SYLLABUS

This syllabus is not part of the Court's opinion. It has been prepared by the Office of the Clerk for the convenience of the reader. It has been neither reviewed nor approved by the Court and may not summarize all portions of the opinion.

**Facebook, Inc. v. State (A-61-21; A-7-22) (087054)**

**Argued March 13, 2023 -- Decided June 29, 2023**

**RABNER, C.J., writing for a unanimous Court.**

The Court considers whether Facebook can be compelled to provide the contents of two users' accounts every 15 minutes for 30 days into the future based only on probable cause, the ordinary standard for a search warrant, or whether the State must instead satisfy certain requirements and apply for a wiretap order, which requires an enhanced showing -- one beyond probable cause -- because gaining access to private communications in real time is considerably more intrusive than a typical search. The 15-minute delay is because of technical limitations; it is as fast as Facebook can provide the information. Even though it seeks extensive information from private user accounts that does not yet exist, in as close to real time as possible, the State argues that, in light of the 15-minute delay, it is obtaining "stored communications," which do not require a wiretap order. Nowhere else in the nation has law enforcement sought prospective communications from Facebook users' accounts without presenting a wiretap order.

In the two matters under review, trial courts quashed the State's request for prospective information based on a Communications Data Warrant (CDW), which is the equivalent of a search warrant and can be issued on a showing of probable cause.

The Appellate Division consolidated the cases and held that the State could obtain prospective electronic communications with a CDW, reasoning that the wiretap statute applied to the contemporaneous interception of electronic communications, not efforts to access communications in storage. 471 N.J. Super. 430, 455-56, 459 (App. Div. 2022). To ensure compliance "with the federal and state constitutions and [New Jersey's] warrant procedures," however, the Appellate Division imposed a 10-day limit on the duration of the CDWs, importing the shorter deadline from Rule 3:5-5(a), which sets a time limit for the execution of search warrants. Id. at 463, 465. The Court granted Facebook leave to appeal, 251 N.J. 378 (2022), and the State leave to cross-appeal the 10-day limit, 252 N.J. 36 (2022).

**HELD:** Based on the language and structure of the relevant statutes, the State's request for information from users' accounts invokes heightened privacy protections.

The nearly contemporaneous acquisition of electronic communications here is the functional equivalent of wiretap surveillance and is therefore entitled to greater constitutional protection. New Jersey's wiretap act applies in this case to safeguard individual privacy rights under the relevant statutes and the State Constitution.

1. The protections guaranteed by the Fourth Amendment to the United States Constitution and Article I, Paragraph 7 of the New Jersey Constitution extend to government surveillance of private conversations. The Supreme Court's landmark opinions in Berger v. New York, 388 U.S. 41 (1967), and Katz v. United States, 389 U.S. 347 (1967), outlined principles to protect individual privacy rights in the area of electronic surveillance. In response to those cases, Congress enacted the Federal Wiretap Act in 1968. 18 U.S.C. §§ 2510 to 2520. New Jersey then enacted the State Wiretap Act, modeled after federal law. Like its federal counterpart, the State Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device." N.J.S.A. 2A:156A-2(c); 18 U.S.C. § 2510(4). The law includes numerous protections, and courts strictly construe the State Wiretap Act to protect individual privacy rights. State v. Ates, 217 N.J. 253, 268 (2014). (pp. 12-17)

2. Stored communications are governed by a different group of statutory provisions. In 1986, Congress enacted the Electronic Communications and Privacy Act (ECPA) to update privacy protections in light of dramatic changes in technology. The ECPA added "electronic" communications to the definition of "intercept" in the Federal Wiretap Act. It also created what is known as the Stored Communications Act (SCA), 18 U.S.C. §§ 2701 to 2713, which focuses on electronic information in storage. New Jersey enacted similar legislation in 1993. The federal and the state stored communications statutes define "electronic communications" and "electronic storage" in nearly identical terms, but they differ in the way they discuss access to stored electronic communications maintained by service providers. Federal law authorizes government entities to require disclosure of a communication "that is in electronic storage" for 180 days or less pursuant to a warrant, or that "has been in electronic storage" for more than 180 days pursuant to a warrant or other specified means. 18 U.S.C. § 2703(a) (emphases added). The parallel New Jersey statute, by contrast, makes no mention of "electronic storage." See N.J.S.A. 2A:156A-29(a). Neither federal nor state law includes enhanced protections for the disclosure of the contents of stored electronic communications. (pp. 18-21)

3. The Court first considers whether the electronic communications the State seeks are covered by New Jersey's equivalent to the SCA. Neither the federal nor the state version of the SCA expressly authorizes disclosure of future communications. See 18 U.S.C. § 2703(a); N.J.S.A. 2A:156A-29(a). The commonsense meaning of the words in the federal SCA -- "is in electronic storage" and "has been in electronic storage" -- do not include content or data that "will be" in storage at a later point in

time. The Court explains why the Federal Dictionary Act does not apply. Although some provisions of the ECPA apply to prospective surveillance activities, the SCA, which governs "stored" communications, does not. And the State's argument fares no better under the State Wiretap Act. The New Jersey Legislature did not incorporate language about electronic storage in N.J.S.A. 2A:156A-29(a). In addition, reflecting the structure of the ECPA, the state code addresses wiretap interceptions at N.J.S.A. 2A:156A-1 to -26 and stored communications at N.J.S.A. 2A:156A-27 to -34. The forward-looking aspects of the act appear in the wiretap sections only, not in the sections about stored communications. The federal and state statutes do not support the use of a warrant to access the contents of prospective electronic communications. (pp. 22-27)

4. The Court next considers whether the requests for information in this appeal are subject to the enhanced privacy protections of the wiretap acts. The State argues the wiretap acts do not apply because the stored messages it seeks will not be intercepted contemporaneously, in real time. Although multiple federal circuits have held that an "intercept" must occur contemporaneously with transmission, the word "contemporaneous" does not appear in the ECPA or its state counterpart. Those rulings stem instead from a Fifth Circuit decision that preceded the ECPA and held that the term "intercept" in the 1968 Federal Wiretap Act required contemporaneity. And, significantly, those federal rulings involved purely historical communications, such as cassette tapes, prior postings on a password-protected website, and stored emails. In none of those cases did anyone access communications either while they were in flight or nearly contemporaneously to their transmission. Some Circuit Courts have raised questions about the contemporaneity requirement. (pp. 27-32)

5. A strict contemporaneity rule adopted before the advent of the Internet would not be a good fit to address the situations technology presents today. Nor would it be consistent with the underlying purpose of the wiretap statutes -- to protect individual privacy. From a practical standpoint, if a strict contemporaneity approach applied, law enforcement would never need to apply for a wiretap order to obtain future electronic communications on an ongoing basis. It would be only natural to apply instead for a CDW, which is easier to obtain but has fewer safeguards for privacy. And in time, as technology improves, today's unavoidable 15-minute delay may well get shorter. The logical extension of the State's position is that law enforcement could avoid the requirements of the wiretap acts by simply asking Facebook to wait a few minutes, while data is stored, before providing electronic communications on an ongoing, future basis. That cannot be right given the underlying aim of the statutes. Based on the language, structure, and intent of the State Wiretap Act, it applies to the near real-time acquisition of prospective electronic communications. Attempts to acquire electronic communications every 15 minutes, for 30 days into

the future, are not covered by New Jersey's equivalent of the SCA. They are instead subject to the requirements of the State Wiretap Act. (pp. 32-33)

