Alexander Shalom (BAR No. 021162004)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102

**SUPREME COURT OF NEW JERSEY**

| | |
|---|---|
| FACEBOOK, INC.,<br>*Plaintiff*,<br><br>v.<br><br>STATE OF NEW JERSEY<br>*Defendant*. | : Criminal Action<br>: No. 087054<br>:<br>: Superior Court of New Jersey,<br>: Appellate Division<br>: Nos. A-3350-20, A-0119-21 |
| 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. | : Sat Below:<br>: Hon. Jack M. Sabatino, P.J.A.D.<br>: Hon. Garry S. Rothstadt, J.A.D.<br>: Hon. Jessica R. Mayer, J.A.D. |

# BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION & AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY

Alexander Shalom (BAR No. 021162004)
Jeanne LoCicero (BAR No. 024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
ashalom@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
2101 Webster Street #1300
Oakland, CA 94612
Tel: (415) 343-0758
jgranick@aclu.org

* *Pro hac vice* pending

*Attorneys for* Amici Curiae

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**CASES**

**STATUTES**



**OTHER AUTHORITIES**

## PRELIMINARY STATEMENT

The Appellate Division concluded that so long as the State makes a single showing of probable cause, the sole limitation on the State's ability to surveil an individual's prospective private communications is Rule 3:5-5(a), which requires that a warrant be executed within 10 days of issuance. Under the ruling below, therefore, courts can issue warrants for communications and related data (communications data warrants or "CDWs") so long as the surveillance is limited to 10 days' worth of future conversations. This ongoing communications surveillance, the Appellate Division held, is not subject to enhanced safeguards contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 *et seq*. (hereinafter "Wiretapping and Electronic Surveillance Act" or "Title III")[1], or the equivalent provisions of the New Jersey Wiretapping and Electronic Surveillance Act ("NJWESCA"), N.J.S.A. 2A:156A-2, 2A:156A-12.

The Appellate Division's conclusion is wrong, and Meta's argument that a CDW cannot authorize ongoing surveillance of future communications is correct. The Appellate Division's ruling violates *Berger v. New York*, 388 U.S. 41 (1967), with deeply troubling consequences for privacy in modern digital

[1] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, Title III, 18 U.S.C. §§ 2510–20.

communications. In *Berger*, the U.S. Supreme Court held that the sensitivity of and privacy interest in private conversations require enhanced procedural safeguards to cabin executive discretion, minimize the risk of abuse, and avoid the problem of general warrants. *Id.* In response to *Berger*, the U.S. Congress and state legislatures, including New Jersey's, passed comprehensive legislation regulating wiretaps and electronic surveillance. *See* Wiretapping and Electronic Surveillance Act; NJWESCA. These statutes govern prospective, ongoing searches and seizures of communications, and the surveillance at issue here can only be constitutionally conducted with the kinds of safeguards that these statutes provide.

Indeed, regardless of whether the novel surveillance here is labeled an "interception," the constitutional concerns that motivated the *Berger* Court plainly apply and should guide this Court's ruling. In the five decades since *Berger*, technological developments have vastly expanded the universe of private communications susceptible to government intrusions and at risk of indiscriminate government rummaging. Service providers now store extensive records of past conversations, far more revealing even than the eavesdropping or wiretapping of old. In 1967, police had to tap into conversations at the right place and the right time, or the conversations instantly disappeared. Now, law enforcement can go back in time, and scour vast repositories of emails, texts,

direct messages, photos, location data, search histories, and more. As with the interception of current or prospective conversations, when law enforcement engages in surveillance of sensitive digital communications content, the Constitution requires scrupulous adherence to the dictates of the Fourth Amendment, especially the particularity requirement, to balance the relationship between the state and the individual and to ensure that police do not abuse the extensive access modern technology affords to intimate matters.

Finally, the New Jersey Constitution provides protections beyond those of the Fourth Amendment, and therefore dictates that this Court hold that the types of protections codified in Title III and the NJWESCA must also apply to the communications surveillance at issue here.

