SUPREME COURT OF NEW JERSEY
DOCKET NO. 087054

FACEBOOK, INC., Plaintiff-Respondent, v. STATE OF NEW JERSEY, Defendant-Movant. _____ IN THE MATTER OF THE APPLICATION OF THE STATE OF NEW JERSEY FOR A COMMUNICATIONS DATA WARRANT AUTHORIZING THE OBTAINING OF THE CONTENTS OF RECORDS FROM FACEBOOK, INC.	APPELLATE DIVISION NOS. A-000119-21, A-003350-20 Sat Below: Hon. Jack M. Sabatino, J.A.D. Hon. Garry S. Rothstadt, J.A.D. Hon. Jessica R. Mayer, J.A.D. Criminal Actions

PROPOSED BRIEF OF *AMICI CURIAE* CENTER FOR DEMOCRACY & TECHNOLOGY, ELECTRONIC PRIVACY INFORMATION CENTER, AND ELECTRONIC FRONTIER FOUNDATION

Geoffrey S. Brounell
(NJ Bar No. 012142008)
DAVIS WRIGHT TREMAINE LLP
1251 Ave. of the Americas, 21st Floor
New York, New York 10020
Tel: (212) 489-8230
GeoffreyBrounell@dwt.com

David M. Gossett
(*pro hac application pending*)
DAVIS WRIGHT TREMAINE LLP
1301 K Street NW, Suite 500 East
Washington, DC 20005
Tel: (202) 973-4216
DavidGossett@dwt.com

MaryAnn T. Almeida
(*pro hac application pending*)
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue, Suite 3300
Seattle, WA 98104
Tel: (206) 622-3150
MaryAnnAlmeida@dwt.com

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Federal Cases

State Cases

Constitutional Provisions

Federal Statutes

State Statutes

Other Authorities

INTERESTS OF THE *AMICI*

The *amici curiae* are organizations that work at the intersection of technology and civil liberties. Staffed with experts on technology, policy, and the law, each advocates for the protection of civil liberties and individual rights in the modern era. The organizations are deeply concerned by the implications of the Appellate Division's opinion for the law governing electronic surveillance. Under the Wiretap Act and its New Jersey analogue, the State may obtain precisely the material it seeks in this case; it just must first meet the heightened standards required by those acts, rather than the lower requirements for a traditional warrant. *Amici* appear before this Court to advocate that this Court reinforce existing Fourth Amendment law and hold that the State must satisfy those heightened standards before being able to require tech companies to provide ongoing access, over the course of 10 or more days, to their customers' private communications.

The Center for Democracy & Technology is a non-partisan, non-profit organization dedicated to promoting individual rights and democratic values amid changes in technology. It champions laws, policies, and technical designs that foster positive uses of technology while guarding against unwarranted surveillance and other invasions of personal privacy. It has long been an

advocate to courts and policymakers regarding the intersection of technology and individual liberty.

The Electronic Privacy Information Center (EPIC) is a non-profit research center in Washington, DC, whose mission is to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC believes privacy is a fundamental right. While advances in technology have potential to enhance our lives, the government and courts must guard against abuses, including invasive surveillance.

The Electronic Frontier Foundation (EFF) is a member-supported, nonprofit civil liberties organization that works to protect free speech and privacy in the digital world. EFF regularly pursues litigation and serves as *amicus* in cases addressing Fourth Amendment protection for data and communications stored by third-party communications providers.

INTRODUCTION AND SUMMARY OF ARGUMENT

The Fourth Amendment has long been understood to protect private communications, regardless of the method by which those communications take place. Technological advances have fostered new ways to communicate, but the liberty and privacy rights Americans enjoy do not change with those changes in technology. And while advances in law-enforcement technology have similarly

enabled new forms of surveillance, the law still guards against erosion of bedrock Fourth Amendment protections.

