New York 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 AND ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF MOTION FOR LEAVE TO APPEAL

FAIZA PATEL
MICHAEL PRICE
BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW
161 Avenue of the Americas, 12th Floor
New York, New York 10013
Tel.: (646) 292-8335
Fax: (212) 463-7308

Counsel for Amicus Curiae Brennan Center for Justice at NYU School of Law

BRETT J. WILLIAMSON
(Pro Hac Vice Admission Pending)
DAVID K. LUKMIRE
NATE ASHER
O'MELVENY & MYERS LLP
Times Square Tower
7 Times Square
New York, New York 10036
Tel.: (212) 326-2000
Fax: (212) 326-2061

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

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Other Authorities

Constitutional Provisions

INTEREST OF AMICI CURIAE

The Brennan Center for Justice at NYU School of Law is a nonpartisan 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 *Matter of a Warrant (Microsoft Corp. v. United States)*, No. 14-2985-cv (2d Cir. 2015); *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 Electronic Frontier Foundation ("EFF") is a San Francisco-based, donor-supported, nonprofit 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).

SUMMARY OF ARGUMENT

This Court should grant leave for Facebook to appeal because the First Department's ruling threatens the constitutional rights of hundreds of Facebook users, ignores Facebook's role in copying and seizing the data, and eliminates Facebook's ability to protect its users from unlawful government intrusion. The ruling will open the door to future large-scale data seizures and deprive hundreds or thousands of New Yorkers of the opportunity to challenge potentially improper collection and retention of their private messages, photographs, videos, and other communications.

As the facts of this case demonstrate, the bulk warrant tactic endorsed by the First Department risks unconstitutionally overbroad data collection and virtually

ensures that large numbers of citizens who are never charged will have their private information retained by the government indefinitely. Here, although the Supreme Court endorsed 381 separate search warrants requiring Facebook to copy nearly all data relating to 381 of its users and disclose that data to law enforcement, the state eventually prosecuted only 62 of those 381 users. The remaining 319 users were never charged and thus never learned that their data had been seized and retained indefinitely. Facebook stepped in to fill this void and protect the constitutional rights of these 319 users who otherwise would have had no legal recourse of their own. But both the trial court and the First Department denied Facebook the ability to do so. This case presents the appropriate vehicle to resolve that pressing constitutional question.

Moreover, the ruling below rested in part on an incomplete Fourth Amendment analysis and a misapprehension of the privacy concerns associated with electronic data. Given the importance of the rights at issue in this case, the Court should grant leave to appeal to ensure that constitutional rights are not deprived due to incorrect or incomplete constitutional analyses. The Court should also grant leave because this issue is sure to arise again in trial courts and the Appellate Division, and without a ruling from this Court, the state's law will continue to be set by—and trial courts will be bound by—the Appellate Division. But this case involves rights so fundamental, and concerns so practical, that this

Court, and not the First Department, should establish New York law to protect this state's citizens from overbroad collection and retention of electronic data.

For these reasons, the Brennan Center and the Electronic Frontier Foundation urge the Court to hear this appeal.

ARGUMENT

I. Allowing the First Department's Decision to Stand Means That No One Can Ever Challenge Bulk Electronic Warrants.

Regardless of whether the order sanctioned by the Supreme Court is dubbed a "warrant" or "subpoena," Facebook must have a right to challenge it. Where there is a constitutional wrong, there must be a remedy. *See Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 163 (1803); *Bell v. Hood*, 327 U.S. 678, 684 (1946) ("[W]here federally protected rights have been invaded, it has been the rule from the beginning that courts will be alert to adjust their remedies so as to grant the necessary relief."). But here, the First Department's ruling leaves both individuals and third-party data companies without any redress, despite the lingering harm to personal privacy.

Under the decision below, only those individuals actually charged with a crime have a right to challenge the indefinite retention of vast amounts of private data. *In re 381 Search Warrants Directed to Facebook, Inc. v. New York Cnty. District Attorney's Office*, 2015 N.Y. Slip Op. 06201, at *7–8 (App. Div. 1st Dep't July 21, 2015). But as the Second Circuit recently recognized in *United States v.*

Ganias, there are serious constitutional concerns with allowing prosecutors to stockpile gigabytes of personal data not relevant to a charged crime for future law enforcement use. 755 F.3d 125 (2d Cir. 2014) (holding that the Fourth Amendment does not permit law enforcement to "indefinitely retain every file . . . for use in future criminal investigations," even if that data was initially seized with a valid warrant) *reh'g en banc granted*, 791 F.3d 290 (2d Cir. 2015). It is thus imperative for courts to prevent situations where personal data can be collected *wholesale* without anyone being able to challenge the government's actions.