## STATEMENT OF FACTS AND PROCEDURAL HISTORY

For the purpose of this brief, *amici* accept the statement of facts and procedural history contained in Meta's Appellate Division brief, adding the following: The Appellate Division affirmed the trial court's quashing of the communication data warrants, but held that wiretap orders were not required. *Facebook, Inc. v. State*, 471 N.J. Super. 430, 436 (App. Div. 2022). The panel imposed certain temporal limitations on the use of communication data warrants. *Id.* Thereafter, Facebook sought leave to appeal, which this Court

granted. *Facebook, Inc. v. State*, 251 N.J. 378 (2022). The State sought and obtained leave to cross-appeal. *Facebook, Inc. v. State*, 252 N.J. 36 (2022).

## ARGUMENT

### I. Today's data surveillance is far more invasive even than eavesdropping and wiretaps of old.

Computers and other digital devices contain an immense amount of private, sensitive data. Three and a half decades separate the world's first e-mail message[2] from the vast storage and communicative capacities of cloud computing.[3] With cloud computing, previously unimaginable troves of information—including private photos, voice recordings, videos, documents, diaries, correspondence, appointments, medical records, and more—are stored by third-party companies and can be accessed by a user at any time, via any device with an Internet connection.

These advances also mean that individuals can engage in an increasing variety and volume of cloud-based electronic communications, including emails, SMS and text messages, chats on messaging apps, and social media messages. Those communications can include not just conversations, but also

---

[2] Samuel Gibbs, *How Did Email Grow from Messages Between Academics to a Global Epidemic?*, Guardian (Mar. 7, 2016) (Aa29).

[3] Antonio Regalado, *Who Coined 'Cloud Computing'?*, MIT Tech. Rev. (Oct. 31, 2011) (Aa2) (noting 2006 as the year Google's Eric Schmidt introduced the term to an industry conference, with the term quickly gaining popularity after).

all of the kinds of digital files now stored in our devices and on our Internet accounts.

In recent years, the use of cloud-based services for digital storage and communication has skyrocketed. Today's most popular cloud storage platforms allow personal users to store massive quantities of personal information on their servers. Microsoft, Dropbox, Apple, and Google all offer their users several gigabytes of data storage for free and up to two terabytes by subscription.[4] A terabyte of cloud storage totals over 250,000 personal photos, nearly 21 continuous days of high-definition video, or the equivalent of 6.5 million pages of documents spanning 1,300 physical filing cabinets.[5]

With many cloud-based services, users can set up their systems so that their personal data and files are instantaneously and automatically transmitted from their local computer or hard drive, and stored on remote servers.[6] The owner can then access those files, share access with others, and maintain control across platforms over who has editing access or viewing rights. The low cost of cloud storage also means that social media companies allow users

---

[4] Microsoft, *OneDrive Personal Cloud Storage* (Aa25); Dropbox, *Choose the Right Dropbox for You* (Aa12); Apple, *iCloud Storage Plans and Pricing* (Aa8); Google One, *One Membership to Get More Out of Google* (Aai).

[5] Dropbox, *How Much is 1 TB of Storage?* (Aa17).

[6] Microsoft 365, *OneDrive PC folder backup* (Aa20).

to constantly add content—conversations, photos, videos, audio recordings, and other files—without having to delete older data, resulting in years of personal and communicative information stored online.

In short, today's digital platforms store far more information revealing individuals' private matters than one could obtain from past physical analogs. *See Riley v. California*, 573 U.S. 373, 394–95 (2014); *see also United States v. Comprehensive Drug Testing, Inc.* (hereinafter "*CDT*"), 621 F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam).

Because online accounts "collect[ ] in one place many distinct types of information"—for example, an address, a note, a prescription, a bank statement, or a video—digital data "reveal much more in combination than any isolated record," *Riley*, 573 U.S. at 394, and they reveal much more about "an individual's private interests or concerns." *Id.* at 395. Moreover, while our garages and desk drawers may fill all the way up with knickknacks, requiring periodic spring cleaning, digital data can pile up and persist indefinitely. Law enforcement access to electronically stored data can expose years'—even decades'—worth of personal information. *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018); *Riley*, 573 U.S. at 394. This combination of volume, depth, and longevity of personal information raises severe privacy risks when it comes to digital searches.

