APL-2015-00318
New York County Clerk's Index Nos. 30207/13 and 30178/14

Court of Appeals
of the
State of New York

IN RE 381 SEARCH WARRANTS DIRECTED TO FACEBOOK, INC.,
AND DATED JULY 23, 2013

FACEBOOK, INC.,

Appellant,

– against –

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE,

Respondent.

IN THE MATTER OF THE MOTION TO COMPEL DISCLOSURE OF
THE SUPPORTING AFFIDAVIT RELATING TO CERTAIN SEARCH WARRANTS
DIRECTED TO FACEBOOK, INC., DATED JULY 23, 2013

FACEBOOK, INC.,

Appellant,

– against –

NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE,

Respondent.

BRIEF OF *AMICI CURIAE* BRENNAN CENTER FOR JUSTICE, ELECTRONIC FRONTIER FOUNDATION, ACCESS NOW, AND TECHFREEDOM

FAIZA PATEL
MICHAEL PRICE
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
Counsel for Amicus Curiae Brennan Center for Justice
120 Broadway, Suite 1750
New York, New York 10013
Tel.: (646) 292-8335
Fax: (212) 463-7308

BRETT J. WILLIAMSON
NATE ASHER
DAVID K. LUKMIRE
O'MELVENY & MYERS LLP
Counsel for Amici Curiae Brennan Center for Justice, Electronic Frontier Foundation and TechFreedom
Times Square Tower
7 Times Square
New York, New York 10036
Tel.: (212) 326-2000
Fax: (212) 326-2061

CARA L. GAGLIANO
(Pro Hac Vice Application Pending)
O'MELVENY & MYERS LLP
Counsel for Amici Curiae Brennan Center for Justice, Electronic Frontier Foundation and TechFreedom
Two Embarcadero Center, 28th Floor
San Francisco, California 94111
Tel.: (415) 984-8899
Fax: (415) 984-8701

PETER MICEK
AMIE STEPANOVICH
ACCESS NOW
Counsel for Amicus Curiae Access Now
34 West 27th Street, 6th Floor
New York, New York 10001
Tel.: (888) 414-0100

RULE 500.1(f) CORPORATE DISCLOSURE STATEMENT

Amicus curiae Brennan Center for Justice at NYU School of Law ("Brennan Center") is a non-profit, non-partisan 501(c)(3) organization. The Brennan Center has no parents, subsidiaries, or affiliates.

Amicus curiae Electronic Frontier Foundation ("EFF") is a non-profit, non-partisan 501(c)(3) organization. EFF has no parents, subsidiaries, or affiliates.

Amicus curiae Access Now is a non-profit, non-partisan 501(c)(3) organization. Access Now has three non-U.S. affiliates. Access Now Tunis is registered in Tunisia as a foreign association branch. Fundacion Access is registered in Costa Rica as a representative office of Access Now. Access Now Europe is registered in Belgium as an international not-for-profit association.

Amicus curiae Technology Freedom Institute, d/b/a TechFreedom, is a non-profit, non-partisan 501(c)(3) organization. TechFreedom has no parents, subsidiaries, or affiliates.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Other Authorities

PRELIMINARY STATEMENT

This Court has long been mindful of protecting New York citizens' Fourth Amendment freedoms. The First Department's decision, if allowed to stand, will enable future violations of constitutional privacy rights. It should be reversed and Facebook's motion to quash granted, based on three key principles that should guide both this Court's analysis of the 381 warrants served on Facebook (the "Bulk Warrants") and broader judicial consideration of digital information gathering.[1]

First, courts should apply the Fourth Amendment with full force to protect against improper government access to personal data that is stored with Internet Service Providers ("ISPs").[2] This data often includes both "sensitive records previously found in the home" and highly personal information "never found in a home in any form." *Cf. Riley v. California*, 134 S. Ct. 2473, 2491 (2014). It also tends to include significant amounts of expressive material, making robust Fourth Amendment protection crucial to guarding First Amendment freedoms. The fact that such data is held by a third-party ISP like Facebook should not diminish Fourth Amendment protections. If anything, searches and seizures of data held by ISPs deserve heightened Fourth Amendment scrutiny because the aggregation and

[1] The statements of interests of *amici curiae*, as well as their disclosure statements, are attached in the Appendix to this brief.

[2] As used in this brief, an ISP is any entity that offers a web-based service, such as a web browser, a search engine, web-based email, a social media platform, or cloud-based file storage.

remote storage of private data greatly reduces resource constraints on law enforcement and allows for the bulk warrant tactics employed here.

Second, the Fourth Amendment's particularity requirement must be carefully considered when evaluating warrants authorizing the search and seizure of electronic data. The particularity requirement ensures that the government cannot obtain a general warrant to rummage indiscriminately through a person's papers and effects. The broad spectrum of data stored and commingled in digital form threatens to convert any warrant for electronic information into a general warrant if not tightly constrained. And that is precisely what happened here: the government seized, searched, and retained essentially all of the information contained in the Facebook accounts of 381 individuals. Much more than just individual posts or photos, the seized data also exposed to the government a trove of sensitive, personal information that users never chose to share with ***anyone***. Although the practical complexities of digital searches may require some degree of initial "overseizure," courts should not allow these complexities to eviscerate the Fourth Amendment by endorsing a "seize-all, search-all" approach.