In these two cases, now consolidated, Facebook challenged the use of Communication Data Warrants to require it repeatedly to provide the contents of users' communications to law enforcement—and indeed, to do so on *2,880 distinct occasions*, or once every 15 minutes for 30 days. Facebook argued that this surveillance is as invasive as a traditional wiretap because it required the company repeatedly to access and provide to the government *future* communications and therefore required the State to meet heightened standards before a warrant could issue. But the court of appeals authorized law enforcement to surveil communications through warrants (albeit limiting the surveillance to a period of 10 days rather than 30). The Appellate Division's decision thus undermines two core principles in Fourth Amendment jurisprudence: that a single warrant, based on probable cause, supports only a single incident of search, and that law enforcement requests to surveil unfiltered, future communications—rather than communications that have already occurred—are subject to heightened standards beyond what the law requires for a traditional search warrant. Meanwhile, the State has argued in its cross appeal that the 10-day limitation is too restrictive and it should be allowed to continue its "prospective observation" of account data for a full 30 days on a single

warrant. *See* Suppl. Br. & App. on Behalf of the State (Dec. 13, 2022) (State Suppl. Br.).

These developments are alarming. The Appellate Division's erosion of longstanding protections is unprecedented in this nation, and it harms not only targets of investigation but also anyone with whom those targets communicate. The precedent the Appellate Division's decision sets is particularly troubling in light of the highly private communications that may be swept into the surveillance it authorizes. This Court should reverse the Appellate Division's determination and hold that any repeated surveillance of prospective communication—regardless of the method by which that communication occurs—must comply with the federal Wiretap Act, 18 U.S.C. §§ 2510-2522, and the state Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 2A:156A-1 to -26.

STATEMENT OF FACTS AND PROCEDURAL HISTORY

Amici rely on the statements of facts and procedural history provided by the parties.

ARGUMENT

The Appellate Division's decision violates longstanding Fourth Amendment case law and subverts the more stringent, privacy-protective requirements of the federal and New Jersey wiretap acts. In doing so, the

decision has exposed to invasive surveillance not only the targets of investigations, but also anyone with whom those targets communicate. The online communications at issue here, stored as data by platform providers, are increasingly common and no less private than phone conversations merely because they occur online. Indeed, many individuals today use Internet-based apps and services—such as Zoom, Microsoft Teams, WhatsApp, and Facebook Messenger—for voice or video communications in place of traditional phone calls. These services sometimes preserve communications for subscribers' convenience and later use, introducing the risk that the government's position would steadily erode wiretap protections for *all* remote communications as technology advances. And despite the government's emphasis on Facebook "posts" covered by the communications data warrants, *see, e.g.*, State Suppl. Br. 45, there is no basis in the Appellate Division's decision or the government's position to distinguish between public posts and private communications. The Court should reverse and confirm that online communications are subject to the same protections as phone calls under the Fourth Amendment.

I. Under The Fourth Amendment, Wiretaps Are Subject To Heightened Protections.

"Privacy of communication is an important interest" under the Fourth Amendment. *Bartnicki v. Vopper*, 532 U.S. 514, 532 (2001) (internal quotation marks omitted). At its core, the Appellate Division's decision expands law

enforcement's ability to surveil private communications that occur electronically, simply because of the way they take place. But while the "Framers of the [Constitution] surely did not foresee the advances in science that" enable modern methods to intercept private communications, *id.* at 518, the law recognizes the significance of a person's privacy interests in their communications regardless of the technology used. Indeed, "[a]s technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes," courts are obligated to "assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Carpenter v. United States*, 138 S. Ct. 2206, 2214 (2018).

The Appellate Division's decision here violates two principles from long-standing Fourth Amendment precedent: *first*, that a single showing of probable cause supports only one search, not continuing surveillance; and *second*, that court orders authorizing ongoing prospective surveillance must be limited and specific—beyond the specificity required for a traditional search warrant—to prevent law enforcement overreach.