Technology has also given law enforcement the ability to obtain previously unknowable information, *Carpenter*, 138 S. Ct. at 2217–18, such as records of what we read (Internet browsing history), where we've gone (location history), what we've said (extensive conversations in the form of email or text), and to whom we've said it (associational information), along with efficient and centralized access to medical records and other sensitive information. Courts have already recognized some of these categories of information as deserving of particularly stringent privacy protections. *See, e.g.*, *Riley*, 573 U.S. at 395–96 (search and browsing history "could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD") ; *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010) (email); *In re Grand Jury Subpoena*, 828 F.3d 1083 (9th Cir. 2016) (same). As the Ninth Circuit has explained, "searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers." *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009).[7]

[7] In addition, searches of computers or other digital devices that are connected to the Internet present risks that law enforcement searching through a device could access more than locally stored physical media but online accounts, too. *See, e.g.*, *United States v. Shipp*, 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019) (Police access to social media accounts and online communications services

## II. Under *Berger*, the Fourth Amendment requires that warrants seeking ongoing access to future private communications contain special safeguards, like those enshrined in Title III and the NJWESCA, regardless of whether acquisition is contemporaneous or not.

The Supreme Court's decision in *Berger* governs the ongoing surveillance of future private communications at issue in this case. The State asserts that it may obtain multiple disclosures of future private electronic communications without complying with either the federal or state wiretap and electronic surveillance statutes, solely because the technological means of transmitting information over the Internet involves temporary storage on a provider's servers. However, the State cannot avoid the constitutional safeguards that *Berger* prescribes by pointing to minor technological differences between how companies facilitated prospective communications surveillance in the 1960s and today.

In *New York v. Berger*, the U.S. Supreme Court held that a New York statute—which authorized the interception of communications based only on reasonable grounds to believe that evidence of crime may be obtained—violated the Fourth Amendment. 388 U.S. 41 (1967). The New York statute

---

present a "threat [that] is further elevated . . . because, perhaps more than any other location—including a residence, a computer hard drive, or a car—[they] provide[] a single window through which almost every detail of a person's life is visible.").

did not require particularity as to the communications, conversations, or discussions to be seized, the facilities where the interception would take place, or the communications that would be obtained. Nor did it require a showing of necessity, minimization of innocent or irrelevant conversations, nor reporting to the judge. *Id.* at 59.

In ruling the New York statute unconstitutional, the Court noted that access to "private discourse" is particularly invasive and susceptible to abuse. *Id.* at 45. Indeed, eavesdropping invades "the innermost secrets of one's home or office," *id.* at 63, and presents "inherent dangers." *Id.* at 60. Eavesdropping "involve[d] an intrusion on privacy that is broad in scope," *id.* at 56.

In particular, the Court held that the New York statute violated the Fourth Amendment in part because it permitted a single warrant to authorize multiple prospective searches and seizures. The Court stated that eavesdropping for a two-month period was "[the] equivalent of a series of intrusions, searches and seizures pursuant to a single showing of probable cause[,] . . . [and avoids] prompt execution." *Id.* at 59. The Fourth Amendment requires that continuation of surveillance be based on "*present* probable cause," and not on the probable cause showing in the original warrant. *Id.* Yet that is exactly what the State seeks to do here.

The Court further noted that the search was unreasonable because of its impact on uninvolved third parties. "During such a long and continuous (24 hours a day) period[,] the conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation." *Id.* Again, the information the State would obtain should this warrant be enforced will have a broad impact over a much longer period of time than a day.

