RECORD IMPOUNDED

NOT FOR PUBLICATION WITHOUT THE APPROVAL
OF THE APPELLATE DIVISION

SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-3350-20
A-0119-21

FACEBOOK, INC.,

Plaintiff-Respondent,

v.

STATE OF NEW JERSEY,

Defendant-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.

APPROVED FOR PUBLICATION

April 4, 2022

APPELLATE DIVISION

Argued January 31, 2022 – Decided April 4, 2022

Before Judges Sabatino, Rothstadt and Mayer.

On appeal from the interlocutory orders of the Superior Court of New Jersey, Law Division, Atlantic County, Warrant No. 1527-CDW-21 and Mercer County, Warrant No. 1311-CDW-21.

Sarah C. Hunt, Deputy Attorney General, argued the cause for appellant State of New Jersey (Andrew J.

Bruck, Acting Attorney General, attorney; Sarah C. Hunt, of counsel and on the brief).

Seth P. Waxman (Wilmer Cutler Pickering Hale and Dorr LLP) of the District of Columbia bar, admitted pro hac vice, argued the cause for respondent Facebook Inc. (Javerbaum, Wurgaft, Hicks, Kahn, Wikstrom & Sinins, PC, Seth P. Waxman, John K. Roche (Perkins Coie, LLP) of the District of Columbia and Virginia bars, admitted pro hac vice, Mikella M. Hurley (Perkins Coie, LLP) of the District of Columbia and New York bars, admitted pro hac vice, Ronald C. Machen and Catherine M.A. Carroll (Wilmer Cutler Pickering Hale and Dorr LLP) of the District of Columbia bar, and George P. Varghese, (Wilmer Cutler Pickering Hale and Dorr LLP) of the Massachusetts bar admitted pro hac vice, attorneys; Rubin Sinins, Seth P. Waxman, Ronald C. Machen, Catherine M.A. Carroll, John K. Roche, Mikella M. Hurley, and George P. Varghese, on the brief).

The opinion of the court was delivered by

ROTHSTADT, J.A.D.

In these two appeals, which we calendared back to back and have consolidated for the purpose of writing one opinion, we are asked to determine as a matter of first impression whether communication data warrants (CDWs) or, conversely, wiretap orders had to be served on Facebook, Inc. n/k/a Meta Platforms, Inc. (Facebook) in order for law enforcement officers to secure prospective electronically stored information from two of Facebook's users' accounts as part of separate ongoing criminal investigations. For the reasons

stated in this opinion, we conclude that only the CDWs and not wiretap orders were required, where, as here, the data sought was from information that would be stored by Facebook as compared to simultaneous transmission of information through interception. However, we also conclude the CDWs relied upon in these two matters were too lengthy in duration under our state's warrant procedures, and therefore require modification, as discussed herein.

The appeals arise from orders entered by two Law Division judges who quashed, in part, separate CDWs in these unrelated matters in response to Facebook's motions. Both judges determined that wiretap orders, rather than CDWs, were required to compel Facebook to turn over information it would collect and store prospectively from two of its users' accounts, without any notice to the individuals who are subjects of the investigations. While we conclude that such orders were not required, we affirm for other reasons,[1] with a significant temporal modification explained herein. We do so with the understanding that our determination is without prejudice to the Facebook account users' privacy claims should they be asserted in the future.

[1] "[B]ecause an appeal is taken from a trial court's ruling rather than reasons for the ruling, [we] may rely on grounds other than those upon which the trial court relied" when, as here, that ruling has been challenged. State v. Adubato, 420 N.J. Super. 167, 176 (App. Div. 2011).

I.

Warrants and the Trial Court Proceedings

At the outset, we summarize the proceedings before the two motion judges, one in the Atlantic vicinage (A-3350-20) and the other in Mercer (A-0119-21). According to the State, the Atlantic application for the CDW[2] established "probable cause for believing that the said Facebook account believed to be used by ["Anthony"[3]] . . . and other as yet unidentified individuals, will provide evidence of, tend to show violations of, and identify individuals engaged in" drug distribution crimes, contrary to N.J.S.A. 2C:35-5(a)(1), recruitment to join a street gang, contrary to N.J.S.A. 2C:33-28, gang criminality, contrary to N.J.S.A. 2C:33-29, promotion of organized street crime, contrary to N.J.S.A. 2C:33-30, and conspiracy to commit each of these, contrary to N.J.S.A. 2C:5-2.