A. Each Incident of Search Must Be Supported by a Separate Showing of Probable Cause.

The first of these two principles—the "one warrant, one search" rule—holds that "a single search warrant authorizes but a single search and may be executed only once," with "no additional search … undertaken on the same

warrant." 79 C.J.S. Searches § 260; *see also* 2 Wayne R. LaFave, Search & Seizure, Intensity and duration, § 4.10(d) (6th ed.) (a "second search could not be justified as an additional search under authority of the warrant."). This rule follows directly from *Berger v. New York*, where the Supreme Court held unconstitutional a New York law that permitted a "broadside" "authorization of eavesdropping for a two-month period" because it was "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause," which the Fourth Amendment did not allow. 388 U.S. 41, 58-59 (1967).

The one warrant, one search rule applies to traditional searches and other forms of surveillance alike. *See, e.g.*, *State v. Parsons*, 83 N.J. Super. 430, 447 (App. Div. 1964) (photographs taken during second search of physical premises inadmissible); *In re Ord. Authorizing Prospective & Continuous Release of Cell Site Location Recs.*, 31 F. Supp. 3d 889, 894 (S.D. Tex. 2014) ("one-time search" rule covers cell location data). And it has been embraced universally in federal and state courts, as Facebook's brief and the American Civil Liberties Union's *amicus* brief describe.

The Appellate Division's opinion authorizes repeated collections of data pursuant to a single warrant. It allows law enforcement to search a user's account as frequently as every 15 minutes for up to 10 days. That enables *960 searches* based on a single warrant—and based on the single showing of probable cause

to support that warrant. This violates the one warrant, one search principle 959 times over.[1] Worse still, the same logic would justify repeated searches at even smaller intervals, so long as the communications were stored. Repeated searches at a minimal interval—every 15 *milliseconds*, for instance—would negate any distinction between a wiretap and a warrant for electronic communications data.

B. Prospective Surveillance Requires Heightened Scrutiny.

Case law also establishes that prospective, ongoing surveillance is more sensitive than a one-time search because it involves a broader invasion of the target's privacy. The scope of invasion for traditional investigative tools is limited by what those methods seek. For instance, "[a]n administrative subpoena or a civil discovery request is typically satisfied by a one time production of documents; a search warrant for records authorizes one-time access, not repeated searches of the same premises, day after day, week after week, month after month." *In re Ord. Authorizing Prospective*, 31 F. Supp. 3d at 894-95. By contrast, authorization for future surveillance lacks a natural limit. The State's position that "there [i]s no constitutional defect justifying the categorical ten-day cap" underscores this point: in the State's view, prospective surveillance carries no particular time restriction. *See* State Suppl. Br. 57-66. Ongoing,

[1] The State argues in its cross appeal that the Appellate Division erred in limiting the warrants to 10 days; under the State's proposed 30-day rule, one warrant would authorize *2,880* distinct searches.

prospective surveillance also lacks any check to prevent intrusions on private information unrelated to the investigation, which may be highly sensitive to the person communicating.

That is why it is firmly established that prospective, ongoing surveillance requires more safeguards beyond a plain showing of probable cause—requirements the Appellate Division's rule would eviscerate. *See, e.g.*, *Berger*, 388 U.S. at 59 (New York's law permitting repeated, prospective surveillance "g[ave] the officer a roving commission to 'seize' any and all conversations," which "leaves too much to the discretion of the officer executing the order."); *Katz v. United States*, 389 U.S. 347, 356-58 (1967) ("advance authorization by a magistrate" was necessary for a lawful search using electronic surveillance, even though "the agents in th[at] case acted with restraint").

C. Anticipatory Warrant Case Law Does Not Change These Requirements.

In an attempt to defend the constitutionality of these Communications Data Warrants, the State analogizes them to anticipatory warrants. *See* State Suppl. Br. 33-37. The analogy does not support the government's position. In *United States v. Grubbs*, the U.S. Supreme Court upheld the constitutionality of warrants for future searches on applications that "require the magistrate to determine (1) that it is *now probable* that (2) contraband, evidence of a crime, or a fugitive *will be* on the described premises (3) when the warrant is executed."

