U.S.C. § 2703(d) orders, search warrants, and wiretap orders); 2) describing the differences in forms of legal process; 3) reporting on both the number of selectors specified in a request (names, email addresses, and other ways of identifying the subjects of a request) and the number or users and/or accounts responsive to a request; 4) explanations of what legal process the company requires for certain types of information; 5) explanations and examples of the difference between "content" and "non-content" information that the company may turn over; 6) reporting numbers on compliance with each kind of legal process as well as the different ways that a company may respond to a request; 7) reporting the number of users notified for unsealed requests; the number of users not notified for unsealed requests, and the number of sealed requests where companies were prevented from notifying users; and 8) reporting on the number of orders from the Foreign Intelligence Surveillance

These transparency best practices highlight how complex government requests for digital information can be, and how little the public knows without each service provider disclosing detailed, numeric and explanatory information about the requests they receive. In service providers' reports, the number of law enforcement requests often do not correspond on a one-to-one basis to the number of people whose data is given to law enforcement. *See* Google, Transparency Report, United States Jan2018-Jun2018 (In the six-month period, Google received 6,900 warrants for 18,091 user accounts).[16] And without explanation of the types of data that may be disclosed in response to each of the different legal mechanisms to request data, the public is left in the dark about new practices and methods law enforcement uses to obtain potentially privacy invasive information.

Voluntary transparency reporting by providers is the primary, but not sole, means by which the public learns about law enforcement requests for user data. There are a few statutes that require the federal government and courts to report statistics on certain electronic surveillance practices to Congress, but these reports do not provide enough information for meaningful public oversight. For example,

---

Court and on the number of requests for information that were made using national security letters. *Id.* at 4–5.

[16] https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts,compliance;authority:US;time:Y2018H1&lu=user_requests_report_period&legal_process_breakdown=expanded:0 (last visited Jan. 25, 2018).

the Pen Register Act requires the Attorney General to report the number of PR/TT requests from federal law enforcement agencies in a given year, including information about the duration and extensions of these orders, what offenses and investigations the requests are connected to, and district-level detail of the law enforcement agency making the requests. 18 U.S.C. § 3126. But the U.S. Department of Justice has been inconsistent in making this information available to the public. For instance, the DOJ's "FOIA Library" includes aggregated summaries from 2004–2017, showing only a thousand-foot view of how federal law enforcement uses this legal mechanism.[17] Only after a Freedom of Information Act lawsuit by the American Civil Liberties Union (ACLU) did the DOJ release the detailed reports required by statute, and then only for the years 2010 and 2011. *American Civil Liberties Union v. DOJ*, No. 12-CV-4093 (S.D.N.Y. May 23, 2012).[18] Further, the public cannot easily contrast the government's yearly report with communication service providers' reports because providers have not consistently reported the number of pen register orders they have received.[19] *See,*

[17] *FOIA Library*, U.S. Dep't of Justice (updated Nov. 27, 2018), https://www.justice.gov/criminal/foia-library; *see* Brief of Petitioners-Appellants at 6–7 (describing the paucity of DOJ's PR/TT order disclosures for 2017).

[18] The ACLU published the reports at https://www.aclu.org/other/pen-register-trap-and-trace-foia-request-documents-released-department-justice.

[19] Because of the lack of public information regarding pen register requests, researchers have not been able to adequately study whether reporting discrepancies exist between the government and communication service providers. However,

e.g., Facebook Transparency, United States (begins reporting number of pen registers received in January 2014);[20] Verizon, United States Report (provides pen register requests numbers for the second half of 2015);[21] Microsoft, Law Enforcement Requests Report (does not provide the number of pen register requests received).[22]

Public access to the court records sought here, not just the statistical information provided in reports that may be inaccurate, would provide a comprehensive record of law enforcement demands to companies for their users' data. By tracking docket entries, the public can see which companies are more frequently served with requests for electronic surveillance, and electronic

---

researchers have found significant discrepancies for other types of legal process. For instance, the Administrative Office of the U.S. Courts (AO) reported a total of 3,554 federal and state wiretaps for 2014, but the four biggest U.S. telephone companies (Verizon, AT&T, T-Mobile, and Sprint) reported a collective 10,712 wiretaps for 2014. *See* Albert Gidari, *Wiretap Numbers Don't Add Up*, Just Security (July 6, 2015), https://www.justsecurity.org/24427/wiretap-numbers-add/. Similarly, in 2015, the AO reported 4,148 total wiretaps, while the four carriers reported a total of 11,633 wiretaps. *See* Albert Gidari, *Wiretap Numbers Still Don't Add Up*, Stanford Ctr. for Internet and Soc'y (Nov. 29, 2016), http://cyberlaw.stanford.edu/blog/2016/11/wiretap-numbers-still-dont-add.

[20] https://transparency.facebook.com/government-data-requests/country/US/jan-jun-2014 (last visited Jan. 25, 2018).

[21] https://www.verizon.com/about/portal/transparency-report/us-report/ (last visited Jan. 25, 2018).

[22] https://www.microsoft.com/en-us/corporate-responsibility/lerr/ (last visited Jan. 25, 2018).

surveillance applications might show what legal mechanisms are used to make those requests.

B. Public Disclosure Would Also Help the Public Hold Private Companies Accountable Should They Fail to Adequately Protect Users' Data.

The public has an interest in knowing when and how frequently companies provide users' data to law enforcement. Disclosure of the records sought would not only fill in gaps in company and government reporting described above, it would also allow the public to check whether providers "walk the talk" when it comes to living up to their public promises to protect user data.