Similar to the Atlantic CDW, the State contends the Mercer CDW application demonstrated "probable cause for believing that" "Maurice," the Facebook user, "and other individuals," who are not specified, "are engaging in,

[2] The sworn affidavits submitted in support of the CDWs are not in the record.

[3] We refer to the account holders by pseudonyms to protect their privacy and to maintain the confidentiality of the investigation. See R. 1:38-3(c)(10) and 3:5-4. The account holders are not parties in these cases.

and are committing, have committed, and are about to commit" Chapter 35 drug distribution offenses, including N.J.S.A. 2C:35-5, N.J.S.A. 2C:35-10, and a conspiracy to violate both, contrary to N.J.S.A. 2C:5-2. Unlike the Atlantic CDW, the Mercer warrant also stated, "[t]he Captioned Facebook Account has been and continues to be used" by the target of the search "to facilitate the commission of the specified crimes."

Based on the State's applications, which were filed in March 2021 by the Atlantic County Sheriff's Office in Atlantic and a State Trooper in Mercer, separate judges issued two CDWs directed to Facebook. Both CDWs sought substantially the same types of data from Facebook, which included the contents of electronic communications, location data, and basic subscriber information. However, only the contents of stored electronic communications are at issue in this appeal.

The Atlantic CDW directed Facebook to disclose, among other things, the contents of electronic communications from a Facebook account controlled by the user identified as Anthony, from January 1, 2021, through the duration of the order—thirty days after the CDW's issuance. The Mercer CDW directed Facebook to disclose to the State, among other things, "the contents of stored electronic communication" concerning a user identified as Maurice from

December 1, 2020, through the duration of the order—thirty days after its issuance. Included in "the contents of stored electronic communications," were images, videos, audio files, posts, comments, histories, and the contents of all private messages in all message folders, including inbox, sent, chat messenger, and trash folders,[4] dating back to January 1, 2021(with respect to the Atlantic CDW) and December 1, 2020 (as to the CDW from Mercer) "through the duration of th[e] order" with respect to both.

The warrants also provided for "real-time" access to such communications via creation of a "cloned," "ghost," or "active duplicate account" to be linked to an account or electronic mailbox exclusively controlled by the New Jersey State Police or other law enforcement agencies assisting with the investigation. Both warrants further directed the "installation and operation" of duplicate accounts used to obtain access to these communications that "shall begin and terminate as soon as practicable, and continue for a period of 30 days," during which time the "devices [could] be utilized 24 hours a day . . . Monday through Sunday."

[4] The Atlantic CDW, but not Mercer's, also sought "stories," "profiles," and "billing records." The CDW described "stories" as "temporary videos that users post that can be accessed by clicking on the user's profile photograph." A "profile" ordinarily contains the same types of data already captured by the definition of stored electronic communications, discussed infra. See Oracle Am., Inc. v. Google Inc., 172 F. Supp. 3d 1100, 1105 (N.D. Cal. 2016) (discussing the data contained within typical Facebook profile).

The Atlantic CDW, but not the Mercer CDW, specified that the "real-time" data so obtained and stored on servers must be "provided to law enforcement officials in approximately 15-minute intervals." In its brief, the State represents that the 15-minute interval procedure had been its practice since at least February 2020, and that its omission from the Mercer CDW was error.

In total, the CDWs compelled the ongoing disclosure of prospective electronic communications for thirty consecutive days, and the immediate disclosure of at least twice as many days' worth of historical communications—seventy-four days in the Atlantic CDW; sixty-three days in Mercer.