547 U.S. 90, 96 (2006). With these showings, "[a]nticipatory warrants are, therefore, no different in principle from ordinary warrants." *Id.*

But nothing about *Grubbs* eliminates the fact that a warrant—whether immediately executable or executable at a specific future time—authorizes only one search, nor that the standards to authorize wiretapping and equivalent forms of surveillance are higher than for a traditional warrant, again whether present or anticipatory. As the Supreme Court explained in *Grubbs*, anticipatory warrants can arise "in the context of electronic surveillance," including wiretaps. *Id.* at 95. "When police request approval to tap a telephone line, they do so based on the probability that, during the course of the surveillance, the subject *will* use the phone to engage in crime-related conversations." *Id.* The requirement that law enforcement establish that probability is written into the Wiretap Act, which the Court cited in *Grubbs* for the proposition that such a showing is required. *See id.* at 96 (citing 18 U.S.C. § 2518(3)(b)). In other words, anticipatory warrants in the context of electronic surveillance must meet all of the requirements of the Wiretap Act, if they are to be constitutional.

II. The Federal Wiretap Act and Its New Jersey Analogue Permit Law Enforcement Surveillance Akin To the Warrants at Issue Here—But Only with Heightened Safeguards.

The federal and state wiretap statutes provide the government with adequate law-enforcement tools. Congress enacted the Wiretap Act to establish

a mechanism for law enforcement to obtain evidence through electronic surveillance within the bounds of the Fourth Amendment. "Congress undertook to draft comprehensive legislation both authorizing the use of evidence obtained by electronic surveillance on specified conditions, and prohibiting its use otherwise," "[l]argely in response to" *Berger* and *Katz*. *Bartnicki*, 532 U.S. at 523. The federal Wiretap Act's "restrictions are intended to protect [the important] interest [in private communications,] thereby encouraging the uninhibited exchange of ideas and information among private parties." *Id.* at 532 (internal quotation marks omitted).

New Jersey modeled its Wiretapping and Electronic Surveillance Control Act on the federal Wiretap Act, permitting a judge to authorize interceptions of communications after making specific findings supported by probable cause that such surveillance is necessary to obtain particular communications about a specific, enumerated crime. *State v. Ates*, 217 N.J. 253, 266-67, (2014). Under this Court's precedent, "The [New Jersey] Wiretap Act must be strictly construed to safeguard an individual's right to privacy." *Id.* at 268.

But although the State thus can obtain the types of information it sought in these two cases, it must meet a higher burden to do so: the requirements for authorization of continued surveillance under the Wiretap Act and New Jersey's analogue are far more protective than the probable-cause showing for a warrant.

First, the Wiretap Act requires law enforcement to avoid unnecessary intrusions where less invasive investigative means are feasible. An application must state, and a judge must determine based on the facts, that "other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(1)(c); *id.* § 2518(3)(c); *see also* N.J.S.A. 2A:156A-9(c)(6) (requiring wiretap application to include "[a] particular statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ").

Far from being a nuisance, as the State suggests, *see, e.g.*, State Suppl. Br. 34-35, these protections ensure that a highly invasive wiretap may be authorized only where less invasive mechanisms will not work or have already failed. *See, e.g.*, *United States v. Lilla*, 699 F.2d 99, 104 (2d Cir. 1983) (wiretap failed necessity requirement where "affidavit fail[ed] to specify the facts upon which [the investigator] based th[e] conclusion [that other investigative means would not work]; there is no indication why simple surveillance of [the target's] place of work or his home would not have been useful" or that the investigation "presented problems different from any other small-time narcotics case");

United States v. Mondragon, 52 F.3d 291, 294 (10th Cir. 1995) (suppressing evidence where affidavit failed to satisfy necessity requirement).