To illustrate the lack of adequate protections in the New York law, the Court compared warrants authorized by the New York statute to a court order it upheld in another case, *Osborn v. United States*, 385 U.S. 323 (1966). In particular, the Court noted that the *Osborn* warrant "authorized *one limited intrusion*[,] *rather than a series or a continuous surveillance*." 388 U.S. at 57 (emphasis added). The Court also noted that the *Osborn* officer's subsequent searches were based on a new probable cause order. Further, the officer executed the warrants "with dispatch, and not over a prolonged and extended period." *Id.* In contrast, the State here seeks an order permitting a series of intrusions, based on one showing of probable cause, and without need to go back to court to resume or initiate a new search. The surveillance would take place over a prolonged period. Such an order would violate the Fourth Amendment for the same reason that the statute in *Berger* did. *Id*.

The State argues that it need not comply with the dictates of *Berger*, and thus not of the federal or state statutes that apply to wiretaps and electronic surveillance, because it has contrived to avoid an "interception," which, it says, means only the acquisition of the contents of communications *contemporaneous* with their transmission. The State's legal argument exploits the "store and forward" nature of the computer protocols underlying the Internet, even though the information it seeks to obtain is functionally indistinguishable from what a wiretap would produce, but without the constitutionally-required safeguards. *Cf. United States v. Espudo*, 954 F. Supp. 2d 1029, 1034–35 (S.D. Cal. 2013) (holding that when the government "obtain[s] cell site location data for forward-looking periods of time," it must abide by the rules governing real-time surveillance, notwithstanding that the data is "maintained by the cell phone provider, however briefly, before it [is] sent to the Government").

Moreover, *Berger* does not draw the sharp line between contemporaneous and stored communications that the State says it does. While *Berger* uses the term "intercept," it does not define it as "contemporaneous acquisition." To the extent the examples in *Berger* involved contemporaneous access, that is likely because, in 1967, such access was the only reliable way to obtain private conversations. Then, as people talked, the words disappeared

forever unless someone was right there to hear them or had devised physical means to record them.

But nothing in *Berger*'s reasoning turns on whether the intrusions are contemporaneous or delayed by 15 minutes. The *Berger* Court's analysis was based on the invasiveness of government access to private conversations, and not the technology by which police accomplish the surveillance. While legislatures subsequently sought to implement the constitutionally-required safeguards in statutes regulating "wiretaps and electronic surveillance," *see* Wiretapping and Electronic Surveillance Act *and* NJWESCA, *Berger* itself emphasized how its principles reached a variety of surveillance methods. Indeed, the Court noted how communications surveillance had evolved through the years, from eavesdroppers lurking near windows or walls to intercepting telegraph signals, connecting to a telephone line, planting "bugs," beaming electronic rays at walls or glass windows, using tiny concealed or parabolic microphones, or employing a combination mirror transmitter that transmits images as well as sounds. 388 U.S. at 45–47. It explained that "few threats to liberty exist which are greater than that posed by the use of eavesdropping devices," regardless of the nature of that device. *Id.* at 63.

*Berger* is clear that law enforcement access to ongoing private electronic communications requires safeguards beyond a traditional warrant. The State

would use a technological wrinkle to gain exactly that kind of broad access on a repeated, prospective basis, with just one probable cause showing and without showing necessity, minimization, or particularity as to conversations or facilities, and without following other procedures acclaimed in *Berger* and codified in statute. But *Berger*'s reasoning does not depend on the technology employed. The *Berger* safeguards enshrined in New Jersey's wiretapping statute apply to conversation surveillance accomplished by ongoing access to today's online accounts, just as much as they do to surveillance accomplished by ongoing access to private communications using older techniques such as telephone surveillance. For these reasons, Meta's view that a CDW is insufficient and the State must comply with Title III and the NJWESCA is correct.

## III. If the Court disagrees that the proposed series of ongoing acquisitions of electronic communications are an "interception", the *Berger* and subsequent electronic search cases nevertheless require strict adherence to Fourth Amendment safeguards.