6. The wiretap statutes are infused with constitutional considerations, as identified in Berger and Katz. The Constitution sets the benchmark for a reasonable search: the use of a warrant based on probable cause. When a lesser expectation of privacy is involved, or when a search involves a minimal intrusion on an individual's privacy, fewer protections are required. The same is true in reverse. More intrusive searches call for enhanced protections. Here, the privacy interests at stake and the level of intrusion are substantial. There are no limits to the content the State seeks, yet the CDW orders have no minimization requirements. In essence, the State seeks the functional equivalent of a wiretap -- but without the added safeguards the wiretap acts require. If it were possible to obtain the contents of future electronic communications from Facebook in real time, the parties agree the wiretap statutes and protections would apply. The same privacy interests exist here. A warrant based on probable cause is not enough to monitor prospective electronic communications in nearly real time, on an ongoing basis. The principles set forth in Berger and its progeny require the State to make a heightened showing and adhere to the additional safeguards provided in the wiretap acts. The Court's conclusion is grounded in the privacy protections the State Constitution guarantees. (pp. 34-39)

7. Reviewing the required enhanced protections and time limits established by the State Wiretap Act, the Court notes that the 10-day time limit set forth in Rule 3:5-5 is not the right benchmark. The Rule does not apply here. Nor does it resolve any of the statutory or constitutional concerns the CDWs present. Facebook contends the CDWs are flawed because they represent "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause." The heightened protections of the Wiretap Act address that concern. The Court affirms at the same time the principles in State v. Earls, 214 N.J. 564 (2013). (pp. 39-40)

8. Turning to additional arguments raised by the State, the Court explains why the CDWs here are not anticipatory warrants and why the reasonable continuation doctrine does not apply. (pp. 40-43)

9. The Court's ruling appears to align with practices elsewhere. The arguments presented do not identify any jurisdictions, other than New Jersey, which have sought prospective electronic communications based on a search warrant. (p. 43)

**REVERSED. The specified portions of the CDWs are QUASHED.**

**JUSTICES PATTERSON, SOLOMON, PIERRE-LOUIS, and WAINER APTER join in CHIEF JUSTICE RABNER's opinion. JUSTICE FASCIALE and JUDGE SABATINO (temporarily assigned) did not participate.**

SUPREME COURT OF NEW JERSEY

A-61 September Term 2021

A-7 September Term 2022

087054

Facebook, Inc.,

Plaintiff-Appellant/Cross-Respondent,

v.

State of New Jersey,

Defendant-Respondent/Cross-Appellant.

In re the Application of the State of New Jersey for a Communications Data Warrant Authorizing the Obtaining of the Contents of Records from Facebook, Inc.

On appeal from the Superior Court, Appellate Division, whose opinion is reported at 471 N.J. Super. 430 (App. Div. 2022).

| Argued | Decided |
| --- | --- |
| March 13, 2023 | June 29, 2023 |

Seth P. Waxman (Wilmer Cutler Pickering Hale and Dorr) of the District of Columbia bar, admitted pro hac vice, argued the cause for appellant/cross-respondent Facebook, Inc. (Javerbaum, Wurgaft, Hicks, Kahn, Wikstrom & Sinins, attorneys; Rubin Sinins, Seth P. Waxman, Ronald C. Machen (Wilmer Cutler Pickering Hale and Dorr) of the District of Columbia bar, admitted pro hac vice, Catherine M.A. Carroll (Wilmer Cutler Pickering Hale and Dorr) of the District of Columbia and

Virginia bars, admitted pro hac vice, John K. Roche (Perkins Coie) of the District of Columbia, Virginia, and Maryland bars, admitted pro hac vice, Mikella M. Hurley (Perkins Coie) of the District of Columbia and New York bars, admitted pro hac vice, and George P. Varghese (Wilmer Cutler Pickering Hale and Dorr) of the Massachusetts and Pennsylvania bars, admitted pro hac vice, on the briefs).

Sarah C. Hunt, Deputy Attorney General, argued the cause for respondent/cross-appellant State of New Jersey (Matthew J. Platkin, Attorney General, attorney; Sarah C. Hunt, of counsel and on the briefs, and Lila B. Leonard, Deputy Attorney General, on the briefs).

Jennifer Stisa Granick (American Civil Liberties Union) of the California bar, admitted pro hac vice, argued the cause for amici curiae American Civil Liberties Union and American Civil Liberties Union of New Jersey (American Civil Liberties Union of New Jersey Foundation, and American Civil Liberties Union Foundation, attorneys; Alexander Shalom, Jeanne LoCicero, and Jennifer Stisa Granick, on the brief).

Erez Liebermann argued the cause for amici curiae Microsoft Corporation and Google, LLC (Debevoise & Plimpton and Herrick Feinstein, attorneys; Erez Liebermann, Michelle M. Sekowski, and James Pastore (Debevoise & Plimpton) of the New York bar, admitted pro hac vice, on the brief).

Brian J. Neary argued the cause for amicus curiae New Jersey State Bar Association (Jeralyn L. Lawrence, President, New Jersey State Bar Association, attorneys; Jeralyn L. Lawrence, of counsel, and Brian J. Neary, Robert B. Hille, Holly A. Maynard, James H. Maynard, and Matheu D. Nunn, on the brief).

Peter T. Blum, Assistant Deputy Public Defender, submitted a brief on behalf of amicus curiae Public

Defender of New Jersey (Joseph E. Krakora, Public Defender, attorney; Peter T. Blum, of counsel and on the brief).

Geoffrey S. Brounell submitted a brief on behalf of amici curiae Center for Democracy & Technology, Electronic Privacy Information Center, and Electronic Frontier Foundation (Davis Wright Tremaine, attorneys; Geoffrey S. Brounell, David M. Gossett, of the District of Columbia and Illinois bars, admitted pro hac vice, and MaryAnn T. Almeida, of the District of Columbia and Washington bars, admitted pro hac vice, on the brief).

---

CHIEF JUSTICE RABNER delivered the opinion of the Court.

---

In this case, law enforcement officers seek to compel Facebook to provide the contents of two users' accounts every 15 minutes for 30 days into the future. The 15-minute delay is because of technical limitations; it is as fast as Facebook can provide the information.

To conduct a search, the State ordinarily must demonstrate there is probable cause to believe evidence of a crime will be found at a particular place and must obtain a warrant. Gaining access to private communications in real time, however, is considerably more intrusive than a typical search. In those instances, the State must satisfy certain heightened requirements and apply for a wiretap order, which requires an enhanced showing -- one beyond probable cause.

That approach attempts to balance law enforcement's legitimate need to investigate crime and the reasonable privacy rights that individuals possess. Here, even though the State seeks extensive information from private user accounts that does not yet exist, in as close to real time as possible, it claims it only needs to show probable cause. For support, the State presents arguments based on statutes that govern stored communications and wiretap interceptions. In short, the State argues that because of the brief 15-minute delay involved, it is obtaining "stored communications" rather than intercepting live ones, so fewer safeguards apply.

We do not agree. And nowhere else in the nation has law enforcement sought prospective communications from Facebook users' accounts without presenting a wiretap order. Based on the language and structure of the relevant statutes, we find that the State's request for information from users' accounts invokes heightened privacy protections. We also find that the nearly contemporaneous acquisition of electronic communications here is the functional equivalent of wiretap surveillance and is therefore entitled to greater constitutional protection.