Second, wiretaps are subject to stringent minimization requirements. The Wiretap Act requires that law enforcement "minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective." 18 U.S.C. § 2518(5); *see also* N.J.S.A. 2A:156A-12(f) ("Every order entered under this section shall require that such interception begin and terminate as soon as practicable and be conducted in such a manner as to minimize or eliminate the interception of such communications not otherwise subject to interception under this act by making reasonable efforts, whenever possible, to reduce the hours of interception authorized by said order."). "[M]inimization is to be conducted intrinsically on a call-by-call basis." *State v. Catania*, 85 N.J. 418, 432 (1981). Minimizing surveillance of calls not pertinent to an investigation avoids intrusion into other conversations, perhaps as sensitive as talking with a doctor about a medical condition, a romantic partner about intimate activities, or a priest about personal life choices. "In addition to being required by statute, minimization is thus necessary to safeguard an important constitutional value: the privacy right of those who use the telephone to be secure from indiscriminate wiretapping that intercepts all conversations, no matter how non-relevant or

personal, in violation of the Fourth Amendment proscription against unreasonable searches and seizures." *Id.* at 429.

Wiretaps also are authorized only for specific communications, and a wiretap order must "specify … a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates." 28 U.S.C. § 2518(4)(c). *See also* N.J.S.A. 2A:156A-9(c)(2)-(3) (application must state "details as to the particular offense that has been, is being, or is about to be committed; … [t]he particular type of communication to be intercepted; and a showing that there is probable cause to believe that such communication will be communicated" over the subject facilities).

These minimization requirements are equally applicable to the types of online communications that the State seeks to obtain by the two warrants at issue here. Just as law enforcement might be required to determine at the outset whether a telephone call is relevant to the subject of a wiretap, so too should it be required to determine whether a Facebook Messenger exchange—be it audio, video, or in writing—is relevant to the subject of the investigation. By contrast, warrants sweep in *all* nature of communications when they surveil online communications—not just the specific messages targeted by the orders. This

means that innocent communications will necessarily be exposed to law enforcement scrutiny.

Third, wiretaps are permissible only for limited durations—typically only until the intended communications have been obtained. *See* 18 U.S.C. § 2518(1)(d) (application under the Wiretap Act must state "a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter," if the interception will be authorized beyond "when the described type of communication has been first obtained"); N.J.S.A 2A:156A-9 (c)(5) (authorization terminates "when the described type of communication has been first obtained" unless authorized for a longer duration). And any application for an extension must state what results have been obtained to date, as well as the details of all previous applications. 18 U.S.C. § 2518(1)(e)-(f). The Wiretap Act also allows the authorizing judge to require regular reports by law enforcement to the judge, to "show[] what progress has been made toward achievement of the authorized objective and the need for continued interception." *Id.* § 2518(6). Judicial scrutiny of further interception of future communications prevents law-enforcement mission creep. Surveillance under a warrant—including the communications data warrants at issue here—has no corresponding check.

Fourth, the New Jersey statute permits wiretapping only for certain enumerated crimes. *See* N.J.S.A. 2A:156A-8 (listing crimes for which law enforcement may seek a wiretap to investigate). This prevents the use of wiretap surveillance where the state legislature has concluded that the public safety interest in an investigation does not outweigh the invasion of privacy, such as for low-level offenses. And to the extent the Attorney General believes that wiretaps should be authorized for additional crimes, *see* State Suppl. Br. 15, the appropriate route is to lobby the legislature to change that limitation, not to ignore it.

III. The Court of Appeals' Decision Has Profoundly Negative Implications for the Personal Liberty of Surveillance Targets and Those with Whom They Communicate.