Both CDWs ordered Facebook not to disclose the existence of the investigation to the subscribers. While the Mercer CDW's nondisclosure component was to expire in 180 days, the Atlantic CDW's nondisclosure order would continue indefinitely "until further order of th[e] [c]ourt," though terminating when the investigation ends. The Atlantic CDW frames the notice issue as precluding Facebook from providing "notice to anyone involved with the account or any of the data, messages, and content intercepted," whereas the Mercer CDW contains no form of the term "intercept." (Emphasis added).

Facebook partially complied with both CDWs, providing all requested historical electronic communications on the targets' accounts that were stored

on its servers as of the date the CDWs issued, as well as non-content communications, such as, among other things, location information, that occurred during the thirty-day period following issuance of the CDWs. What Facebook declined to do, in each case, was provide the contents of any prospective electronic communications, which, again, are the only electronic communications at issue in this appeal.

The Trial Courts' Rulings

Facebook filed a motion to quash in each vicinage. In response, the two judges entered orders quashing the portions of the CDWs with which Facebook had not complied; the Atlantic judge did so on May 6, 2021, and the Mercer judge on June 25, 2021. In each case, the judge partially quashed the CDWs to the extent they compelled disclosure of the contents of prospective communications. The judges found the future disclosures tantamount to electronic surveillance, necessitating a wiretap order, rather than an ordinary search warrant.

With respect to the Atlantic CDW, the motion judge observed that the Fourth Amendment grants every citizen the right "to enjoy privacy in their communications," and framed the search and seizure issue as "whether the State has a right to intrude on that privacy." Because the CDW compelled disclosure

of the prospective contents of communications, that authorization should be viewed more "stringently" than customer or subscriber records, and had to "comply with constitutional requirements." As the CDW sought "information that is in the future," the surveillance was "tantamount to eavesdropping" and "an interception," notwithstanding the fifteen-minute delay in the prospective disclosures. The length of the delay did not matter, because "[i]t's in the future," the court held, which meant "there has to be a required showing and a time limit." Because the CDW compelled "a series of intrusions" the State needed to meet "the heightened protections" required under the federal and state wiretap acts. Accordingly, the Atlantic judge partially granted the motion to quash to the extent it compelled disclosures of prospective communications.

Similarly, the Mercer motion judge held at the outset that "[e]lectronic surveillance constitutes a search fully protected by the safeguards of the Fourth Amendment." The judge declined to construe the term "intercept" as "limited solely to . . . instantaneous transmission," opting instead to apply the term to the "ongoing prospective acquisition of content of the user's electronic communications." The judge explained that the CDW sought to obtain electronic communications "in real[-]time," notwithstanding the fifteen-minute delay, which, in the judge's view, was "an inherent part of the transmission

process," based on Facebook's representation "that their systems [were] incapable of providing perfectly simultaneous real[-]time access."

Relying on the Seventh Circuit's decision in United States v. Szymuszkiewicz, 622 F.3d 701, 705-06 (7th Cir. 2010), and the First Circuit's decision in United States v. Councilman, 418 F.3d 67, 71 (1st Cir. 2005), the Mercer judge held that "when there is a delay inherent in the transmission of an electronic communication that involves a brief [storage] period . . . before it can possibly be intercepted . . . an interception can occur after an electronic communication is held briefly in electronic storage during its transmission," as would be the case with the fifteen-minute delays. The judge held "placing of the electronic communications on Facebook servers prior to the dissemination [wa]s intrinsic to the transmission process."

Like the Atlantic motion judge, the Mercer judge was also concerned with the thirty-day length of the CDW because it raised "legitimate concerns as it [was] a prolonged period of intrusion on an individual's privacy." The order to quash the Mercer CDW was, like the Atlantic order, limited to the compelled disclosures of the contents of prospective electronic communications generated after issuance of the CDW.

II.

A.

After the orders were entered, the State moved for leave to appeal, which we granted in both cases. On appeal, the State's sole legal argument is that the motion judges erred by granting Facebook's motions to partially quash the CDWs.