Two trial courts quashed the State's request for prospective information based on a Communications Data Warrant (CDW), the equivalent of a search warrant. The Appellate Division, however, concluded that a showing of

probable cause under a CDW was sufficient and ordered Facebook to turn over future electronic communications. We now reverse that judgment and hold that the protections of New Jersey's wiretap act apply in this case in order to safeguard individual privacy rights under the relevant statutes and the State Constitution.

I.

A CDW is "the equivalent of a search warrant." State v. Lunsford, 226 N.J. 129, 133 (2016). Like a standard search warrant, a CDW can be issued based on a showing of probable cause. State v. Finesmith (Finesmith II), 408 N.J. Super. 206, 212 (App. Div. 2009). It "is not subject to the more restrictive procedures and enhanced protections of the Wiretap Act." Ibid.

In March 2021, the New Jersey State Police applied for a CDW to obtain electronic information from the Facebook[1] account of "Maurice" -- a pseudonym for the account holder. Maurice was under investigation for various drug-related offenses. A trial court judge in the Mercer Vicinage granted the CDW application on March 5, 2021.

In an unrelated case the same month, the Atlantic County Sheriff's Office applied for a CDW for information from another Facebook user's

[1] Facebook, Inc. changed its name to Meta Platforms, Inc. in October 2021, months after court proceedings in this matter began. Consistent with filings throughout the case, we continue to use the name Facebook.

account. "Anthony," another pseudonym, was under investigation for gang- and drug-related offenses. A judge in the Atlantic Vicinage granted the CDW on March 16, 2021.

Using slightly different wording, the CDWs sought, among other things, the names, addresses, phone numbers, and email addresses associated with the accounts, as well as the contents of "stored electronic communications." The latter category included "real time access to email with attachments, whether opened or unopened"; "private messaging content"; and "real time access to media . . . uploaded to the account[s]," including images, videos, audio files, and "the contents of private messages in all message folders." The Atlantic CDW also specified Messenger chats; the Mercer CDW specified "posts, comments, [and] messages."

Although both CDWs sought "real time" access to data, the Atlantic CDW noted that "[a]ny 'real time' data obtained from Facebook Inc. is stored on the respective servers and then provided to law enforcement officials in approximately 15 minute intervals."

The CDWs ordered Facebook not to reveal the existence of the investigation for 180 days in the Mercer order, and until further order of the court in the Atlantic order.

The warrants directed Facebook to disclose the contents of both historical and future communications. Law enforcement sought all communications dating back to December 1, 2020 in the Mercer matter and to January 1, 2021 in the Atlantic matter. Facebook turned over those historical records, and they are not part of this appeal.

The CDWs also required Facebook to provide the contents of all future communications for the next 30 days in "real time" -- that is, every 15 minutes. Facebook did not produce any prospective communications and moved to quash that part of the CDWs.

Both trial court judges granted Facebook's motion. The trial court in the Mercer matter observed that ongoing disclosures "in 15-minute increments . . . is the closest that the State can possibly get to real-time interception." The court rejected a narrow construction of the term "interception" in the wiretap statute as "being limited solely to . . . instantaneous transmission." The court also noted that the "prolonged period of intrusion on an individual's privacy" for 30 days "raises legitimate concerns."

The trial court in the Atlantic matter underscored "the right of every citizen to enjoy privacy in their communications." The court observed that the disclosure of future communications every 15 minutes is "tantamount to eavesdropping." The "series of intrusions," the court concluded, needs "to be

authorized not just by a search warrant with probable cause, but with a wiretap warrant which has heightened protections."

The Appellate Division granted the State's motions for leave to appeal and consolidated the two cases. The appellate court held that the State could obtain prospective electronic communications with a CDW but only for a 10-day period. Facebook, Inc. v. State, 471 N.J. Super. 430, 459, 465 (App. Div. 2022).

The Appellate Division reasoned that the wiretap statute applied to the contemporaneous interception of electronic communications, not efforts to access communications in storage. Id. at 455-56. Because the communications the State sought were not "in flight" and had been stored on Facebook's servers, the court found the wiretap act did not apply. Id. at 457.

The Appellate Division instead concluded that the request was governed by federal and state statutes relating to stored communications. Id. at 458-59. The appellate court found that the text of both the federal and state statutes, which we turn to later, encompasses past and prospective communications, that is, "electronic communications not yet in storage when legal process issues." Id. at 459-62.

To ensure compliance "with the federal and state constitutions and [New Jersey's] warrant procedures," however, the Appellate Division imposed a 10-

day limit on the duration of the CDWs. Id. at 465. The court imported the shorter deadline from Rule 3:5-5(a), which sets a time limit for the execution of search warrants. Id. at 463, 465. To obtain communications beyond 10 days, the court held the State must apply for a new CDW based on a new showing of probable cause. Ibid.

The Appellate Division denied Facebook's motion for reconsideration. We granted its motion for leave to appeal, 251 N.J. 378 (2022), and the State's motion for leave to cross-appeal the 10-day limitation, 252 N.J. 36 (2022).

We also granted leave to participate as amici curiae to the American Civil Liberties Union and the American Civil Liberties Union of New Jersey (jointly, the ACLU); the New Jersey State Bar Association (NJSBA); the Office of the Public Defender; Microsoft Corporation and Google, LLC, participating together; and the Center for Democracy & Technology, Electronic Privacy Information Center, and Electronic Frontier Foundation, participating together (collectively, the Center).

II.

Facebook argues that neither federal nor state statutory law authorizes the use of a search warrant to compel disclosure of the contents of prospective communications. Facebook instead maintains that the challenged searches are governed by the enhanced privacy protections of the wiretap acts.

Facebook also contends that the Appellate Division's decision contravenes the Federal and State Constitutions, which bar multiple intrusions based on a single warrant. Facebook argues as well that the CDWs are not anticipatory warrants and cannot be justified under the reasonable continuation doctrine.

The Attorney General, on behalf of the State, submits that the judgment of the Appellate Division should be upheld except for the 10-day limitation imposed on the CDWs. Because the State contends that it seeks only stored electronic communications and not contemporaneous interceptions, it argues that the wiretap acts do not apply. The State also maintains that no language in the relevant statutes about stored communications distinguishes between historical and prospective communications.

The Attorney General additionally argues that continuing disclosure of stored electronic communications under a CDW is constitutional. According to the State, CDWs are appropriate anticipatory warrants; the 15-minute installments satisfy the reasonable continuation doctrine; and the overall intrusion on privacy is reasonable.

Finally, the Attorney General challenges the 10-day limitation imposed by the Appellate Division. The State contends the appellate court incorrectly relied on Rule 3:5-5 to arrive at that limit.

Amici all support Facebook's position. The ACLU emphasizes that "data surveillance" today is "far more invasive" than "wiretaps of old." As a result, the ACLU urges the Court to apply wiretap-like protections, as does the NJSBA.

Microsoft and Google represent that no other jurisdiction has sought ongoing, prospective surveillance of electronic communications based on a warrant. The companies state that when law enforcement agencies outside of New Jersey have made similar requests, they have presented wiretap orders.

The Center warns that the appellate ruling will have a profound negative effect on the personal liberty of surveillance targets as well as the individuals with whom they communicate.

The Public Defender argues more broadly that heightened wiretap-like protections should apply to all efforts by law enforcement to examine large swaths of private electronic communications -- both historical and prospective. Access to entire social media accounts, the Public Defender submits, provides a vast amount of private information about subscribers.

III.