Third, courts must recognize that copying electronic data—whether done by law enforcement or a third party acting at the government's behest—is a seizure and thus a Fourth Amendment event, regardless of whether the data is ever reviewed. "A 'seizure' of property occurs when there is some meaningful

interference with an individual's possessory interests in that property." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). Under well-established legal principles, copying electronic data interferes with an individual's possessory interests in controlling access to that data. The Appellate Division's contrary conclusion opens the door to the over-collection and retention of personal data.

ARGUMENT

I. User Data Stored with Internet Service Providers Requires Vigorous Fourth Amendment Protections.

The First Department's startling suggestion that "the Fourth Amendment's protections are potentially far weaker" when "applied to information stored online" (Appellate Division opinion at A.26) turns a growing body of federal and state case law on its head. It also reflects a flawed understanding of the Fourth Amendment that threatens individual privacy if not corrected by this Court.

A. The Types of User Data Stored by ISPs Heighten the Privacy Interests at Stake.

The quantity and breadth of data commonly stored by ISPs can turn even a limited search and seizure into a substantial invasion of privacy. The U.S. Supreme Court's opinion in *Riley v. California* highlights the unique Fourth Amendment challenges posed by collection of digital data. In *Riley*, the Court recognized that searches of digital data are qualitatively different from physical searches and instructed courts to consider how these differences impact the scope of Fourth Amendment protection. *See* 134 S. Ct. at 2484–85, 2488–89. Although

Riley dealt with cell phone data rather than ISP-held user data, the concerns that the Court voiced in *Riley* apply equally here. In fact, the Court's three examples of data that raise special privacy concerns—Internet search and browsing history, historical location information, and mobile application data—are each implicated by searches and seizures of Facebook user data, as detailed below.

1. *"An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."*[3]

The Bulk Warrants required Facebook to provide "[a]ll 'Searches' data" associated with each target account. (Sample search warrant at A.42.) Like any Internet search history, users' Facebook searches disclose what was occupying their minds—even things people may never share with others. Just as with the cell phone at issue in *Riley*, Facebook allows users to search for things like illness support groups, treatment center reviews, and resources for guidance on personal finances, marital issues, or parenting decisions.[4] Likewise, Facebook data includes information about "the types of content [users] view or engage with."[5] If

[3] *Id.* at 2490.

[4] *See What can I search for on Facebook?*, Facebook, https://www.facebook.com/help/400002116752060?helpref=uf_permalink (accessed Nov. 26, 2016).

[5] *Data Policy*, Facebook, https://www.facebook.com/full_data_use_policy (last revised Sept. 29, 2016).

a user clicks on links about marital advice, or views news stories about medical breakthroughs, that information will also be reflected in Facebook's records.[6] This would include frequent visits to articles on WebMD, which uses Facebook's services.[7] Moreover, the Bulk Warrants directed Facebook to provide all "Likes on Other Sites' data"—*i.e.*, data created when an individual clicks on the "Like" button—for each target account. (A.42.)

2. *"Mobile application software on a cell phone, or 'apps,' offer a range of tools for managing detailed information about all aspects of a person's life . . . which together can form a revealing montage of the user's life."*[8]

Facebook owns and operates more than the Facebook social media platform. Popular Facebook-owned apps include Instagram (photo-sharing), Moves (fitness-tracking), WhatsApp (voice-calling and messaging), and Onavo Protect (data usage monitoring).[9] Together, the data from these apps—all of which is

---

[6] Law enforcement can even obtain information about what content a Facebook user chooses *not* to view. The Bulk Warrants sought "[a]ll associated data that is 'Hidden from News Feed,' including any friends, apps, or pages hidden from the News Feed." (A.42.) *See How can I see fewer News Feed stories from a person, Page or group that I follow?*, Facebook, https://www.facebook.com/help/745556738851537?helpref=uf_permalink (accessed Nov. 27, 2016).

[7] *See, e.g.*, *Ulcerative Colitis - Symptoms*, WebMD, http://www.webmd.com/ibd-crohns-disease/ulcerative-colitis/ulcerative-colitis-symptoms (accessed Nov. 26, 2016) (note presence of Facebook "Share" button).

[8] *Riley*, 134 S. Ct. at 2490.

[9] *See The Facebook Companies*, Facebook, https://www.facebook.com/help/111814505650678?helpref=uf_permalink (accessed Nov. 27, 2016) (listing companies owned by Facebook and providing links to their privacy policies).

maintained by Facebook—would form the same kind of "revealing montage" that troubled the *Riley* Court. *See* 134 S. Ct. at 2490. But in addition to the apps it owns, Facebook's records will also reflect information from a host of third-party apps that use Facebook's services. *See Data Policy*, *supra*. One example is Everyday Health's pregnancy-tracking app What to Expect.[10] Permitting the First Department's ruling to stand could allow the government breathtaking access to this kind of intimate personal information.