The State's Clarified Demand for Stored and To-Be-Stored Data Up to 30 Days

At oral argument before us, the State clarified it does not seek the contemporaneous transmission of the account holders' Facebook information, despite the language contained in the CDWs that included the State being given "real-time" access through "cloned" or "ghost" or "duplicate" accounts. According to the State, Facebook historically required that language before it would comply with the CDWs. Through the warrants, the State seeks to obtain, on an ongoing basis, information that has been stored by Facebook through the date of service of the warrant and that which Facebook will store in the future for a period of thirty days.

Despite the State's confirmation that it does not seek to intercept information in "real-time," Facebook contends that there is no federal or state legal authority to allow "the State to obtain the contents of communications that have not yet occurred," without a wiretap order. Doing so "would allow law

enforcement to obtain all prospective communications within minutes after they are stored, on an ongoing basis, for an indefinite period of time, based solely on a warrant" that was issued upon a showing of probable cause that existed at an earlier time. It is undisputed that if the State must secure a wiretap order, it will have to meet a higher burden relating to its need for a wiretap to secure the information it seeks.

Based on that framing of the issue before us, we consider under what parameters, if any, the State can secure through CDWs not only historically stored electronic information, but also later stored information.

Our Scope of Review

We initially observe that as these matters do not involve any disputed facts, and call for statutory and constitutional interpretation, our review is de novo. State v. Hawkins, 461 N.J. Super. 556, 560 (App. Div. 2019). Based on our de novo review of the applicable principles of law, we conclude that prospective information can be obtained through a CDW, but only for a limited amount of time, as contemplated by our statutes and court rules. As discussed infra, we determine that limit by relying upon our court rules as they relate to execution of warrants generally.

B.

Salient Differences Between CDWs and Wiretap Orders

The present appeal highlights the different burdens law enforcement must satisfy before being able to secure a CDW or wiretap order. Succinctly, a CDW is markedly different from a wiretap order. State v. Finesmith, 408 N.J. Super. 206, 211-12 (App. Div. 2009). "A wiretap order permits the interception by law enforcement of a communication contemporaneous with the transmission while a CDW is directed to acquisition of communications in post-transmission electronic storage kept by an electronic communication service [(ECS)] or remote computing service [(RCS)] for reasons of backup protections for the communication." Ibid. (emphasis added). "By definition, an electronic communication in storage cannot be 'intercepted' because it is not contemporaneous with the transmission." Id. at 212.

In In re Application of State for Communications Data Warrants to Obtain the Contents of Stored Communications from Twitter, Inc. (In re CDWs), 448 N.J. Super. 471 (App. Div. 2017), we held that "the audio portions of the videos and video messages held in the accounts by Twitter are 'electronic communications' under the [New Jersey Wiretapping and Electronic Surveillance Control Act" (NJWESCA), N.J.S.A. 2A:156A-1 to -37], in electronic storage and accessible to the State through the CDWs issued by the

Law Division judge, as compared to interception of "electronic communications in transmission." Id. at 485-86. In reaching our holding, we summarized as follows the different burdens of proof the State must satisfy to obtain a wiretap order or a CDW:

> The State may apply ex parte to designated judges for "an order authorizing the interception of a wire, or electronic or oral communication . . . when such interception may provide evidence of the commission of" certain enumerated crimes. N.J.S.A. 2A:156A-8. However, the State must shoulder a heavy burden before it may "intercept" a communication:
>
> > In part, the judge must find probable cause to believe that
> >
> > > a. The person whose communication is to be intercepted is engaging or was engaged over a period of time as a part of a continuing criminal activity or is committing, has or had committed or is about to commit an [enumerated] offense . . . ;
> > >
> > > b. Particular communications concerning such offense may be obtained through such interception; [and]
> > >
> > > c. Normal investigative procedures with respect to such offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ.

> [State v. Ates, 217 N.J. 253, 266-267 (2014) (alterations in original) (quoting N.J.S.A. 2A:156A-10(a) to (c)).]

The Amendment also created a new crime under the Act. N.J.S.A. 2A:156A-27 makes it unlawful to "knowingly . . . obtain[] . . . access to a wire or electronic communication while that communication is in electronic storage." With limited exceptions, an electronic communication service "shall not knowingly divulge . . . the contents of a communication while in electronic storage . . . ." N.J.S.A. 2A:156A-28(a)(1).