This appeal presents a straightforward question: whether law enforcement officials can obtain the contents of electronic communications from a Facebook account prospectively -- every 15 minutes for 30 days into

the future -- based solely on a showing of probable cause. The answer raises intricate questions about (1) the meaning of the statutes that govern the disclosure of stored communications and wiretap surveillance, and (2) the scope of the constitutional principles that led to the enactment of those laws.

We begin by tracing the history of the relevant statutes.

A.

In nearly identical language, the Fourth Amendment to the United States Constitution and Article I, Paragraph 7 of the New Jersey Constitution protect "against unreasonable searches and seizures." Both constitutions state that warrants must be supported by probable cause and must describe with particularity "the place to be searched" and the "things to be seized."

The particularity requirement was designed to repudiate "general warrants known as writs of assistance" that "officers of the Crown had" used to "bedevil[] the colonists." State v. Feliciano, 224 N.J. 351, 366 (2016) (quoting Stanford v. Texas, 379 U.S. 476, 481 (1965)). The requirement served to "prevent . . . 'wide-ranging exploratory searches.'" Ibid. (quoting Maryland v. Garrison, 480 U.S. 79, 84 (1987)). The use of open-ended, general warrants had been condemned as "the worst instrument of arbitrary power," Boyd v. United States, 116 U.S. 616, 625 (1886) (internal quotation

omitted), and "was a motivating factor behind the Declaration of Independence," Berger v. New York, 388 U.S. 41, 58 (1967).

The protections guaranteed by the Federal and State Constitutions extend to government surveillance of private conversations. See generally Berger, 388 U.S. 41; Katz v. United States, 389 U.S. 347 (1967); Feliciano, 224 N.J. 351. As the Supreme Court has explained, "[t]he need for particularity . . . is especially great in the case of eavesdropping," which "involves an intrusion on privacy that is broad in scope." Berger, 388 U.S. at 56.

The Supreme Court's landmark opinions in Berger and Katz "outlined certain principles to protect individual privacy rights in the area of electronic surveillance." Feliciano, 224 N.J. at 367. In Berger, the Court traced the evolution of surveillance methods from the "ancient practice" of eavesdropping -- "listen[ing] by naked ear under the eaves of houses" -- to intercepting telegraph signals, and from wiretapping telephone lines to planting small electronic listening devices or "bugs." 388 U.S. at 45-47. With the advent of "electronic eavesdropping," a number of states attempted to regulate the practice. Id. at 47-49.

The Berger Court struck down a New York law that authorized the government to record communications based on a "reasonable ground to believe that evidence of crime may be thus obtained." Id. at 54. The Court

identified various flaws in the law: it did not require proof that "any particular offense has been or is being committed"; failed to require officers "to describe with particularity the conversations" to be recorded; allowed for the indiscriminate seizure of conversations with anyone in the area of the recording device "without regard to their connection with the crime under investigation"; had no provisions to stop intercepting communications when "the conversation sought [was] seized" or give notice to the person surveilled; and did not require judicial oversight. Id. at 58-60.

The Court also criticized the statute for authorizing two months of interception, "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause," and for permitting extensions on the very grounds on which the original order was issued. Id. at 59. For those and other reasons, the Court found the statute as "offensive" as the general warrants used in colonial times. Id. at 58.

The Supreme Court issued its decision in Katz later the same year. 389 U.S. 347. In that case, the Court rejected a claim that eavesdropping on calls made from a public telephone booth did not implicate the Fourth Amendment. Katz emphasized that the Fourth Amendment protects "people, not places," and required the government to obtain a warrant before "electronically listening to and recording" private conversations. Id. at 351, 353, 358.

B.

In response to Berger and Katz, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Federal Wiretap Act), 18 U.S.C. §§ 2510 to 2520. United States v. U.S. Dist. Ct., 407 U.S. 297, 302 (1972). New Jersey followed suit later that year and enacted the New Jersey Wiretapping and Electronic Surveillance Control Act (the State Wiretap Act), modeled after federal law. See L. 1968, c. 409 (codified at N.J.S.A. 2A:156A-1 to -26); State v. Ates, 217 N.J. 253, 269 (2014).

Like its federal counterpart, the State Wiretap Act empowers prosecutors to apply for a court order that authorizes law enforcement officers to intercept wire, electronic, and oral communications. N.J.S.A. 2A:156A-8; 18 U.S.C. § 2516. The law defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical, or other device." N.J.S.A. 2A:156A-2(c); see also 18 U.S.C. § 2510(4) (same). The Act also limits interceptions to investigations of specified serious offenses. N.J.S.A. 2A:156A-8; see also 18 U.S.C. § 2516.

Among other things, wiretap applications must include "[a] particular statement of facts showing that other normal investigative procedures . . . have been tried and have failed or reasonably appear to be unlikely to succeed if

tried or to be too dangerous to employ." N.J.S.A. 2A:156A-9(c); see also 18 U.S.C. § 2518(3)(c) (similar).

Wiretap orders must contain strict procedures "to minimize or eliminate the interception of . . . communications not otherwise subject to interception." N.J.S.A. 2A:156A-12(f); see also 18 U.S.C. § 2518(5) (similar). That is accomplished through "extrinsic" and "intrinsic" minimization. State v. Catania, 85 N.J. 418, 429 (1981).

Extrinsic minimization calls for "limiting the hours and total duration of interception." Ibid.; see N.J.S.A. 2A:156A-12(f). Intrinsic minimization "on a call-by-call basis" is also required. Catania, 85 N.J. at 429, 434. Officers must make reasonable efforts to "terminat[e] the interception of individual phone calls . . . as it becomes apparent . . . that the call is not relevant to the investigation." Id. at 429.

Law enforcement officials must also minimize the interception of privileged communications. See, e.g., State v. Terry, 218 N.J. 224, 245 (2014) (spousal communications). "[M]onitoring of [a] conversation must cease immediately" "once the parties have been identified and the conversation between them is determined to be nonpertinent or privileged." United States v. DePalma, 461 F. Supp. 800, 821 (S.D.N.Y. 1978) (discussing "privileged communications between husband-wife, attorney-client and doctor-patient");

see also United States v. Chagra, 754 F.2d 1181, 1182 (5th Cir. 1985) ("[The Federal Wiretap Act] requires the interception of privileged communications to be minimized.").

Under state law, wiretap orders are limited in time to only as long as necessary to achieve their objective or a maximum of 20 days. N.J.S.A. 2A:156A-12(f); see also 18 U.S.C. § 2518(5) (up to 30 days). Extensions or renewals can be granted for two additional periods of up to 10 days. N.J.S.A. 2A:156A-12(f); see also 18 U.S.C. § 2518(5) (extensions up to 30 days).

Federal and state law empower judges to require prosecutors to present periodic reports of "what progress has been made toward achievement of the authorized objective and the need for continued interception." N.J.S.A. 2A:156A-12(h); 18 U.S.C. § 2518(6). The reporting requirement allows for judicial oversight of wiretap interceptions.

As added protections, the Act provides for the sealing of applications and orders, and notice to individuals whose conversations were intercepted. N.J.S.A. 2A:156A-15 (sealing); id. at -16 (notice); see also 18 U.S.C. § 2518(8)(b), (d) (same).

Courts must strictly construe the State Wiretap Act to protect individual privacy rights. Ates, 217 N.J. at 268.

C.

Stored communications are governed by a different group of statutory provisions.

In 1986, Congress enacted the Electronic Communications and Privacy Act (ECPA) "to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunication technologies." S. Rep. 99-541, at 1 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555.