3. *"Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."*[11]

Five years before *Riley* was decided, this Court expressed apprehension about GPS tracking in *People v. Weaver*, 12 N.Y.3d 433 (2009). The data from a GPS unit attached to a person's vehicle, the Court observed, would disclose "trips the indisputably private nature of which takes little imagination to conjure" and would provide law enforcement with "a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious,

[10] *Popular Pregnancy App Grows Native Ad Revenue 30% With the Audience Network*, Facebook, https://www.facebook.com/audiencenetwork/success-stories/what-to-expect (accessed Nov. 27, 2016); *cf. Riley*, 134 S. Ct. at 2490 (mentioning "apps for tracking pregnancy symptoms" as a type of app conveying sensitive personal information).

[11] *Riley*, 134 S. Ct. at 2490.

amicable and amorous, to name only a few—and of the pattern of our professional and avocational pursuits." *Id.* at 441–42.

But law enforcement no longer needs to search a suspect's phone or install a GPS device to obtain this information. Of the 1.71 *billion* users who accessed Facebook in June 2016, 91.8% accessed Facebook from a mobile device at least once, and 56.5% accessed Facebook *exclusively* from a mobile device.[12] Mobile usage gives Facebook a record of the historic location of a user's mobile device over a potentially lengthy period of time. *See Data Policy*, *supra* ("We collect information from or about the computers, phones, or other devices where you install or access our Services . . . including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals."). Facebook also stores other data that law enforcement can use to reconstruct a person's movements, including "IP logs,"[13] "check-in" data,[14] and photo metadata.[15]

---

[12] Emil Protalinski, *Facebook passes 1 billion mobile daily active users*, VentureBeat (July 27, 2016, 1:19 PM), http://venturebeat.com/2016/07/27/facebook-passes-1-billion-mobile-daily-active-users/.

[13] *See* A.42. The Internet Protocol ("IP") addresses for each device used to access a Facebook account allows law enforcement to determine users' past locations, with varying degrees of precision. *See generally* Craig A. Shue et al., *From an IP Address to a Street Address: Using Wireless Signals to Locate a Target* (2013), https://www.usenix.org/system/files/conference/woot13/woot13-shue.pdf.

[14] *See* A.42. A "check-in" is a type of Facebook post used to identify the user's location. *See How do I check into a nearby location?*, Facebook, https://www.facebook.com/help/174846215904356?helpref=uf_permalink (accessed Nov. 26, 2016).

The Facebook user data at issue here is precisely the kind of information that the *Riley* Court sought to protect from unlawful searches and seizures. This Court should therefore reject the First Department's suggestion that Fourth Amendment protections are weaker when applied to information stored online and ensure that constitutional guarantees continue to adapt to advances in technology.

B. Privacy of User Data Stored by ISPs Is Key to the Promotion of First Amendment Freedoms.

Assuring robust Fourth Amendment protection for ISP-held user data safeguards more than privacy rights; it also guarantees other essential liberties, including freedom of speech, freedom of the press, and freedom of association. As this Court noted in the GPS-tracking context, "what the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations . . . ." *Weaver*, 12 N.Y.3d at 442. That risk is especially salient in the context of online communications and social media platforms, which are hubs for data having significant expressive and associational value.

---

[15] *See* A.41. When a photo is taken digitally, the resulting image file includes additional information about the photo in the form of metadata, which may include GPS data. *See* Hanni Fakhoury, *A Picture is Worth a Thousand Words, Including Your Location*, Electronic Frontier Foundation: Deeplinks Blog (April 20, 2012), https://www.eff.org/deeplinks/2012/04/picture-worth-thousand-words-including-your-location.

The threat of chill is more than theoretical. This past May, a division of the U.S. Department of Commerce published findings about the chilling effects that result from insufficient privacy protections for online data. Of the more than 41,000 households surveyed, 19% said they had refrained from expressing opinions on controversial or political issues online because of privacy or security concerns.[16] Among those respondents who cited data collection or tracking by the government as a major online privacy concern (18% of the total), the percentage who reported self-censoring rose to 29%. *Id.* Other recent studies have reached similar conclusions.[17]

The Supreme Court has long recognized the close relationship between Fourth Amendment protections and First Amendment freedoms. *See Marcus v. Search Warrants of Prop. at 104 E. Tenth St., Kansas City, Mo.*, 367 U.S. 717, 729

---

[16] Rafi Goldberg, Nat'l Telecomm. & Info. Admin., *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA Blog (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities.

[17] *See, e.g.*, Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 96 Journalism & Mass Comm. Q. 296 (2016) (finding study participants significantly less likely to comment on fictional Facebook posting about U.S. airstrikes against ISIS if they (a) perceived themselves to hold a minority view on the topic, (b) were primed to be aware of online surveillance by the NSA, and (c) believed the NSA's surveillance to be justified), *available at* http://jmq.sagepub.com/content/93/2/296.full.pdf+html; Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 Berkeley Tech. L.J. (forthcoming 2016) (finding significant decrease in page views of terrorism-related Wikipedia articles after June 2013 NSA/PRISM online surveillance revelations), *draft available at* http://btlj.org/wp-content/uploads/2016/05/Penney_31APR2016.pdf.