A large percentage of consumers have expressed a desire to change their communications habits to increase the security of their personal information from government surveillance, but it is hard for consumers to navigate service providers' transparency reports and stay up to date with Fourth Amendment case law so that they can ensure that their information is protected. That is in part why EFF created a consumer guide and policy document called *Who Has Your Back?* to explain corporate law enforcement compliance practices and to push for higher standards among service providers.[23]

[23] EFF has published an annual *Who Has Your Back?* report since 2011, focusing on various corporate disclosure practices and the role electronic communication services play in facilitating, storing, and moderating user speech online. The 2017 report is the latest guide for how electronic communication services respond to

The role of *Who Has Your Back?* is to provide objective measurements for analyzing the policies and advocacy positions of major technology companies when it comes to handing data to the government. Further, the guide is a tool to galvanize widespread changes in the policies of technology companies to ensure users' digital lives are not subject to invasive and undemocratic government searches.

The 2017 edition of *Who Has Your Back?* focused on measuring which companies protect their users by fighting against secret surveillance orders. Communication service providers were scored on whether they follow industry best practices like transparency reports, whether they notify their consumers about government requests, whether they fight against gag orders, whether they have made promises not to sell out users in order to cooperate with the government, and whether they support efforts to reform expansive surveillance laws. Although nine companies evaluated by EFF scored positively in all five categories, the report found serious shortcomings in many other companies' practices. For example, Amazon and WhatsApp, which both handle large quantities of sensitive user data, lacked adequate policies for notifying users of government requests, challenging NSL gag orders, and promises to prevent third parties from collecting and selling users' information to governments. Most notably, the four largest telecommunications

---

government requests for user information. *Who Has Your Back?* is available on EFF's website at https://www.eff.org/who-has-your-back-2017.

companies (AT&T, Comcast, T-Mobile, and Verizon) all lacked sufficient policies to protect their users' privacy.

The format of the report also tracks and provides an incentive for companies to increase their privacy and security practices across time. Between editions of the report, major technology companies have increased their commitment to user privacy and security. From 2013 to 2014, Amazon, Apple, and Yahoo all changed their policies to require law enforcement to provide a warrant to obtain users' content information.[24] The 2014 report actually gives these companies a gold star for their increased commitment to user rights.[25]

Because consumer guides such as *Who Has Your Back?* primarily rely on public statements and actions taken by tech companies, consumers are left to trust companies' promises that they protect user data. The problem is that in practice, service providers don't always hold themselves to their public promises. For instance, Apple marketed the iPhone and other products as some of the most secure devices in the consumer market because of both their hardware and the company's commitment to user privacy and security.[26] But until at least October 2015, the

---

[24] Compare *Who Has Your Back?* 2013, https://www.eff.org/who-has-your-back-2013 with *Who Has Your Back?* 2014, https://www.eff.org/who-has-your-back-2014.

[25] *Who Has Your Back?* 2014.

[26] On Apple's website the company says, "[W]e believe privacy is a fundamental human right . . . We've proved time and again that great experiences don't have to

company had secretly complied with overbroad government demands for assistance under the All Writs Act of 1789 in at least 70 cases involving older models of the iPhone and the iPhone operating system for which Apple had the ability to extract data from a locked iPhone. Katie Benner and Joseph Goldstein, *Apple Wins Ruling in New York iPhone Hacking Order*, N.Y. Times (Feb. 29, 2016).[27] Apple did not publicly challenge the law enforcement practice until a magistrate judge in New York requested Apple's views on whether the government could use the All Writs Act to seek this type of assistance and information. *Id.*; *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, 2015 WL 5920207 (E.D.N.Y. Oct. 9, 2015). Once prompted, Apple advocated for the security concerns of its users, arguing that the government's demand under the All Writs Act exceeded the bounds of mandatory law enforcement assistance, arguments the magistrate judge adopted to deny the request. *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court*, 149 F. Supp. 3d 341, 356–57 (E.D.N.Y. 2016).

Broader public disclosure of the judicial materials requested by Petitioners-Appellants would allow for more regular, permanent oversight of the companies'

---

come at the expense of your privacy and security. Instead, they can support them." Apple, Privacy, https://www.apple.com/privacy/ (last visited Jan. 25, 2018).

[27] https://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html.

disclosure practices. With the public's ability to verify and track service providers' disclosure habits through access to the court's docket and orders, the public will gain a more accurate picture of providers' practices and be in a better position to evaluate whether those actions match their public commitments to users' privacy and security.

CONCLUSION

For the foregoing reasons, *amici* respectfully request that the Court reverse the district court's decision and order the disclosure of court records sought by Petitioners-Appellants.

Dated: January 25, 2019

By: */s/ Aaron Mackey*
Aaron Mackey

Attorneys for Amici Curiae

CERTIFICATE OF COMPLIANCE

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

1. This Brief of *Amicus Curiae* Electronic Frontier Foundation in Support of Petitioners-Appellants complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,185 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 2016, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: January 25, 2019

By: /s/ Aaron Mackey

Aaron Mackey
Camille Fischer
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109-7701
Tel: (415) 436-9333
amackey@eff.org

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I, Aaron Mackey, hereby certify that on January 25, 2019, I electronically filed the foregoing Brief of *Amicus* Curiae of Electronic Frontier Foundation with the United States Court of Appeals for the District of Columbia through the Court's CM/ECF system, which will serve all Counsel who are registered CM/ECF users.

By: */s/ Aaron Mackey*
Aaron Mackey

Attorneys for Amici Curiae