Title I of the ECPA amended the Federal Wiretap Act and, among other things, added "electronic" communications to the definition of "intercept." Pub. L. No. 99-508, § 101(a)(3)(B), 100 Stat. 1848, 1848 (1986) (codified at 18 U.S.C. § 2510(4)). The term had already encompassed "wire" and "oral" communications. Pub. L. No. 90-351, 82 Stat. 211, 212 (1968). The ECPA thus imposed similar restrictions on the interception of electronic communications.

Title II created what is commonly known as the Stored Communications Act (SCA), which focuses on electronic information in storage. 18 U.S.C.

§§ 2701 to 2713. Title III addresses "pen registers" and "trap-and-trace" devices.[2] 18 U.S.C. §§ 3121 to 3127.

New Jersey enacted similar legislation in 1993. The Legislature added new provisions to the State Wiretap Act that largely conform to the Federal SCA. L. 1993, c. 29, §§ 21 to 28 (codified at N.J.S.A. 2A:156A-27 to -34). The new law also protected "electronic" communications by adding the term to the definition of "intercept" under the Wiretap Act. Id. § 1 (codified at N.J.S.A. 2A:156A-2(c)).

The State Wiretap Act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photo-optical system that affects interstate, intrastate or foreign commerce," not including "[a]ny wire or oral communication." N.J.S.A. 2A:156A-2(m); see also 18 U.S.C. § 2510(12) (omitting "intrastate").

Federal and state law define "electronic storage" as "[a]ny temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . [a]ny storage of such communication

---

[2] Pen registers capture phone numbers of outgoing calls placed from a target phone line. Trap-and-trace devices record phone numbers of incoming calls to the target phone. 18 U.S.C. § 3127(3), (4). Neither device captures the content of conversations. Ibid.

by an electronic communication service for purpose of backup protection of the communication." N.J.S.A. 2A:156A-2(q); 18 U.S.C. § 2510(17).

The two statutes differ, however, in the way they discuss access to stored electronic communications maintained by service providers. Federal law authorizes government entities to require disclosure "of the contents of a wire or electronic communication, that is in electronic storage" for 180 days or less pursuant to a warrant, or "has been in electronic storage" for more than 180 days, pursuant either to a warrant, administrative subpoena, or court order.[3] 18 U.S.C. § 2703(a) (emphases added).

The parallel New Jersey statute, by contrast, makes no mention of "electronic storage." The statute instead states that "[a] law enforcement agency, but no other governmental entity, may require" a service provider to disclose "the contents of an electronic communication" pursuant to a warrant. N.J.S.A. 2A:156A-29(a).

[3] Federal law states that administrative subpoenas or court orders may be used in certain instances that are not relevant to this appeal. 18 U.S.C. § 2703(a), (b). In United States v. Warshak, however, the Sixth Circuit held that "[t]he government may not compel a commercial [internet service provider] to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause," and that, "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." 631 F.3d 266, 288 (6th Cir. 2010).

Neither federal nor state law includes enhanced protections for the disclosure of the contents of stored electronic communications.

IV.

Facebook contends the wiretap statutes and the laws that govern stored communications divide generally along the following line: wiretap acts apply to requests to intercept future communications, and laws relating to stored communications cover the disclosure of past communications. The State disputes that distinction. It argues instead that the pivotal question is whether communications are acquired "in flight" -- contemporaneous with their transmission -- or from storage. Under the State's reading of the statutes, laws relating to stored communications encompass future communications so long as they are in electronic storage at the moment law enforcement obtains them.

As noted earlier, the State requested the contents of prospective electronic communications -- for 30 days into the future -- to be delivered every 15 minutes. In writing and at oral argument, Facebook explained that the 15-minute delay is "as near to real time as technologically possible" -- a point the State does not dispute. As the CDW recognizes, Facebook cannot provide communications to the State at the same time as they are created and transmitted. For technical reasons, Facebook must briefly store users' electronic communications before it can forward them to others.

A.

Against that backdrop, we first consider whether the electronic communications the State seeks to obtain are covered by New Jersey's equivalent to the Federal Stored Communications Act. We review that question, as well as other legal issues, de novo. State v. Gomes, 253 N.J. 6, 16 (2023).

1.

The paramount goal when interpreting a statute is to "determine and give effect to the Legislature's intent." State v. Lopez-Carrera, 245 N.J. 596, 612 (2021) (quoting In re Registrant H.D., 241 N.J. 412, 418 (2020)). The plain language of a statute "is typically the best indicator of intent." Id. at 613 (quoting State v. McCray, 243 N.J. 196, 208 (2020)). We "also look to other parts of the statute for context." Malanga v. Township of West Orange, 253 N.J. 291, 310 (2023). When the text is clear, our inquiry is complete. Id. at 311. If the language is ambiguous, we may consider extrinsic materials. Ibid.

Because the State Wiretap Act closely models federal law, "we give 'careful consideration to federal decisions interpreting the federal statute.'" Feliciano, 224 N.J. at 371 (quoting Ates, 217 N.J. at 269). At the same time, we recognize that state law is more restrictive and provides greater protections in several areas. See, e.g., Catania, 85 N.J. at 438-39 (reviewing sections of

the State Wiretap Act that "laid down stricter wiretapping guidelines than did Congress"). States, of course, may enact laws that afford citizens additional privacy protections. Id. at 436.

2.

We begin with the text of the statutes. Neither the federal nor the state version of the SCA expressly authorizes disclosure of future communications. Once again, federal law provides for the disclosure of the contents of a wire communication that "is in electronic storage" for 180 days or less or "has been in electronic storage" for more than 180 days. 18 U.S.C. § 2703(a). State law simply provides for disclosure of content information; the Legislature did not incorporate language about electronic storage or time spent there in the state code. N.J.S.A. 2A:156A-29(a).

The commonsense meaning of the words in the federal SCA -- "is in electronic storage" and "has been in electronic storage" -- do not include content or data that "will be" in storage at a later point in time. The State thus relies on the Federal Dictionary Act in support of its claim that the SCA encompasses both present and future stored communications -- an argument that applies only to the federal statute.

The Dictionary Act provides that "[i]n determining the meaning of any Act of Congress, unless the context indicates otherwise . . . words used in the

present tense include the future as well as the present." 1 U.S.C. § 1 (emphasis added). But when "the definition in [the Dictionary Act] seems not to fit," the phrase "'unless the context indicates otherwise' has a real job to do." Rowland v. Cal. Men's Colony, Unit II Men's Advisory Council, 506 U.S. 194, 200 (1993).

For context here, we look to the overall structure of the Electronic Communications Privacy Act. As noted earlier, it has several components: Title I addresses the Federal Wiretap Act, 18 U.S.C. §§ 2510 to 2521; Title II, the Stored Communications Act, id. §§ 2701 to 2713; and Title III, pen registers and trap-and-trace orders, id. §§ 3121 to 3127.

Facebook points out that Titles I and III apply to prospective surveillance activities -- like the interception of future conversations and the use of devices to collect data about future communications. Those Titles include forward-looking provisions that limit the amount of time to monitor or gather information and offer procedures for "renewal, reporting, minimization, and sealing." In re Application of U.S. for an Order Authorizing Prospective & Continuous Release of Cell Site Location Records (S.D. Tex. Order), 31 F. Supp. 3d 889, 895 (S.D. Tex. 2014).