(1961) ("The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression."); *Frank v. Maryland*, 359 U.S. 360, 376 (1959) (Douglas, J., dissenting) ("[The First, Fourth, and Fifth Amendments] are indeed closely related, safeguarding not only privacy and protection against self-incrimination but 'conscience and human dignity and freedom of expression as well.'"); *see also NAACP v. Alabama*, 357 U.S. 449, 462 (1958) ("This Court has recognized the vital relationship between freedom to associate and privacy in one's associations."). In light of these intertwined interests, "[w]here the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with 'scrupulous exactitude.'" *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)); *see also NAACP*, 357 U.S. at 460–61 ("[S]tate action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny.").

The Sixth Circuit thus observed in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), that email may serve as an "essential means or necessary instrument[ ] for self-expression, even self-identification," requiring "strong protection under the Fourth Amendment." *Id.* at 286 (quoting *City of Ontario v. Quon*, 130 S. Ct. 2619, 2630 (2010)) (alteration in original). In another case, a

federal magistrate expressed concern that warrants seeking information about Facebook groups—such as the warrants at issue here (*see* A.41)—"would require Facebook to turn over membership lists, which implicates the right to free association found in the First Amendment." *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis*, 21 F. Supp. 3d 1, 7 (D.D.C. 2013). By failing to take these considerations into account, the First Department's approach to privacy analysis threatens both Fourth *and* First Amendment rights.

C. The "Third-Party Doctrine" Should Not Apply.

None of the concerns outlined above is lessened by the role of third-party service providers in storing their users' data. Indeed, the majority in *Riley* pointed to the widespread use of cloud-based services as a factor *increasing* the privacy concerns implicated by cell phone searches. 134 S. Ct. at 2491. The Court explained (and the government conceded) that the search-incident-to-arrest exception could not possibly extend to "data stored on remote servers rather than on the device itself"—*i.e.*, data stored by third-party service providers. *Id.*

As Justice Sotomayor warned, the so-called "third-party doctrine" is "ill suited" to an age "in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

Understandably, the doctrine has encountered a growing chorus of criticism as people live more of their lives online. *See generally* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. Nat'l L. & Pol'y 247, 268 (2016). Users of online services are no less reasonable in their expectation of privacy when they store documents on Dropbox or send a private message on Facebook than when they rent a storage locker or hand a letter to a postal worker. Each act involves "entrust[ing] the security of . . . information to a third party" (Appellate Division opinion at A.26), yet no one reasonably contests that the Fourth Amendment protects the contents of both the storage unit and the envelope. Especially in view of the sensitive data they often contain, one's digital "papers" should enjoy at least as much constitutional protection as a letter delivered by the post office.

The Sixth Circuit reasoned in *Warshak* that email "is the technological scion of tangible mail" and that it would "defy common sense to afford emails lesser Fourth Amendment protection." 631 F.3d at 285–86. *Warshak* dismantled the argument that a service provider's ability to access user data diminishes the protection that data should receive. In the context of electronic communications, the court explained, "the ISP is the functional equivalent of a post office or a telephone company"—an intermediary necessary for the system to function, not an invited participant in the conversation. *Id.* at 286. (*Cf.* Sept. 17, 2013 Supreme

Court opinion at A.33 ("Facebook could best be described as a digital landlord, a virtual custodian or storage facility for millions of tenant users and their information.").)

Since *Warshak*, a growing number of courts have concluded that the third-party doctrine need not—and should not—apply to emails, text messages, or private Facebook content. A federal court in Minnesota, for instance, found that a middle-school student whose Facebook and email accounts had been searched by school officials "had a reasonable expectation of privacy to her private Facebook information and messages." *R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149*, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012). Unlike the First Department, the court in *R.S.* distinguished between Facebook content that a user makes visible to the public and content that the user has endeavored to keep private, concluding that for purposes of an electronic data search, "one cannot distinguish a password-protected private Facebook message from other forms of private electronic correspondence." *Id.* In another recent case, a federal court evaluating a motion to suppress evidence seized from a Google account recognized that email contents, address books, contact lists, calendar data, pictures, and files are "indeed protected by the Fourth Amendment." *United States v. Shah*, No. 5:13-CR-328-FL, 2015 WL 72118, at *11 (E.D.N.C. Jan. 6, 2015). Other courts have followed suit. *See Thompson v. City of Chicago Bd. of Educ.*, No. 14-CV-6340, 2016 WL 362375, at

*8 (N.D. Ill. Jan. 29, 2016) (holding that "the third-party doctrine does not control" when the government subpoenas a service provider for the contents of a subscriber's personal emails); *Commonwealth v. Jordan*, No. 1584CR10098, 2015 WL 9902718, at *8 (Mass. Super. Ct. Dec. 30, 2015) ("A cell phone user's strong privacy interest in his or her text messages and other private communications and information does not evaporate merely because, with the advent of cloud computing, those things are now likely to be stored on devices maintained by or for one's wireless service provider."); *State v. Hinton*, 179 Wash. 2d 862, 873–75, 319 P.3d 9, 14–15 (2014) (text messages receive privacy protection under state constitution despite "incidental exposure of private information" to cell phone company); *State v. Clampitt*, 364 S.W.3d 605, 611 (Mo. Ct. App. 2012) (extending *Warshak* to text messaging).