Here, hundreds of people will never have the opportunity to address potentially improper collection and retention of their personal data if the First Department ruling is allowed to stand. Over 80% of the targeted users were never indicted. These New Yorkers will continue to suffer immediate violations of their constitutional rights, and millions of others will remain at risk of similar intrusions into their private lives. It is therefore entirely appropriate for this Court to grant leave and provide a remedy. Both the federal and New York constitutions demand that this case be heard to determine the whether it is appropriate for the government to issue bulk warrants that cannot possibly be challenged by those whose data is being collected or those who the government conscripts to do the collecting. *See People v. Scott*, 79 N.Y.2d 474, 485 (1992) (noting that N.Y.

Const. art. 1, § 12, unlike the Fourth Amendment, additionally protects against "interception of . . . communications").

II. This Court Should Review the First Department's Erroneous Conclusion That Copying Data Does Not Implicate the Fourth Amendment.

This Court should grant leave to address the First Department's error in reasoning that a Fourth Amendment event does not occur until the state actually searches the data obtained from Facebook. This position ignores the fact that Facebook was conscripted to seize user data and opens the door to the over-collection and retention of personal data.

The Appellate Division based its assertion solely on a law review article that has since been renounced by its author. *Compare 381 Search Warrants*, 2015 N.Y. Slip Op. 06201, at *4 (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 the 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."). Amici believe that the First Department erred in relying on this outdated argument and urge this Court to take account of the fact that Facebook was compelled to seize its users' data and provide a copy to law enforcement. Facebook's involvement was not merely a byproduct of the nature of

electronic searches, *contra 381 Search Warrants*, 2015 N.Y. Slip Op. 06201, at *5; it was a government-directed seizure.

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. *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*, 119 Yale L.J. at 703, 711. The First Department largely ignored seizure analysis, ignored Professor Kerr's 2010 article, and ignored recent case law. *See, e.g.*, *Ganias*, 755 F.3d at 135–36 (explaining that data copied from hard drives is seized at the time of copying); *United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (referring to the copying of electronic data as a seizure throughout the opinion); *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002) (describing information retrieved by Yahoo! technicians from two e-mail accounts as a "seizure"); *In re A Warrant for All Content and 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 equates to 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. Taylor*, 764 F. Supp. 2d 230, 237 (D. Me. 2011) (obtaining copies of emails from internet service provider "for subsequent searching" is a seizure); *United States v. Bowen*, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) (copying of entire email account described as a seizure).

The First Department erred by failing to recognize that Facebook was directly engaged in a Fourth Amendment event—a seizure—when it copied its users' data. That error led the First Department to downplay Facebook's involvement in the searches, ignoring the unique implications of mandating electronic searches by third parties. *See ACLU v. Clapper*, 785 F.3d 787, 814–15 (2d Cir. 2015) (program requiring carriers to turn over telephone metadata exceeded government's authority under the Foreign Intelligence Surveillance Act). This Court should not allow that error to stand.

Granting leave to examine this issue would ensure that the First Department's incomplete Fourth Amendment analysis is not the basis for deciding the important question of when electronic searches and seizures occur, and whether Facebook's involvement in a Fourth Amendment event should give rise to a right to challenge the warrants. Moreover, given the prevalence of electronic searches, this Court should be the primary source of precedent in New York regarding

Fourth Amendment concerns arising from a private party's government-mandated electronic copying. Reviewing this decision would also allow the Court to align New York state law with the emerging consensus in New York federal courts. *See Ganias*, 755 F.3d at 135–36; *United States v. Lustyik*, 57 F. Supp. 3d 213, 232 n.13 (S.D.N.Y. 2014) ("To be sure, a 'seizure' also occurred when [the] email service provider copied the contents of his email account and provided that copy to the government."); *Bowen*, 689 F. Supp. at 684. New York law should not ignore that a seizure—a Fourth Amendment event—occurs whenever data is copied.

III. The First Department's Decision Relies on an Erroneous Understanding of the Fourth Amendment's Application in the Digital World.

Hearing this appeal is especially crucial because the First Department's suggestion that "the Fourth Amendment's protections are potentially far weaker" when "applied to information stored online," *381 Search Warrants*, 2015 N.Y. Slip Op. 06201, at *6, has dangerous consequences for privacy. This was not an accident or aside, as evidenced by the court's reasoning that computer records, because they are "stored in a technologically innovative form," raise "the question of whether they are sufficiently like other records to engender the 'reasonable expectation of privacy' required for Fourth Amendment protection." *Id.*