But Title II, which governs "stored" communications, does not contain those features. See In re Application of U.S. for an Order (1) Authorizing the

Use of a Pen Reg. & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info. (E.D.N.Y. Order), 396 F. Supp. 2d 294, 309 (E.D.N.Y. 2005) ("[T]he profound structural differences between the SCA and the electronic surveillance statutes suggest that Congress did not intend the former to be a vehicle for allowing prospective, real-time surveillance.").[4]

Other courts have similarly observed that the structure of the Stored Communications Act reveals that it covers past, not future, communications. See, e.g., In re Application of U.S. for an Order Authorizing the Installation & Use of a Pen Reg. Device, a Trap & Trace Device, & for Geographic Location Info., 497 F. Supp. 2d 301, 309 (D.P.R. 2007) ("Congress's decision not to include in the SCA any provisions typical of prospective surveillance statutes indicates its intent that the SCA be used for the disclosure of historic and not prospective data."); In re Application of U.S. for Orders Authorizing

[4] E.D.N.Y. Order concluded that the SCA did not empower the government to obtain cell-site information on a prospective, real-time basis. 396 F. Supp. 2d at 295, 314. Instead, the government must demonstrate probable cause pursuant to Fed. R. Crim. P. 41. Id. at 321. The United States Supreme Court held in Carpenter v. United States that a warrant based on probable cause is required for law enforcement to obtain historical cell-site location information. ___ U.S. ___; 138 S. Ct. 2206, 2221 (2018). The Carpenter Court did not address the collection of real-time cell-site information. Id. at 2220. This Court, in State v. Earls, 214 N.J. 564, 569 (2013), held that law enforcement officials could obtain cell-phone location information provided they made a sufficient showing of probable cause. The Court based its ruling on the State Constitution, not on an interpretation of the State Wiretap Act. Id. at 589.

Installation & Use of Pen Regs. & Caller Identification Devices, 416 F. Supp. 2d 390, 395 (D. Md. 2006) ("The structure of the SCA shows that the statute does not contemplate orders for prospective information."); E.D.N.Y. Order, 396 F. Supp. 2d at 314 ("[The SCA] does not authorize a court to enter a prospective order to turn over data as it is captured."); In re Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005) ("[T]he entire focus of the SCA is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party service providers.").

In short, Title II was not designed to apply to future events. As a result, because "the context [of the statute] indicates otherwise," the default rules of the Federal Dictionary Act do not apply. See 1 U.S.C. § 1.

The State's argument fares no better under the State Wiretap Act. Starting with the law's text, the New Jersey Legislature did not incorporate language about electronic storage from the federal statute when it described how to access the contents of electronic communications. Compare N.J.S.A. 2A:156A-29(a), with 18 U.S.C. § 2703(a). Although we generally look to federal law to interpret comparable provisions of the State Wiretap Act, Feliciano, 224 N.J. at 371, in this instance the State Legislature parted

company with Congress. As a result, whether the phrase "is in electronic storage" in the Federal Wiretap Act encompasses prospective communications does not reveal much about the State Act's arguably more limited coverage.

In addition, the State Wiretap Act reflects the ECPA's structure. The state code addresses wiretap interceptions at sections 1 to 26 and stored communications at sections 27 to 34. N.J.S.A. 2A:156A-1 to -34. The forward-looking aspects of the act appear in the wiretap sections only.

For those reasons, the language and structure of the federal and state statutes do not support the use of a warrant to access the contents of prospective electronic communications.

B.

Facebook contends the requests for information in this appeal are subject to the enhanced privacy protections of the wiretap acts. We first consider that claim in the context of the relevant statutes.

The State argues the wiretap acts do not apply because the stored messages it seeks will not be intercepted contemporaneously, in real time. Beyond that, the State submits that to read the SCA in a way that excludes future communications from its reach would nullify the contemporaneity requirement of the wiretap acts or leave future stored communications without a home in the legislative scheme.

1.

Multiple federal circuits have "held that an 'intercept' under the ECPA must occur contemporaneously with transmission." Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003); accord United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994).[5]

The word "contemporaneous" does not appear in the ECPA or its state counterpart. The above rulings stem from the Fifth Circuit's conclusion in United States v. Turk, a case that preceded the ECPA. 526 F.2d 654 (5th Cir. 1976). Turk stated that the term "intercept" in the 1968 Federal Wiretap Act required contemporaneous acquisition of a communication. Id. at 658-59. Post-ECPA Circuit Courts followed suit and reasoned that when it enacted the ECPA, Congress intended to retain the prior "judicial definition" given to "intercept." Konop, 302 F.3d at 878. Those courts also found the "conclusion [was] consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.'" Ibid. (quoting

[5] In In re Application of the State for Communications Data Warrants to Obtain the Contents of Stored Communications from Twitter, Inc., 448 N.J. Super. 471, 485 (App. Div. 2017), and Finesmith II, 408 N.J. Super. at 211-12, the Appellate Division agreed with federal courts that find interception contemplates the contemporaneous acquisition of communications.

Webster's Ninth New Collegiate Dictionary 630 (1985)). Under that line of reasoning, communications that have arrived at their destination or are "in storage" can no longer be intercepted.

For additional support, the State points to the definition of electronic communications in the statutes: the "transfer of signs, signals, writings, images, sounds, data, or intelligence." N.J.S.A. 2A:156A-2(m); 18 U.S.C. § 2510(12) (emphasis added). Once a transfer is complete, the State contends, the information is no longer subject to the wiretap acts.

Some Circuit Courts have raised questions about the contemporaneity requirement. The First Circuit, in United States v. Councilman, addressed whether copying incoming emails sent by a third party to the defendant's customers, before they could read the messages, violated the Federal Wiretap Act. 418 F.3d 67, 70-71 (1st Cir. 2005) (en banc). The defendant's company acted as an email provider that managed the email service. Id. at 70. The defendant claimed that because the messages were stored, not intercepted, at the time they were copied, the Wiretap Act did not apply. Id. at 72.

The Court of Appeals disagreed. It found "that the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process." Id. at 79. For the same reason, it concluded the

messages were "intercepted" under the Wiretap Act even though they were in transient electronic storage. Ibid.

In reaching that conclusion, the appellate court declined to address "whether the term 'intercept' applies only to" the acquisition of messages "contemporaneously with [their] transmission." Id. at 80. The First Circuit cited its prior precedent in In re Pharmatrak, Inc. Privacy Litigation, which expressed "concern . . . about the judicial interpretation of a statute written prior to the widespread usage of the internet . . . in a case involving purported interceptions of online communications." 329 F.3d 9, 21 (1st Cir. 2003) (cited at Councilman, 418 F.3d at 80). Pharmatrak noted "the storage-transit dichotomy adopted by earlier courts may be less than apt to address" recent technological developments. Ibid. In Councilman, the court chose not to "plunge into that morass." 418 F.3d at 80.

The Seventh Circuit in United States v. Szymuszkiewicz addressed a similar situation in which a defendant configured his supervisor's email account to automatically forward all incoming messages to the defendant's email account. 622 F.3d 701, 703 (7th Cir. 2010). The server sent copies within a second. Id. at 704. The defendant asserted he should have been charged under the SCA, not the Wiretap Act, because the emails were not intercepted in flight; they were forwarded to him after they had arrived in the

supervisor's inbox. Ibid. The Circuit Court rejected the claim, noting the delay would have been "no more than an eyeblink," which is "contemporaneous by any standard." Id. at 706.