In an age where virtually all private communications go through digital intermediaries, the First Department's reliance on the third-party doctrine threatens to render the Fourth Amendment obsolete as a means of protecting information privacy. At least one lower court has already expressed this fear, but felt constrained by the Appellate Division's direction. In *People v. Thompson*, 51 Misc. 3d 693 (Sup. Ct., N.Y. Cnty. 2016), the first published opinion to apply *381 Search Warrants*, the court criticized the First Department's "assertion that no Fourth Amendment protections apply to [email] communications because email

requires an email account," calling it "an archaic notion which negates the protection of the Fourth Amendment for many of our most private communications." *Id.* at 710. Nonetheless, the court reluctantly acknowledged *381 Search Warrants* as binding precedent that foreclosed Fourth Amendment protection—and thus a suppression remedy—for *any* form of digital content held by an ISP. *Id.* at 709, 713–14. This Court should prevent a repeat of that result.

Indeed, this Court has previously recognized that changes in how we interact should not alter the Fourth Amendment protections afforded those interactions. *See Weaver*, 12 N.Y.3d at 442–43 ("Cell technology has moved presumptively private phone conversation from the enclosure of *Katz*'s phone booth to the open sidewalk and the car, and the advent of portable computing devices has resituated transactions of all kinds to relatively public spaces. . . . [T]his change in venue has not been accompanied by any dramatic diminution in the socially reasonable expectation that our communications and transactions will remain to a large extent private.") *Amici* urge the Court to extend that understanding into the context of online data and decline to extend the third-party doctrine into the digital age.

D. Few Practical Barriers Exist to Dissuade the Government from Executing Broad Searches and Seizures of User Data Stored by ISPs.

The Bulk Warrants illustrate the newfound ease with which law enforcement can conduct highly invasive searches of hundreds of people at a time. In the world

of physical searches, searching the homes of 381 different people would require 381 separate warrants identifying 381 separate physical locations. Law enforcement officials would then have to deploy to those 381 locations, conduct their searches, and gather evidence. The resources required to conduct such an operation would be significant, providing a built-in deterrent to government overreach.

Here, by contrast, an investigator with the District Attorney's Office served all 381 warrants—"identical in scope" and supported by one 93-page affidavit—on a single private party, at once, via an online portal. (A.33; Respondent's Br. at 3.) In other words, one investigator executed 381 warrants with the click of a mouse. Facebook was then required to seize a broad array of data associated with the 381 target accounts and provide it to the District Attorney's Office "in a format convenient for law enforcement." *Id.* No law enforcement personnel were required to be present while Facebook carried out these directives. *Id.*

Hardly any additional effort is required for investigators to include another account, or ten, or a hundred, in a list of search targets—with each addition representing another private life to rifle through. When the costs of an expansive search are so low, investigators have little incentive to narrow their suspect pool or constrain their demands for data. This dramatic shift in the cost-benefit calculus makes judicial scrutiny of warrants directed at online service providers all the more

important, as a single request can sweep up stockpiles of private data belonging to hundreds of people who may never have the opportunity to challenge the lawfulness of the search and seizure.

II. The Particularity Requirement Takes On Special Importance in the Digital Context.

For any warrant to pass muster under the Fourth Amendment, it must "particularly describe[] the place to be searched, and the persons or things to be seized." U.S. Const. Amend. IV. Courts have struggled with questions about what this bedrock principle requires in the digital context, where traditional notions of "places" and "things" are often inapposite. But just as the realities of the digital age demand that constitutional protections extend to user data stored by ISPs, they also highlight the importance of the Fourth Amendment's particularity requirement in the context of digital searches and seizures.

A. Digital Searches and Seizures Implicate Concerns at the Heart of the Particularity Requirement.

The particularity requirement "was designed to prohibit law enforcement agents from undertaking a general exploratory search of a person's belongings." *People v. Brown*, 96 N.Y.2d 80, 84 (2001) (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)). "Indeed, indiscriminate searches pursuant to general warrants 'were the immediate evils that motivated the framing and adoption of the Fourth Amendment.'" *Id.* (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)).

Yet technological advances threaten to undermine this check by aggregating large quantities of private data in one "place" and storing all "things" as long strings of electronic zeros and ones. Authorities are undoubtedly tempted to seize entire caches of private data and sift through it later using sophisticated investigatory software—as was done here. But this process entails seizing vast quantities of private information for which there is no probable cause, an invasion of privacy that only becomes more acute as the amount of data increases.

The U.S. Supreme Court recognized this dynamic in the context of telephone wiretaps, putting the onus on law enforcement to minimize the intrusion on lawful conversations that investigators have no probable cause to monitor. The Court observed that "[b]y its very nature eavesdropping involves an intrusion on privacy that is broad in scope," making "[t]he need for particularity . . . especially great." *Berger v. New York*, 388 U.S. 41, 56 (1967).

Likewise, the particularity requirement assumes an important role in the context of digital searches and seizures, which implicate substantial invasions of privacy far beyond the scope of any suspected wrongdoing. Indeed, courts across the country—including the highest courts of at least five states[18] and at least four

[18] *See Wheeler v. State*, 135 A.3d 282, 307 (Del. 2016) ("[T]he risk that warrants for digital and electronic devices take on the character of 'general warrants' is substantial. This reality necessitates heightened vigilance, at the outset, on the part of judicial officers to guard against unjustified invasions of privacy."); *State v. Castagnola*, 46 N.E.3d 638, 656 (Ohio 2015) holding

federal courts of appeal[19]—have recognized that the volume and breadth of personal information stored on electronic devices and in online accounts demand close attention to the particularity requirement.