Surveillance that by its nature involves a broad intrusion on conversational privacy requires strict adherence to the Fourth Amendment's requirements. In light of the extraordinary volume and breadth of sensitive information contained in today's electronically stored and transmitted information, warrants must impose clear limitations on law enforcement's electronic searches and seizures so as to avoid unnecessary exposure of our

intimate details to investigators. Even if the Court disagrees that the wiretapping statutes apply to this case, it should nevertheless ensure that the CDWs here specify the category of data, date range, or other fact-specific criteria that will ensure particularity and guard against overbreadth, and not authorize a "printout of everything that the user has". *State's Br. in Opp'n to FB's Mot. to Appeal*, at 2. In addition, courts can and sometimes must require investigators to report back, to segregate non-responsive data through the use of clean teams or other means, to delete irrelevant data, and to comply with other privacy-protecting practices to ensure that searches are constitutional.

The Fourth Amendment is intended "to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214 (citation and quotation marks omitted). It requires that search warrants particularly describe the places to be searched and the things to be seized (particularity), and prohibits search for or seizure of anything for which there is not probable cause (overbreadth). Even in the context of warrants authorizing the search and seizure of a person's physical papers, the Supreme Court has long recognized the grave dangers of government access to papers without probable cause. As a result, "responsible officials, including judicial officials, must take care to assure that [searches and seizures] are conducted in a manner that minimizes unwarranted intrusions upon privacy." *Anderson v. Maryland*, 427 U.S. 463,

482 n.11 (1976). These concerns are especially salient in the face of expanding technological search capabilities, *see Riley*, 573 U.S. at 394–95, and *Berger*'s warnings about the "inherent dangers" of unbounded electronic searches and seizures hold true whether law enforcement seeks to obtain future communications or a complete record of those that have already occurred. 388 U.S. at 58–60.

Critically for the account searches and seizures at issue here, the Fourth Amendment requires that searches and seizures be limited by time frame, to relevant categories of information, and by other case-specific factors to the extent possible. There is no need for—and the Fourth Amendment does not allow—"all-content" CDWs demanding seizure of any account content or digital files that might exist.

First, courts regularly require the government to specify discrete categories of digital information to satisfy particularity and obtain a valid warrant. For example, in one federal investigation of an illegal firearms charge, a search warrant demanded that Facebook provide all the user's personal information, activity logs, photos, videos, posts, private messages, chats, friend requests, video call history, check-ins, IP logs, "likes," use of Facebook Marketplace, payment information, privacy settings, blocked users, tech support requests, and more. *United States v. Shipp*, 392 F. Supp. 3d 300,

303–06 (E.D.N.Y. 2019). In another, the government sought all financial records, notes, memoranda, records of internal and external communications, correspondence, audio tapes, video tapes, and photographs, among other information. *United States v. Wey*, 256 F. Supp. 3d 355, 364–66 (S.D.N.Y. 2017). Both courts held that warrants for seizure of any category of data without "link[ing] the evidence sought to the criminal activity supported by probable cause" did "not satisfy the particularity requirement." *Id.* at 387 (citatons omitted); *Shipp*, 392 F. Supp. 3d at 307. *See also In re Three Hotmail Email Accounts*, No. 16-MJ-8036-DJW, 2016 WL 1239916 (D. Kan. Mar. 28, 2016), *overruled in part by In re Info. Associated With Email Addresses Stored at Premises Controlled by the Microsoft Corp.*, 212 F. Supp. 3d 1023 (D. Kan. 2016) (denying warrant to search all content of email accounts).

State courts agree with this principle in the context of both social media and cell phone searches and seizures. *See Richardson v. State*, No. 46, 2022 WL 3711713 (Md. August 29, 2022) ("all-content" warrant to search cell phone should have been limited by time frame and categories of data); *State v. Smith*, 278 A.3d 481 (Conn. 2022) (warrant did not sufficiently limit the search of the contents of a cell phone by a description of the areas within the phone to be searched or by a time frame reasonably related to the crimes); *State v. Fairley*, 457 P.3d 1150 (Wash. Ct. App. 2020) (Fourth Amendment's

particularity requirement is of heightened importance when searching repositories for expressive materials, in the context of cell phones). Thus, courts should authorize seizure of only those categories of data likely to contain evidence of the crime. Without that limitation, a search is overbroad.