The warrants authorized by the Appellate Division lack the heightened protections the federal and New Jersey wiretap acts impose. Those warrants authorize the collection of stored communications at repeated intervals as often as every 15 minutes, for up to 10 days following the issuance of the warrant—enabling law enforcement to continue surveilling all of the target's communications, even after having obtained the type of communication described in the warrant. This collection of prospective communication—through 960 separate searches—unlawfully circumvents the safeguards of the

wiretapping statutes, denying individuals the protections Congress and New Jersey's legislature crafted to be consistent with the Fourth Amendment.

The expansive and long-term surveillance authorized by the warrants in these cases is especially problematic because it is focused on electronic communication. The Appellate Division distinguished the electronic communications sought by the warrants because "the data sought was from information that would be stored by Facebook as compared to simultaneous transmission of information [subject to] interception." Op. at 3. This is wrong for multiple reasons.

First, as a technical matter, the electronic communications at issue are both stored *and* instantly transmitted simultaneously—so the Appellate Division's articulated distinction is invalid. Messaging apps like Facebook, Snap, and WhatsApp offer virtually instantaneous transmission of full messages. To accomplish this transmission, messages "are first broken down into smaller pieces of data—'packets'—and then sent along a series of intermediate routers until the packets reach their destination." Richard T. Wang, *Cookies and Wires: Can Facebook Lure Users into Divulging Information Under the Wiretap Act's Party Exception?*, 106 Cornell L. Rev. 1937, 1945 (2022). This form of transmission is common to other methods of electronic communication. Messaging systems like iMessage, for instance, rely on the same technology,

transmitting messages via packets sent over the internet rather than SMS like traditional text messages. *See* Shira Ovide, *Americans Can't Quit SMS*, N.Y. Times (Feb. 2, 2022), https://tinyurl.com/4v8n8ymd. Email uses this method, too. Wang, *Cookies and Wires*, 106 Cornell L. Rev. at 1945-46 ("Upon transfer, the routers delete the copies shortly thereafter. Once all of the packets arrive at their destination—the recipient's mail server—they are reassembled to form the original email message …. Thus, in contrast to oral and wire communications, emails are constantly 'in transit' and 'in storage' simultaneously."). Although each of these methods of communication result in stored data, they are also instantly transmitted. The Appellate Division's distinction based on the "stored" nature of these communications overlooks their instantaneous nature. Likewise, the government's emphasis on the "ostensibly evanescent" nature of oral communications, *see* State Suppl. Br. 1, 3, 30, 53, fails to account for the sometimes-fleeting character of electronic communications: users may ordinarily delete messages, and some applications do so automatically. Any distinction on this basis fails.

Second, the underlying privacy interests are no less significant because the communication data is also stored. Electronic means have become the norm for communication of all kinds. Long gone are the days when phones were for making calls: today, the average American spends more than four hours a day

using apps on their smart phone. Sarah Perez, *Consumers now average 4.2 hours per day in apps, up 30% from 2019*, TechCrunch (Apr. 8, 2021), https://tinyurl.com/mr9zy3yw; *see also* Ki Mae Heussner, *Phone Fatigue: Voice Calls on the Decline*, ABC News, (Aug. 9, 2010), https://tinyurl.com/3w69wsup. And communication applications provide new ways to have conversations that previously occurred only in person or orally over the phone. Now, applications permit communication electronically on smartphones, laptops, tablets, and even some gaming consoles or internet-connected exercise equipment.

The proliferation of internet-based communication is growing. Younger Americans rely more on online communication than do older generations. Only 22 percent of Millennials (age 25-40) and 23 percent of Gen Z (age 9-24) consider phone calls their "most used" method of communication in their personal life, compared to 33 percent of Gen X (age 41-56) and 48 percent of baby boomers (age 57-75). *See Across Generations, Email Remains a Critical Tool for Daily Life*, Medium (Mar. 30, 2022), https://tinyurl.com/y4pfy4zv. Instead, younger generations rely on text messages, messaging apps, and social media. *Id.* And email remains a dominant mode of personal communication among all age groups. *Id.* The fact that these communications take place over

the internet, rather than phone lines, cannot weaken the privacy protections the Fourth Amendment and the wiretapping laws guarantee.