---

warrant for search of computer insufficiently particularly and highlighting risk to privacy interests posed by overly general electronic warrants); *State v. Fuller*, 332 P.3d 937, 950 (Utah 2014) (concluding warrant was sufficiently particular but warning that "law enforcement must be increasingly cautious with respect to the particularity requirement" in digital contexts); *In re Appeal of Application for Search Warrant*, 71 A.3d 1158, 1175 (Vt. 2012) ("Computer search warrants are the closest things to general warrants we have confronted in the history of the Republic."); *State v. Sprunger*, 811 N.W.2d 235, 244 (Neb. 2012) (explaining that "particularity and probable cause requirements [are] all the more important" in the context of searches of personal computers).

[19] *United States v. Galpin*, 720 F.3d 436, 446–47 (2d Cir. 2013) (electronic search warrants "demand[] a heightened sensitivity to the particularity requirement," lest they become de facto general warrants); *United States v. Rarick*, 636 F. App'x 911, 914–15 (6th Cir. 2016) (courts must "take care not to give the Government free rein to essentially do away with the particularity requirement by allowing it to examine every file on the device"); *United States v. Otero*, 563 F.3d 1127, 1131–32 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important."); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171 (9th Cir. 2010) (The Fourth Amendment requires the government to "maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases."). *See also United States v. Winn*, 79 F. Supp. 3d 904, 918–22 (S.D. Ill. 2015) (warrant for search of smartphone that "merely described the categor[ies] of data [sought], rather than specific items" to be insufficiently particular); *United States v. DSD Shipping, A.S.*, No. CR 15-00102-CG-B, 2015 WL 5164306, at *8 (S.D. Ala. Sept. 2, 2015) ("Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance."); *In re Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159, 166–69 (D.D.C. 2014) (denying application for warrant to search cell phone data based on insufficiently particular proposed search methodology); *In re United States of America's Application for a Search Warrant to Seize & Search Elec. Devices from Edward Cunnius*, 770 F. Supp. 2d 1138 (W.D. Wash. 2011) (discussing importance of particularity requirement for electronic searches and denying warrant application).

B. The Bulk Warrants Are Insufficiently Particular.

The Bulk Warrants failed to meaningfully limit the scope of the initial seizure and subsequent search, demanding virtually all records about everything the targeted users have ever done on Facebook. (*See* Appellant's Br. at 41–43; Appellant's Reply Br. at 27.) While courts have permitted a degree of "overseizure" owing to practical considerations, these concerns cannot trump constitutional rights. Whatever accommodations may be necessary to properly conduct digital searches and seizures, they cannot swallow the Fourth Amendment's particularity requirement and make "seize-all, search-all" the norm.

Even in the digital context, the data to be searched and seized must be described with as much precision as the circumstances allow. At a minimum, the Bulk Warrants should have included temporal limitations relevant to the facts of the disability fraud investigation. They did not.[20] But courts have noted that "a warrant's failure to include a time limitation, where such limiting information is available and the warrant is otherwise wide-ranging, may render it insufficiently particular." *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 460 (S.D.N.Y. 2013) (quoting *United States v. Costin*, No. 5 Cr. 38, 2006 WL 2522377, at *12 (D. Conn. July 31, 2006)). Given the likely scope and volume of unrelated

[20] One category of data, user IP logs, was limited to a three-and-a-half year period. (A.42.) No other category of data had a similar temporal restriction.

personal information contained in the target Facebook accounts, the court should have rejected the Bulk Warrants as insufficiently particular. Instead, the court "authorize[d] law enforcement to seize, search, retrieve, and view ***all*** the data, information, and images provided to them by Facebook." (A.43 (emphasis added).)

The Government's suggestion that the secret 93-page affidavit might somehow excuse these flaws is unavailing. (*See* Respondent's Br. at 47.) The ***warrant*** must be sufficiently particular in order for the court to establish limits for investigators, and for those limits to have teeth. *See Groh v. Ramirez*, 540 U.S. 551, 557 (2004). As is evident from the facts of this case, an unadorned warrant with a secret supporting affidavit is not enough to prevent law enforcement from seizing and searching nearly every bit of data in hundreds of private accounts. That cannot be what the Fourth Amendment means by particularity, or else it is meaningless in the digital age.

Upholding the First Department's decision will send a dangerous signal. The government will have the Court's imprimatur to seize social media accounts in their entirety and search through the data without restriction. And it requires no large leap to apply that logic to email accounts, cell phone records, or computer hard drives as well, raising the specter of a modern-day general warrant where

investigators "fetch[] a sack and fill[] it" with all of one's private digital papers. *See Wilkes v. Wood*, Lofft 1, 4, 98 Eng. Rep. 489, 491 (C.P. 1763).