Second, seizures of account data should be limited by timeframe. CDWs can easily accomplish this. If an offense allegedly took place in 2021, police should not need obtain email from any other year, never mind a copy of the entire account, as it appears the State is seeking here. *See United States v. Abboud*, 438 F.3d 554, 576 (6th Cir. 2006) ("Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad." (citations omitted)); *United States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure records before the first instance of wrongdoing mentioned in the affidavit); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no warrant issued where government did not include a date limitation); *In re Search of Google Email Accounts identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application without date restriction denied as overbroad).

Third, when available, courts can and should also use other criteria of digital information to constrain police and ensure that seizures are scoped to

probable cause, and that the warrant particularly describes the proper data to search, and what to search for. *See United States v. Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (deeming a warrant's failure to narrow a search based on ownership of a cell phone to be insufficiently particular). For example, if conversations between the target and known co-conspirator are potential evidence of a crime, the warrant could demand that Facebook turn over only messages between those two people. *In re Search of Info. Associated With Four Redacted Gmail Accounts*, 371 F. Supp. 3d 843, 845 (D. Or. 2018) (warrant for all emails associated with suspect's account is overbroad because Google is able to disclose only those emails the government has probable cause to search). If investigators' analysis reveals that another person may be involved, law enforcement can get a warrant to expand the search. But, as *Berger* points out, "conversations of any and all persons" should not be "seized indiscriminately and without regard to their connection with the crime under investigation." 388 U.S. at 59. Yet, that is what a "snapshot" of a Facebook account does.

Finally, depending on the facts of the investigation, which judges have access to via affidavits in support of warrants, courts may further constrain potentially abusive rummaging through private data. To protect the intermingled information that investigators do not have probable cause to seize

or review, courts can enhance oversight by imposing search protocols or requiring forensic examiners to log queries for later judicial review. Courts might also require law enforcement to use clean teams, and to segregate and delete irrelevant data, or implement other privacy-protecting means as may be appropriate. *CDT*, 621 F.3d at 1177.

In sum, the surveillance here must be conducted under the safeguards prescribed in *Berger* and implemented by Title III and the NJWESCA. *See* Part II *supra*. But if the Court disagrees, a CDW for one or more complete "snapshots" of a Facebook account should only issue if it closely adheres to Fourth Amendment safeguards. Failure to do so can put the target and everyone he or she communicates with at risk of a series of general searches and seizures that could be easily abused.

## IV. The New Jersey Constitution also requires these safeguards, as it is more protective than the federal Constitution.

Although New Jersey's Wiretap and Electronic Surveillance Act, NJWESCA, N.J.S.A. 2A:156A-1–26, was modeled after Title III of the Omnibus Crime and Safe Streets Act, 18 U.S.C. §§ 2510–20, *State v. Ates*, 217 N.J. 253, 266 (2014), courts interpreting the state law must look to the State Constitution to ensure their interpretation "safeguard[s] an individual's right to privacy." *State v. Feliciano*, 224 N.J. 351, 370, 372–77 (2016) (*quoting Ates*, 217 N.J. at 268). The United States Constitution, as interpreted by the United

States Supreme Court, provides important guidance for this Court. But as the Court has emphasized before, while those interpretations "may serve to guide us in our resolution of New Jersey issues, 'we bear ultimate responsibility for the safe passage of our ship.'" *State v. Cooke*, 163 N.J. 657, 666–67 (2000) (quoting *State v. Hempele*, 120 N.J. 182, 196 (1990)). For more than four decades the New Jersey Constitution has protected individuals' rights where its federal counterpart has not. *See State v. Alston*, 88 N.J. 211, 225 (1981) (discussing divergence from federal constitutional jurisprudence).