The Sixth Circuit follows the line of authority that interprets "intercept" to require the contemporaneous acquisition of a communication. Luis v. Zang, 833 F.3d 619, 627-28 (6th Cir. 2016). The Circuit Court, however, also includes "near real-time monitoring" within the meaning of the Wiretap Act. Id. at 631 (emphasis added).

2.

As noted earlier, neither the federal nor the state wiretap statute contains a contemporaneity requirement. The rule stems from federal cases that interpret the federal statute. And the facts underlying those cases are telling.

The above federal cases that adopted a strict contemporaneity rule involved purely historical communications. In Turk, for example, an officer listened to two cassette tapes seized from a car. 526 F.2d at 656. In Steve Jackson Games, officers read 162 private unread emails stored on a computer that operated an electronic bulletin board. 36 F.3d at 459-60. A private employer in Konop accessed an employee's password-protected website and read prior postings located there. 302 F.3d at 872-73. Steiger and Fraser, likewise, involved access to the contents of a computer, 318 F.3d at 1043-44,

and to emails saved on a server, 352 F.3d at 110. In none of those cases did anyone access communications either while they were in flight or nearly contemporaneously to their transmission. The communications were plainly not intercepted in or close to real time.

Imagine instead an attempt by law enforcement to gain broad access to future electronic communications, including private messages, within 15 minutes, the earliest possible moment they are available, for 30 days -- the very situation this case presents. A strict contemporaneity rule adopted before the advent of the Internet would not be a good fit to address that or other situations technology presents today. Nor would such a rule be consistent with the underlying purpose of the wiretap statutes -- to protect individual privacy.

In addition, from a practical standpoint, if a strict contemporaneity approach applied, law enforcement today would never need to apply for a wiretap order to obtain future electronic communications from Facebook users' accounts on an ongoing basis. With either a wiretap order or a CDW, the State today cannot receive information from Facebook any sooner than 15 minutes after a communication has been transmitted. In light of that reality, it would be only natural for law enforcement to apply for a CDW, which is easier to obtain but has fewer safeguards for individual privacy.

The State's argument raises yet other, similar concerns. In time, as technology improves, today's unavoidable 15-minute delay may well get shorter and shorter. The logical extension of the State's position is that law enforcement could avoid the requirements and protections of the wiretap acts by simply asking Facebook to wait a few minutes, while data is stored, before providing electronic communications on an ongoing, future basis. That cannot be right given the underlying aim of the statutes.

Based on the language, structure, and intent of the State Wiretap Act, we find that it applies to the near real-time acquisition of prospective electronic communications.

C.

For those reasons, we conclude that attempts to acquire electronic communications every 15 minutes, for 30 days into the future, are not covered by New Jersey's equivalent of the Stored Communications Act. We find they are instead subject to the requirements of the State Wiretap Act.[6]

---

[6] The parties also discuss the way the wiretap statutes treat the acquisition of voicemails. The ECPA added the electronic storage of voicemails to the federal definition of "wire communication" in 1986, see Pub. L. No. 99-508, § 101(a)(1)(D), and our Legislature did likewise in 1993, see L. 1993, c. 29, § 2(a). Congress rescinded that change in 2001 as part of the USA Patriot Act, Pub. L. No. 107-56, § 209, 115 Stat. 272, 283 (2001), and returned stored "voicemail messages to the lower level of protection provided other electronically stored communications," Konop, 302 F.3d at 878. The State Legislature did not. See N.J.S.A. 2A:156A-2(a). Because the debate does not

V.

The arguments of the parties and amici also raise constitutional concerns. Ordinarily, "we strive to avoid . . . constitutional questions unless required to" consider them. Comm. to Recall Menendez v. Wells, 204 N.J. 79, 95 (2010). If a case can be decided on statutory grounds, we do so "for sound jurisprudential reasons." Harris v. McRae, 448 U.S. 297, 306-07 (1980).

We assess whether constitutional principles also require additional protections in this case for a particular reason: the wiretap statutes themselves are infused with constitutional considerations. As noted earlier, Congress crafted the Federal Wiretap Act to address a series of constitutional concerns the Supreme Court identified in Berger and Katz. U.S. Dist. Ct., 407 U.S. at 302. New Jersey then modeled its statute after the federal law. Ates, 217 N.J. at 269. Neither Congress nor the State Legislature started with a blank slate; they attempted to follow constitutional commands when they enacted special protections from wiretapping. We therefore turn to constitutional considerations implicated in this appeal after we resolve a preliminary issue.

---

provide persuasive authority for the questions before the Court, we do not consider the issue further.

A.

For the first time, the State now argues that Facebook's privacy interest is not the same as an individual who might later be prosecuted based on information obtained through the CDWs. The State contends that distinction is relevant to any reasonableness analysis, but it does not argue that Facebook lacks standing to challenge the CDW orders. Instead, the State contends that defendants later charged with crimes based on evidence obtained through a CDW can assert their privacy interests and contest the orders when they are prosecuted.

We consider the reasonableness of the CDWs under all the relevant circumstances, not the narrower prism the State now advances.

B.

When federal and state legislators drafted the wiretap statutes in 1967 and 1968, they could not have envisioned the technological advances of the last five decades. Hardly anyone could foresee that 50 years later, electronic messages could be transmitted, stored, and made available to law enforcement officials all within minutes. Yet the constitutional principles underlying the Supreme Court's ruling in Berger remain relevant. And those principles call for heightened protections -- similar to what is required for wiretap

interceptions -- when law enforcement officials acquire and monitor prospective electronic communications in nearly real time.

Reasonableness is the touchstone of the Fourth Amendment. State v. Bruzzese, 94 N.J. 210, 217 (1983). To assess whether a search is reasonable, courts balance the State's legitimate interest in investigating criminal conduct and protecting the public against the level of intrusion on a person's privacy. See New Jersey v. T.L.O., 469 U.S. 325, 337 (1985).

The Constitution sets the benchmark for a reasonable search: the use of a warrant based on probable cause. U.S. Const. amend. IV; N.J. Const. art. I, ¶ 7. When a lesser expectation of privacy is involved, or when a "search involves a minimal intrusion" on an individual's privacy, the Fourth Amendment requires correspondingly fewer protections. Winston v. Lee, 470 U.S. 753, 767 (1985). The same is true in reverse. More intrusive searches call for enhanced protections, as Berger demonstrates.

Examples abound in the law. Law enforcement officers, for example, can obtain basic Internet subscriber information with a grand jury subpoena. State v. Reid, 194 N.J. 386, 404 (2008). "More intrusive records, like cell-phone location information, are entitled to greater protection," Lunsford, 226 N.J. at 132, and require a search warrant based upon probable cause, State v. Earls, 214 N.J. 564, 588 (2013).

Similarly, in another area, officers need only reasonable and articulable suspicion that a person is engaged in criminal activity to conduct an investigative stop. Terry v. Ohio, 392 U.S. 1, 30 (1968). But to frisk the individual, a brief but more serious intrusion on personal security, the police need reason to believe the person is armed and dangerous. Id. at 27. And to search a private home, the "first among equals" when it comes to privacy interests, officers must demonstrate probable cause and obtain a warrant. State v. Wright, 221 N.J. 456, 467-68 (2015) (quoting Florida v. Jardines, 569 U.S. 1, 6 (2013)).

When the level of intrusion or the privacy interest is greater still, the Fourth Amendment calls for heightened protections. "[E]avesdropping and wiretapping, search of a private home during the nighttime, or intrusions into the human body" may, "because of their unusual degree of intrusiveness, require more than the usual quantum of probable cause." 2 Wayne R. LaFave et al., Criminal Procedure, § 3.3(b) (4th ed. 2022).