III. Copying Electronic Data Is a Seizure and Therefore a Fourth Amendment Event.

In its briefs, Facebook describes the undue burden it faced in conducting an unconstitutional search and seizure of its users' data at the government's behest. (Appellant's Br. at 27; Appellant's Reply Br. at 11–13.) Facebook believes the search and seizure not only violated the constitutional rights of its users, but conscripted Facebook to engage in those violations in a way that could undermine confidence in the company's services. The government disputes this position, claiming that mere discomfort does not evidence undue burden. (Respondent's Br. at 44.) But this improperly downplays the key Fourth Amendment moment when Facebook copied and thereby seized its users' data on behalf of the government. Facebook was not a mere bit player uncomfortable with its role; rather, it seized user information while acting as an agent of the government. The Court should heed Facebook's concerns about being conscripted to take part in that seizure.

The First Department incorrectly brushed aside the notion that Facebook played a meaningful role in any Fourth Amendment events. (*See* Appellate Division opinion at A.23 (criticizing Facebook's argument that it was responsible for seizing data as "oblivious to the . . . context of digital information").) But the First Department was relying on an outdated law review article that has been

repudiated by its author in reaching that view. *Compare id.* at A.23–A.24 (citing Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005)) *with* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 704 (2010) (explaining that approach regarding seizures in his earlier article "was wrong" and "did not recognize the importance of access to data in the regulation of government evidence collection."). Later scholarship and case law make clear that the Fourth Amendment is implicated at the moment data is copied, and thereby seized.

As many courts and commentators agree, copying data constitutes a seizure because the act of copying interferes with the user's possessory interests in controlling the flow of the data and who has access to the data.[21] *See United States v. Jacobsen*, 466 U.S. 109, 113 (1984) ("A 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."). By copying electronic data, the government "interrupts the course of the data's possession or transmission" and "interferes with the owner's right to control the [data]." *See* Kerr, *Fourth Amendment Seizures*, *supra*, at 703, 711. Recognizing this, the Second Circuit recently described data-copying by Microsoft

[21] As Facebook's Terms of Service assures Facebook users, "[they] own all of the content and information [they] post on Facebook, and [they] can control how it is shared through [their] privacy and application settings." *Statement of Rights and Responsibilities*, Facebook, https://www.facebook.com/legal/terms (last revised Jan. 30, 2015).

pursuant to a warrant to be a "seiz[ure] by Microsoft, acting as agent of the government." *In re a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft*, No. 14-2985, 2016 WL 3770056, at *17 (2d Cir. July 14, 2016) (en banc). The court further held that the seizure in question happened at the moment the data was copied. *Id.* *See also United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (en banc) (referring to copying of electronic data as seizure throughout opinion); *Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (same); *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002) (describing retrieval by Yahoo! technicians of information from two e-mail accounts as a "seizure"); *In re Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.Com Maintained at Premises Controlled by Google, Inc.*, No. 14 Mag. 309, 2014 WL 3583529, at *4–5 (S.D.N.Y. Aug. 7, 2014) (copying of electronic evidence is an "exercise of dominion essentially amount[ing] to a 'seizure' even if the seizure takes place at the premises searched and is only temporary"); *United States v. Lustyik*, 57 F. Supp. 3d 213, 232 n.13 (S.D.N.Y. 2014) (finding seizure "also occurred when [the] email service provider copied the contents of his email account and provided that copy to the government.").

"The text of the Fourth Amendment reflects its close connection to property." *Jones*, 132 S. Ct. at 949. In the case of intangible property such as

electronic communications, "[t]he value of data lies in the information it contains and the ability to exclude others from accessing it." Price, *supra*, at 279. Indeed, as the Tenth Circuit recently recognized, an individual's ability to exclude others from accessing data harkens a property owner's right to prevent trespasses to chattel. *See United States v. Ackerman*, 831 F.3d 1292, 1307–08 (10th Cir. 2016). As Justice Alito noted in his concurring opinion in *Jones*, common law previously permitted a chattel owner to pursue a trespass claim even absent damage to the chattel, so long as the "dignitary interest in the inviolability of chattel[]" was harmed. *See Jones*, 132 S. Ct. at 958 n.4 (internal quotation omitted). And because the Fourth Amendment was meant to be "no less protective of persons and property against government invasions than the common law was at the time of founding," this Court should view the Government's copying of user data as undermining the inviolability of that data, thereby constituting a Fourth Amendment event. *Ackerman*, 831 F.3d at 1307.

Both the First Department and the government erred by failing to recognize that Facebook was directly engaged in a Fourth Amendment event—a seizure—when it copied its users' data. This Court should correct those errors and appropriately weigh Facebook's role as the seizing party when evaluating its "undue burden" argument. Regardless of how the Court decides that issue, the

ruling should recognize that copying data constitutes a seizure and thus implicates the Fourth Amendment.

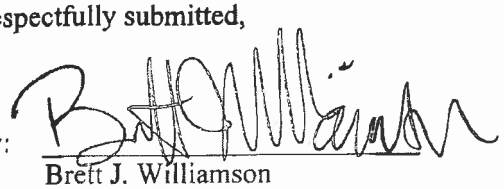
CONCLUSION

This Court has long been mindful of protecting New York citizens' Fourth Amendment freedoms. The First Department's decision, if allowed to stand, will enable future violations of constitutional privacy rights. *Amici* therefore urge this Court to decide in Facebook's favor on each of the issues raised on this appeal and set clear precedent on the scope of Fourth Amendment protection afforded to electronic data.