Third, the Appellate Division's baseless distinction is even more dangerous when considering the kind of communications that can be swept within the broad scope of warrants such as these—that is, communication of all kinds, about all subjects personal and private. The surveillance contemplated by the warrants, like a "traditional wiretap or electronic eavesdropping device[,] constitutes a dragnet, sweeping in all conversations within its scope—without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations." *Berger*, 388 U.S. at 65. And "[e]lectronic surveillance monitors continuously, increasing the likelihood that people other than the target of the surveillance will have their private information disclosed. Even hardened criminals talk to their mothers and lovers, and these conversations are recorded along with their criminal plots." Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 Ala. L. Rev. 9, 18 (2004). The erosion of protections for electronic communication thus harms not only the target of surveillance, but also anyone with whom they communicate—their family, friends, and others not under investigation.

Minimizing state surveillance and data collection is essential to protect individual autonomy. Data minimization practices used by domestic violence hotline and shelter programs, for example, could be undermined by additional law enforcement access to those communications when they take place online. *See* Elec. Priv. Info. Ctr., *In the Matter of Lifeline and Link Up Reform and Modernization; Affordable Connectivity Program; Supporting Survivors of Domestic and Sexual Violence* (FCC, WC Docket No. 11-42 *et al.*) (Aug. 2022), https://tinyurl.com/mtvuy872. Such programs sometimes implement systems to mask a survivor's information, blocking the texter's phone number when receiving texts, for instance. *Id.* But these efforts do not obscure all personal information in all circumstances, and misuse of that information by law enforcement is an "uncomfortable reality" where, for example, an abuser has connections within police departments or is an officer. *Id.* Retaining strong protections to limit and control law-enforcement access to private communications is essential.

Similarly, expanded law enforcement surveillance will risk the sanctity of personal communications about private decisions regarding medical care. The proliferation of state laws criminalizing reproductive care since the United States Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*, 142 S. Ct. 2228 (2022), means law enforcement has reason to

surveil people planning to seek or provide abortion services—even in states where abortion rights are protected if the individuals seeking care live elsewhere but communicate with people in that state or plan to travel there. *Cf.* N.J.S.A. 10:7-1(h) ("[I]t shall be the policy of this State to[] explicitly guarantee, to every individual, the fundamental right to reproductive autonomy, which includes the right to contraception, the right to terminate a pregnancy, and the right to carry a pregnancy to term."). "[P]rosecutors in anti-abortion states will apply for warrants and court orders—as well as issue subpoenas—to obtain communications data of people and providers of reproductive health services[,]" obtaining a "vast" "range of private information" that "includes the most personal details about their medical activities, family plans, and romantic relationships." Jake Laperruque *et al.*, *Following the Overturning of Roe v Wade, Action is Needed to Protect Health Data*, Ctr. for Democracy & Tech., (June 24, 2022), https://tinyurl.com/4556f2nk. This will have an "outsized impact on communities already disproportionately impacted by policing, including people of color, LGBTQ people, and disabled people." *Id.*

Likewise, state laws prohibiting transgender youth from obtaining gender-affirming health care and exposing parents whose children receive that care to child-abuse investigations may lead law enforcement to investigate parents who travel with their children to other states to receive this care and seek

evidence from the places where it occurred. *See* Adam Schwartz, *Trans Youths Need Data Sanctuary*, Elec. Frontier Found., (Aug. 26, 2022), https://tinyurl.com/283e8sd3.