The above examples illustrate a simple principle: "the greater the degree of intrusion into [private areas] by the government, the greater the level of protection" the Constitution requires. Lunsford, 226 N.J. at 131; see also Winston, 470 U.S. at 767 ("[W]hen the State seeks to intrude upon an area in

which our society recognizes a significantly heightened privacy interest, a more substantial justification is required to make the search 'reasonable.'").

In this appeal, the privacy interests at stake and the level of intrusion are substantial. A person's unfiltered private conversations can be quite revealing. See State v. McQueen, 248 N.J. 26, 49 (2021) (noting that monitoring telephone conversations "peer[s] 'into the most private sanctums of people's lives'" (quoting State v. Manning, 240 N.J. 308, 328 (2020))). And nearly contemporaneous access to a wide array of prospective electronic communications, every 15 minutes for a full month into the future, is highly intrusive.

There are no limits to the content the State seeks here. In addition to public posts by Facebook users, the proposed orders encompass private communications of all sorts, including any messages to one's spouse, cleric, doctor, or lawyer. Yet the CDW orders have no minimization requirements.

In essence, the State seeks the functional equivalent of a wiretap -- but without the added safeguards the wiretap acts require. If it were possible for the State to obtain the contents of future electronic communications from Facebook in real time, the parties agree the wiretap statutes and their protections would apply. The same privacy interests exist when the identical

content is disclosed, just minutes after it is transmitted, for an extended period of time into the future.

As a result, we find that a warrant based on probable cause is not enough to monitor prospective electronic communications in nearly real time, on an ongoing basis, under the constitution. The principles set forth in Berger and its progeny require the State to make a heightened showing and adhere to the additional safeguards provided in the wiretap acts. Our conclusion is grounded in the privacy protections the State Constitution guarantees. See Earls, 214 N.J. at 589.

The required enhanced protections include a particularized showing of need, N.J.S.A. 2A:156A-9(c); minimization procedures, both extrinsic, id. at -12(f), and intrinsic, Catania, 85 N.J. at 434; judicial oversight and reporting, N.J.S.A. 2A:156A-12(h); and notice, id. at -16, among others.[7] The time limits of the Wiretap Act should also apply: the State may obtain disclosures for up to 20 days, with possible extensions or renewals for additional 10-day periods. Id. at -12(f).

[7] Facebook challenged only the disclosure of prospective communications. It disclosed historical communications, which are not part of this appeal. Nonetheless, the State is obliged to take steps to ensure it does not review or rely on privileged information contained in past communications -- as it would during the physical search of a home or another location.

The 10-day time limit set forth in Rule 3:5-5 is not the right benchmark. See Facebook, 471 N.J. Super. at 464-65. The Rule requires that search warrants be executed promptly after they are issued to ensure "that probable cause supporting the warrant does not dissipate" before the search is conducted. State v. Carangelo, 151 N.J. Super. 138, 150 (Law Div. 1977). The Rule does not apply here. Nor does it resolve any of the statutory or constitutional concerns the CDWs present.

Facebook advances another constitutional concern as well. Citing Berger, 388 U.S. at 59, Facebook contends the CDWs are flawed because they represent "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause." The heightened protections of the Wiretap Act address that concern. We note at the same time that we affirm the principles in this Court's ruling in Earls, 214 N.J. 564.

VI.

The State presents two other arguments to defend its use of CDWs. First, it points to a body of law relating to anticipatory warrants. That type of warrant is based on "probable cause that at some future time (but not presently) certain evidence of crime will be located at a specified place." United States v. Grubbs, 547 U.S. 90, 94 (2006) (quoting 2 Wayne R. LaFave, Search and Seizure, § 3.7(c) (4th ed. 2004)).

Anticipatory warrants are typically conditioned on a triggering event that would establish probable cause to search. Ibid. The anticipated delivery of contraband to a residence, for example, could establish probable cause to search the home provided there is also probable cause to believe the delivery will take place. Id. at 96-97.

The CDWs here are not anticipatory warrants. They are not based on the likelihood of an event that will supply probable cause to search in the future. They rest on a traditional assertion that probable cause to search -- to capture future electronic communications -- exists at the moment the warrants are signed.

Second, the State relies on the reasonable continuation doctrine. Under that principle, the "police may in some circumstances temporarily suspend a search authorized by a warrant and re-enter the premises at a later time to continue the search." State v. Finesmith (Finesmith I), 406 N.J. Super. 510, 519 (App. Div. 2009). The later "entry must . . . be a continuation of the original search, [and not] a new and separate search." Ibid. (omission in original) (quoting United States v. Keszthelyi, 308 F.3d 557, 569 (6th Cir. 2002)). And "the decision to conduct a second entry to continue the search must be reasonable under the totality of the circumstances." Ibid. (quoting Keszthelyi, 308 F.3d at 569). The doctrine, however, does not authorize a

second search based on a single warrant "that is not a continuation of the first." State v. Carrillo, 469 N.J. Super. 318, 339 (App. Div. 2021).

The Appellate Division applied the doctrine in Finesmith I. In that case, the police arrived at the defendant's home with a warrant to search for all computers located there. 406 N.J. Super. at 520. Members of the search team found evidence of child pornography on a computer in the basement, left for the defendant's office after he told them an additional laptop was located there, and later returned to continue the search at the home after the defendant said the laptop was in a van in the garage. Id. at 515-17.

The appellate court upheld the search. Id. at 521. It observed that "but for the fact" the defendant said his laptop was elsewhere, the search of the home would have continued until the police found the item. Ibid. The court also noted that officers returned immediately when they learned the laptop was in the garage. Ibid. Under the circumstances, the Appellate Division found the second entry was a reasonable continuation of the original search, not a new and separate one. Ibid.; accord State v. Hai Kim Nguyen, 419 N.J. Super. 413, 427 (App. Div. 2011) (upholding a second search of the roof of a car "within a short time after the original search" as a reasonable continuation); see also Michigan v. Tyler, 436 U.S. 499, 511 (1978) (finding that arson investigators who left the scene at 4 a.m. because of darkness, steam, and

smoke could continue their lawful investigation and seize evidence shortly after daylight).

The reasonable continuation doctrine does not apply here. Law enforcement would not be returning to continue or complete a single search that had been interrupted. Instead, the CDWs seek newly created evidence from Facebook every 15 minutes for the next 30 days.

VII.

Although no court has addressed an application like this one, today's ruling appears to align with practices elsewhere. According to Facebook, it "has received thousands of requests from law enforcement for contents of prospective communications," and "access is obtained via a wiretap order" "in every other jurisdiction." Microsoft and Google, as friends of the court, advise that law enforcement in 2021 made more than 140,000 requests for user data, including more than 25,000 for content information, "[b]ut just 16 of those requests were for ongoing, prospective surveillance of electronic communications, and all of those took the form of wiretap orders."

The arguments presented do not identify any federal or state jurisdictions, other than New Jersey, which have sought prospective electronic communications based on a search warrant.

## VIII.

For the reasons outlined above, we reverse the judgment of the Appellate Division and quash the parts of the CDWs that direct Facebook to provide prospective electronic communications.

JUSTICES PATTERSON, SOLOMON, PIERRE-LOUIS, and WAINER APTER join in CHIEF JUSTICE RABNER's opinion. JUSTICE FASCIALE and JUDGE SABATINO (temporarily assigned) did not participate.