(Signatures on following pages)

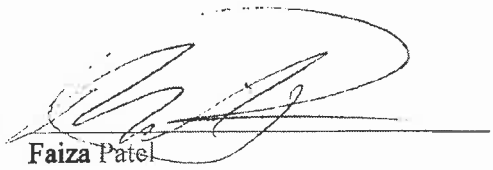
Dated: New York, New York
December 30, 2016

Respectfully submitted,

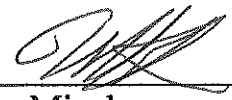
By: 

Brett J. Williamson
Nate Asher
David K. Lukmire
O'MELVENY & MYERS LLP
7 Times Square
New York, NY 10036
(212) 326-2000

Cara L. Gagliano (Pro Hac Vice Application Pending)
O'MELVENY & MYERS LLP
Two Embarcadero Center, 28th Floor
San Francisco, California 94111
(415) 984-8899

By: 

Faiza Patel
Michael Price
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
120 Broadway, Suite 1750
New York, New York 10271
(646) 292-8335

By: 

Peter Micek
Amie Stepanovich
ACCESS NOW
34 West 27th Street, 6th Floor
New York, New York 10001
(888) 414-0100

Counsel for Amicus Curiae
Access Now

APPENDIX

STATEMENTS OF INTEREST OF *AMICI CURIAE*

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice, including access to the courts and constitutional limits on the government's exercise of power. The Center's Liberty and National Security ("LNS") Program uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic surveillance and related law enforcement policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on privacy and First Amendment freedoms. As part of this effort, the Center has filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including in *In re a Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft*, No. 14-2985 (2d Cir. July 14, 2016); *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008); and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008). The

Brennan Center's views as *amicus curiae* in this case do not and will not purport to represent the position of NYU School of Law.

The Electronic Frontier Foundation ("EFF") is a San Francisco-based, donor-supported, non-profit civil liberties organization working to protect and promote free speech, privacy, and openness in the digital world. Founded in 1990, EFF now has roughly 23,000 dues-paying members throughout the United States. EFF represents the interests of technology users in both court cases and broader policy debates regarding the application of law in the digital age, and is a recognized leader in privacy and technology law. EFF has served as counsel or amicus in privacy cases including *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015), *Riley v. California*, 134 S. Ct. 2473 (2014), *United States v. Jones*, 132 S. Ct. 945 (2012), *Nat'l Aeronautics & Space Admin. v. Nelson*, 131 S. Ct. 746 (2011), and *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010).

Access Now is a non-profit organization that defends and extends the digital rights of users at risk around the world by combining innovative policy, global advocacy, and direct technical support to fight for open and secure communications for all. Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and universality, and wields an action-focused global community of users from more than 185 countries. Access Now advocates for

reform of government surveillance authorities in order to bring activities in line with global human rights standards. Access Now has participated as amicus in litigation including *In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No. ED 15–0451M (C.D. Cal. 2016), *Arizona v. Nat'l Telecomms. & Info. Admin.*, No. 3:16-cv-00274 (S.D. Tex. 2016), *Viacom Int'l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110 (S.D.N.Y. 2013), and *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

The Technology Freedom Institute ("TechFreedom") is a non-profit, non-partisan think tank dedicated to educating policymakers, the media, and the public about technology policy. Founded in 2010, TechFreedom advocates for policies that promote dynamism, entrepreneurship, and permissionless innovation in tech, and fights against abuses of civil liberties wherever they are found. Along those lines, TechFreedom is deeply concerned with certain domestic programs, including dragnet warrantless surveillance, which threaten to stifle the very creativity and innovation that drive the tech sector. TechFreedom regularly participates in administrative rulemakings and Congressional hearings, and has filed multiple amicus briefs to challenge perceived privacy abuses, including in *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014), and *In re LabMD, Inc.*, Docket No. 9357 (F.T.C. 2016).

NEW YORK STATE COURT OF APPEALS
CERTIFICATE OF COMPLIANCE

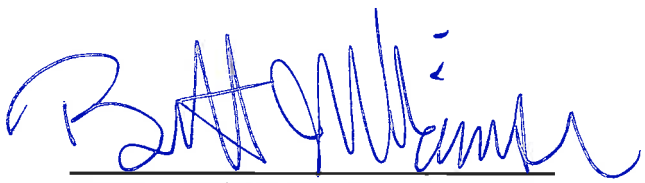
I hereby certify pursuant to 22 NYCRR PART 500.1(j) that the foregoing brief was prepared on a computer using Microsoft Word.

Type. A proportionally spaced typeface was used, as follows:

Name of typeface: Times New Roman
Point size: 14
Line spacing: Double

Word Count. The total number of words in this brief, inclusive of point headings and footnotes and exclusive of pages containing the table of contents, table of citations, proof of service, certificate of compliance, corporate disclosure statement, questions presented, statement of related cases, or any authorized addendum containing statutes, rules, regulations, etc., is 6,978 words.

Dated: December 30, 2016



Brett J. Williamson
O'MELVENY & MYERS LLP
7 Times Square
New York, NY 10036
(212) 326-2000

Counsel for Amici Curiae Brennan Center for Justice at NYU School of Law, Electronic Frontier Foundation, and TechFreedom