New Jersey courts recognize that the State Constitution provides greater protections than its federal counterpart in a host of relevant contexts. For example, New Jersey courts have refused to erect barriers to civilians' ability to challenge unlawful searches and seizures. *Compare Alston*, 88 N.J. at 228–29 (taking broad view of standing to challenge validity of searches), *with Rakas v. Illinois*, 439 U.S. 128, 134 (1978) (taking narrow view). When a police officer violates a person's rights, the New Jersey Constitution provides a remedy, regardless of the officer's subjective intent. *Compare State v. Novembrino*, 105 N.J. 95, 157–58 (1987) (rejecting good-faith exception to the exclusionary rule) *and State v. Carter*, 247 N.J. 488, 532 (2021) (declining, under the State Constitution, to adopt a reasonable mistake of law exception) *with United States v. Leon*, 468 U.S. 897, 905 (1984) (recognizing good-faith

exception) *and Heien v. North Carolina*, 574 U.S. 54, 61 (2014) (finding stop justified even when based on a reasonable mistake about what the law forbids). Similarly, New Jersey Courts have recognized the peril of allowing police to easily circumvent the warrant requirement through a lax view of consent. *Compare State v. Johnson*, 68 N.J. 349, 353–54 (1975) (requiring showing that consent to search was knowingly given) *and State v. Carty*, 170 N.J. 632, 651 (2002) (disallowing routine requests for consent to search in automobile stops) *with Schneckloth v. Bustamonte*, 412 U.S. 218, 225 (1973) (requiring simply that consent to search be voluntary) *and Florida v. Bostick*, 501 U.S. 429, 434 (1991) (approving routine requests for consent without reasonable suspicion).

Most critically here, this Court has found expectations of privacy where the United States Supreme Court and some federal appellate courts have not, recognizing the vast swaths of personal information that would be revealed in a search of curbside garbage (*compare Hempele*, 120 N.J. at 215 (expectation of privacy in curbside trash) *with California v. Greenwood*, 486 U.S. 35, 37 (1988)), bank records (*compare State v. McAllister*, 184 N.J. 17, 26 (2005) (expectation of privacy in bank records) *with United States v. Miller*, 425 U.S. 435, 442 (1976) (no expectation of privacy in bank records)), utility records (*compare State v. Domicz*, 188 N.J. 285, 299 (2006) (acknowledging expectation of privacy in utility records) *with Smith v. Maryland*, 442 U.S.

735, 743–44 (1979) (no expectation of privacy in calling records)), Internet Service Provider subscription records (*compare State v. Reid*, 194 N.J. 386, 389 (2008) (expectation of privacy in Internet Service Provider records) *with, e.g.*, *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (no expectation of privacy in Internet Service Provider records)), and cellphone location (*compare State v. Earls*, 214 N.J. 564, 585 (2013) (expectation of privacy in real-time cell phone location data) *with Carpenter*, 138 S. Ct. at 2220 (finding expectation of privacy in historical cell phone location data, but expressing no view on real-time cell tracking)).

As discussed above, the United States Constitution requires at least as much restraint and as many safeguards as a wiretap order for the prospective surveillance the State is asking for here. The New Jersey Constitution requires at least as much as well, if not more.

## CONCLUSION

For the reasons set forth above, the Court should hold that the privacy protections codified in Title III and the NJWESCA apply to the communications surveillance at issue here.

Dated: October 5, 2022

Respectfully submitted,

Alexander Shalom (BAR No. 021162004)
Jeanne LoCicero (BAR No. 024052000)
AMERICAN CIVIL LIBERTIES UNION
OF NEW JERSEY FOUNDATION
570 Broad Street, 11th Fl.
Post Office Box 32159
Newark, NJ 07102
Tel: (973) 854-1714
ashalom@aclu-nj.org
jlocicero@aclu-nj.org

Jennifer Stisa Granick*
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
2101 Webster Street #1300
Oakland, CA 94612
Tel: (415) 343-0758
jgranick@aclu.org

* *Pro hac vice* pending

*Attorneys for* Amici Curiae