One such exception permits disclosure to law enforcement "of the contents of an electronic communication," but not a wire communication, "without notice to the subscriber . . . if the law enforcement agency obtains a warrant[,]" i.e., a CDW. N.J.S.A. 2A:156A-29(a)(5). We have previously held

> a CDW is not subject to the more restrictive procedures and enhanced protections of the . . . Act, which include a showing of necessity because normal investigative procedures have failed, N.J.S.A. 2A:156A-10. By contrast, N.J.S.A. 2A:156A-29(a) requires only that a law enforcement agency obtain a warrant upon a showing of probable cause.
>
> [Finesmith, 408 N.J. Super. at 212.]

Additionally, unlike a wiretap order which may only be issued to intercept evidence of the commission of certain crimes, N.J.S.A. 2A:156A-8, a CDW may be

> obtained without regard to the nature of the crime being investigated.
>
> [In re CDWs, 448 N.J. Super. at 476-78 (emphases omitted) (footnotes omitted) (quoting Ates, 217 N.J. at 266-67, and Finesmith, 408 N.J. Super. at 212).]

Moreover, if issued, a wiretap order requires that "[e]very interception . . . is subject to minimization, N.J.S.A. 2A:156A-12(f), requiring the State to terminate 'as soon as practicable,' any unnecessary interception." Id. at 482 n.8.

State and Federal Statutes

As discussed in more detail infra, separate state and federal laws restrict the issuance of CDWs and wiretap orders under limited circumstances and subject to certain conditions.[5] In order to understand the concerns those laws are meant to address, we briefly turn our attention to the fundamental privacy

[5] Where the federal and state statutes overlap, we look to the federal court for guidance. As we have explained:

> Although the [NJWESCA] is "more restrictive than the federal act in some respects," we have recognized that "when sections of the federal and state acts are substantially similar in language, it is appropriate to conclude that our Legislature's 'intent in enacting the sections of the . . . Act . . . was simply to follow the federal act.'" Interpretations of the federal act, therefore, provide additional guidance in construing similar provisions of the NJWESCA.
>
> [In re CDWs, 448 N.J. Super. at 479-80.]

rights that warrant constitutional protection from government searches, including through the use of wiretaps, which warrant the application of higher standards for the interception of an individual's prospective communications with others on an ongoing basis as compared to obtaining historically stored material.

Constitutional Limitations

The Fourth Amendment of the United States, incorporated in all States through the Fourteenth Amendment, Mapp v. Ohio, 367 U.S. 643, 655 (1961), provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no [w]arrants shall issue, but upon probable cause, supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
>
> [U.S. Const. amend. IV.]

The New Jersey Constitution provides the same protections in nearly identical language. N.J. Const. art. I, ¶ 7.

"The Fourth Amendment prohibits a general warrant." United States v. Zimmerman, 277 F.3d 426, 432 (3d Cir. 2002). Lawful searches and seizures must be limited to particular items. To satisfy the Fourth Amendment, a search

warrant "must . . . describe the things to be seized with sufficient particularity and be 'no broader than the probable cause on which it is based.'" Ibid. (quoting United States v. Weber, 923 F.2d 1338, 1342 (9th Cir. 1991)).

Fourth Amendment protections extend to personal conversations. "The right of privacy -- the right to be free from government officials arbitrarily prying into our personal conversations -- is one of the preeminent rights in our constitutional hierarchy." State v. McQueen, 248 N.J. 26, 31 (2021). "[I]t has been an established principle, at least since the Supreme Court's decision in Katz v. United States, [389 U.S. 347, 361-62 (1967) (Harlan, J., concurring),] that the Fourth Amendment protects individuals from intrusions upon their private electronic conversations." R.S. ex rel. S.S. v. Minnewaska Area Sch. Dist. No. 2149, 894 F. Supp. 2d 1128, 1142 (D. Minn. 2012). This protection extends to "not only physical searches but also electronic interception of phone conversations." State v. Feliciano, 224 N.J. 351, 367 (2016).