As the Supreme Court recently recognized, this approach is both inconsistent with the Fourth Amendment and defies common sense. In 2015, virtually all private communications are through digital intermediaries, and with the advent of

modern "cloud" computing, e-mail and social networking accounts contain vast amounts of personal information aside from the content of messages. *See Riley*, 134 S. Ct. at 2491. Thus, in deciding that a modern smartphone could not be searched incident to an arrest without a separate warrant, the Supreme Court observed that the Fourth Amendment may demand *greater*—not less—scrutiny of law enforcement activity in the digital age, since smartphones (just like the Facebook accounts at issue here) "place vast quantities of personal information literally in the hands of individuals," and the search of which "bears little resemblance to a physical search." *Id.* *See also United States v. Otero*, 563 F.3d 1127, 1132 (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 . . . ."). The First Department's view also conflates information such as public posts on Facebook with information that would not be publicly available to other Facebook users. The rise of social media has generated more data in the hands of third parties than ever before, and this Court should grant leave to appeal to ensure that the privacy of this data is not eroded due to the First Department's erroneous assumption about the implications of using a website such as Facebook.

IV. The First Department's Errors Should Be Corrected Now.

The dangerous precedent set in the First Department will remain the law of this State unless this Court intervenes now. As this Court knows, trial courts across New York must follow the First Department's ruling unless and until this Court or another Department overrules it. *People v. Brisotti*, 652 N.Y.S.2d 206, 207 (App. Div. 1st Dep't 1996) ("*[S]tare decisis* requires trial courts [and the Appellate Term] in this department to follow precedents set by the Appellate Division of another department until the Court of Appeals or [the Appellate Division of this department] pronounces a contrary rule."). But for at least two reasons, no other Department is likely to announce a contrary ruling, making it incumbent on this Court to hear this case on the merits.

First, "the jurisdiction of the First Department of the Appellate Division over New York City's financial district probably makes it the country's most important state appellate court in the commercial field." Jill Botler, et al., *The Appellate Division of the Supreme Court of New York: An Empirical Study of Its Powers and Functions as an Intermediate State Court*. 47 Fordham L. Rev. 929, 929 (1979). What was then (and still is) true for financial institutions applies equally to today's technology companies storing vast amounts of personal data. As of 2014, lower Manhattan was home to 600 technology-related companies. Office of the State Comptroller, *New York City's Growing High-Tech Industry* at 3 (Apr. 2014),

available at https://www.osc.state.ny.us/osdc/rpt2-2015.pdf (discussing the "Silicon Alley" cluster of technology companies in Midtown South). Google and Facebook, both of which have significant operations in Manhattan, alone have hundreds of millions of users of their e-mail and social networking services.

That the private data of millions is subject to the First Department's jurisdiction not only underscores the importance of hearing this case, but also means that the issues presented by this appeal will likely recur in the First Department, making it critical for this Court to correct the errors below now. *See E. Meadow Cmty. Concerts Ass'n v. Bd. of Ed. of Union Free Sch. Dist. No. 3*, 18 N.Y.2d 129, 135, 219 N.E.2d 172, 175 (1966) ("It is settled doctrine that an appeal will, nevertheless, be entertained where, as here, the controversy is of a character which is likely to recur not only with respect to the parties before the court but with respect to others as well.").

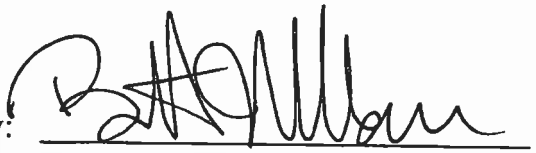
CONCLUSION

This Court has long been mindful of protecting New York citizens' Fourth Amendment freedoms. The issue presented here—whether officials of this State may collect with impunity and then indefinitely retain vast amounts of New Yorkers' intimate personal information—is of great importance to the public. The First Department's decision, if allowed to stand, will enable future violations

of constitutional privacy rights. Brennan Center and EFF therefore urge this Court to grant Appellant Facebook's motion for leave to appeal.

Dated: New York, New York
October 23, 2015

Respectfully submitted,

By: 

Brett J. Williamson
(Pro Hac Vice Admission Pending)
David K. Lukmire
Nate Asher
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 and Electronic Frontier Foundation

By: 

Faiza Patel
Michael Price
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW
161 6th Ave., 12th Floor
New York, New York 10012
(646) 292-8335

Counsel for Amicus Curiae Brennan Center for Justice at NYU School of Law

TO: BENJAMIN E. ROSENBERG
General Counsel and Assistant District Attorney
New York County District Attorney's Office
One Hogan Place
New York, New York 10013
Attorney for Respondent

GIBSON DUNN & CRUTCHER LLP
Orin Snyder
Alexander H. Southwell
Thomas H. Dupree, Jr.
Gabriel K. Gillett
200 Park Avenue, 47th Floor
New York, New York 10166
Tel.: (212) 351-4000
Fax: (212) 351-4035
Attorneys for Appellant