Although investigations of these particular issues may well be unlikely in New Jersey, this Court's decision here will nonetheless set the precedent for other states' approaches, too. And without special protections for prospective, ongoing communications regarding these and other sensitive topics—regardless of whether they occur over the phone or electronic means—the State will easily be able to intrude on these protected communications. The Appellate Division's decision diminishes the guardrails set up by the Wiretap Act and the Wiretapping and Electronic Surveillance Control Act in the context of online communications because they are "stored" as a technical matter, despite their instantaneous nature and the personal information they contain. These communications merit no less protection than traditional phone calls. Those statutes were enacted following *Berger*'s holding that any "series of intrusions" requires more than an ordinary warrant, but that is precisely what the Appellate Division authorized here.

CONCLUSION

The Court should reverse the Appellate Division's holding and require that any surveillance of prospective communications comply with the requirements of the state and federal wiretap acts.

Respectfully submitted,

/s/ Geoffrey S. Brounell

Geoffrey S. Brounell
(NJ Bar No. 012142008)
DAVIS WRIGHT TREMAINE LLP
1251 Ave. of the Americas, 21st Floor
New York, New York 10020
Tel: (212) 489-8230
GeoffreyBrounell@dwt.com

David M. Gossett
(*pro hac application pending*)
DAVIS WRIGHT TREMAINE LLP
1301 K Street NW, Suite 500 East
Washington, DC 20005
Tel: (202) 973-4216
DavidGossett@dwt.com

MaryAnn T. Almeida
(*pro hac application pending*)
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue, Suite 3300
Seattle, WA 98104
Tel: (206) 622-3150
MaryAnnAlmeida@dwt.com

Dated: January 9, 2023

SUPREME COURT OF NEW JERSEY
DOCKET NO. 087054

FACEBOOK, INC., Plaintiff-Respondent, v. STATE OF NEW JERSEY, Defendant-Movant. _____ IN THE MATTER OF THE APPLICATION OF THE STATE OF NEW JERSEY FOR A COMMUNICATIONS DATA WARRANT AUTHORIZING THE OBTAINING OF THE CONTENTS OF RECORDS FROM FACEBOOK, INC.	APPELLATE DIVISION NOS. A-000119-21, A-003350-20 Sat Below: Hon. Jack M. Sabatino, J.A.D. Hon. Garry S. Rothstadt, J.A.D. Hon. Jessica R. Mayer, J.A.D. Criminal Actions

CERTIFICATE OF SERVICE

Geoffrey S. Brounell
(NJ Bar No. 012142008)
DAVIS WRIGHT TREMAINE LLP
1251 Ave. of the Americas, 21st Floor
New York, New York 10020
Tel: (212) 489-8230
GeoffreyBrounell@dwt.com

David M. Gossett
(*pro hac application pending*)
DAVIS WRIGHT TREMAINE LLP
1301 K Street NW, Suite 500 East
Washington, DC 20005
Tel: (202) 973-4216
DavidGossett@dwt.com

MaryAnn T. Almeida
(*pro hac application pending*)
DAVIS WRIGHT TREMAINE LLP
920 Fifth Avenue, Suite 3300
Seattle, WA 98104
Tel: (206) 622-3150
MaryAnnAlmeida@dwt.com

I certify that true copies of the Proposed Brief of *Amici Curiae* Center for Democracy & Technology, Electronic Privacy Information Center, and Electronic Frontier Foundation was served by Electronic Service or by Overnight UPS service this date upon the following:

Heather Joy Baker
Clerk of the Supreme Court
Supreme Court of New Jersey
Hughes Justice Complex
P.O. 970
25 West Market Street
Trenton, New Jersey 08625

Honorable Matthew J. Platkin, Attorney General
Office of the Attorney General
State of New Jersey
Richard J. Hughes Justice Complex
25 West Market Street
Trenton, New Jersey 08625

Rubin Sinins
Javerbaum Wurgaft Hicks Kahn Wikstrom & Sinins, P.C.
505 Morris Ave.
Springfield, NJ 07081

/s/Geoffrey S. Brounell
Geoffrey S. Brounell

Dated: January 9, 2023