In 1967, in two "landmark" cases, Berger v. New York, 388 U.S. 41, 54 (1967) and Katz, 389 U.S. at 348, the United States Supreme Court applied Fourth Amendment limitations upon searches that employed electronic surveillance, specifically, "phone conversations," to "safeguard individual privacy rights in this area." Ates, 217 N.J. at 266. The Fourth Amendment's

application to "the area of electronic surveillance" of private conversations remains governed by the constitutional principles espoused in the Supreme Court's "seminal opinions in Katz and Berger." Feliciano, 224 N.J. at 367.

In Berger, the Court held that a New York statute's "blanket grant of permission to eavesdrop" lacked "adequate judicial supervision or protective procedures," in part because the two-month, court-ordered eavesdropping period allowed under the statute was "the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause." 388 U.S. at 59. It also authorized two-month extensions of the surveillance window premised only on the "public interest," which could be satisfied by reasserting the original grounds for probable cause, without showing "present probable cause for the continuance of the eavesdrop." Ibid. The statute "place[d] no termination date on the eavesdrop once the conversation sought [wa]s seized," leaving it "entirely in the discretion of the officer" whether to continue the surveillance. Id. at 59-60.

Katz, 389 U.S. at 348, also involved electronic surveillance. FBI agents, without obtaining a warrant, installed an electronic recording device that captured six electronic recordings of an individual using a publicly accessible telephone booth to illegally transmit gambling information. Ibid. The Court

held that "electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied," which was "a 'search and seizure' within the meaning of the Fourth Amendment" that needed a warrant to justify it. Id. at 353. Echoing Berger, the Katz majority held, "[b]ypassing a neutral predetermination of the scope of a search" left the subjects of the surveillance "secure from Fourth Amendment violations 'only in the discretion of the police,'" and violated our constitutional structure. Id. at 358-59 (quoting Beck v. Ohio, 379 U.S. 89, 97 (1964)).

C.

Further Statutory Developments

Against that backdrop, one year after 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 2522, which aimed to "define on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized" and "to prohibit any unauthorized interception of such communications, and the use of the contents thereof in evidence." Pub. L. No. 90-351, § 801(b), 82 Stat. 197 (1968). "Title III established minimum standards for federal and state law enforcement officials

to follow when seeking to intercept wire, oral, and electronic communications." Ates, 217 N.J. at 266 (citing 18 U.S.C.A. 2516(2)).

Later that same year, New Jersey enacted the NJWESCA modeled on the Federal Wiretap Act. L. 1968, c. 409, §§1 to 28; Ates, 217 N.J. at 266. The purpose of the state Act was to "protect[ ] the privacy of individuals," and to "control[ ] intrusive police activity." State v. Toth, 354 N.J. Super. 13, 21 (App. Div. 2002). Our Supreme Court has held that "[t]he Act must be strictly construed to safeguard an individual's right to privacy." Ates, 217 N.J. at 268.

Under both statutes, any person who "intentionally," under the federal law, or "purposely" in New Jersey, "discloses, or endeavors to disclose . . . the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic[6] communication" shall be subject to a fine or criminal imprisonment, or both.[7] 18 U.S.C. § 2511(1); N.J.S.A. 2A:156A-3. In New

[6] "[E]lectronic" communication was added to this group in the federal law in 1986, and in the NJWESCA in 1993. Pub. L. No. 99-508, §§ 101 to 111, 100 Stat. at 1849; L. 1993, c. 29, § 1.

[7] The statutes also make violators subject to civil suit. 18 U.S.C. § 2511(1); N.J.S.A. 2A:156A-24.

Jersey, the person "shall be guilty of a crime of the third-degree." N.J.S.A. 2A:156A-3.

In accord with Katz, both Acts allow qualified law enforcement officials to obtain from a judge with appropriate jurisdiction an ex parte order "authorizing . . . the interception of wire or oral communications" when it "may provide evidence" that would aid in the investigation of any of a series of specified criminal offenses. 18 U.S.C. § 2516(1)(g); N.J.S.A. 2A:156A-8. "Intercept," is defined in both statutes as "the aural or other[8] acquisition of the contents of any wire, electronic,[9] or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4); N.J.S.A. 2A:156A-2(c).

In accord with Berger, the federal and state Acts further set forth procedures law enforcement officers must follow when seeking such applications. Among other things, the statutes mandate that affiants on whose sworn oaths wiretap orders rest must give a "particular" description of the "type

---

8 As enacted, the statutes applied strictly to "aural acquisition," Pub. L. No. 90-351, § 802, 82 Stat. at 212; L. 1968, c. 409, § 2, but were later expanded.

9 "Electronic" was added in the 1986 amendments to the Federal Wiretap Act, Pub. L. 99-308, § 101(a)(1)(D), 100 Stat. 449, and in the 1993 amendments to the State Wiretap Act, L. 1993, c. 29, § 1.

of communication to be intercepted" and a factual statement demonstrating that other investigative techniques had failed, were "unlikely to succeed," or were "dangerous." 18 U.S.C. § 2518(1)(b)(iii), (c); N.J.S.A. 2A:156A-9(c)(3), (6).

These and similar mandatory procedures were designed to bring electronic eavesdropping by law enforcement within the constitutional confines established in Berger and Katz the previous year. See State v. Minter, 116 N.J. 269, 274-75 (1989) ("The [Federal Wiretap Act] . . . responded to the concerns raised in Berger and Katz by creating a limited system of wire surveillance and electronic eavesdropping within the framework of the [F]ourth [A]mendment and the guidelines of Berger and Katz.").

D.

More Statutory Changes

Eighteen years later, Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510 to 2521. Pub. L. No. 99-508, 100 Stat. 1848 (1986). Title I amended the Federal Wiretap Act, modifying certain definitions and adding provisions concerning mobile tracking devices. §§ 101 to 111, 100 Stat. at 1848-59. Title II was referred to as the Stored Wire and Electronic Communications and Transactional Records Access Act (SCA), a new chapter, codified at 18 U.S.C. §§ 2701 to 2711. Pub. L. No. 99-508, §§ 201 to 202, 100 Stat. at 1860-68. Title III, codified at 18 U.S.C. §§ 3121 to 3127, concerned "pen registers" and "trap and trace" devices.[10] Pub. L. No. 99-508, §§ 301 to 302, 100 Stat. at 1868-73.

Seven years after the federal amendments, in 1993, the New Jersey Legislature amended its own statutory scheme to substantially conform state law

[10] "A 'pen register' is a device that records the numbers dialed for outgoing calls made from the target. A trap and trace device captures the numbers of calls made to the target phone." In re Application for Pen Reg. & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 752 (S.D. Tex. 2005) (footnote omitted).

to the ECPA.[11] N.J.S.A. 2A:156-27 to -34. The State Legislature, like Congress, altered the definition of "intercept" to include the acquisition of "the contents of any . . . electronic communication" in addition to "any wire or oral communication." 18 U.S.C. § 2510(4); N.J.S.A. 2A:156A-2(c).[12]

The federal and state statutes both define "electronic communication" to include "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, photoelectronic or photo optical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12); N.J.S.A. 2A:156A-2(m). "[C]ontents" of electronic communications include "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8); N.J.S.A. 2A:156A-2(g). "Electronic storage" means, "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," as well as "any storage of such communication

[11] The NJWESCA "was modeled after Title III of the [Federal Wiretap] Act, 18 U.S.C.A. §§ 2510 to 2520, . . . and must be strictly construed to safeguard an individual's right to privacy." In re CDWs, 448 N.J. Super. at 479 (internal quotation marks and citations omitted).

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

The SCA and the NJWESCA, provide different standards for the disclosure of stored electronic records depending on whether the person or entity doing the disclosing is an ECS or an RCS. The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. § 2510(15), and an RCS as a service providing users with "computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2). The NJWESCA defines the terms substantially similarly. N.J.S.A. 2A:156A-2(p), (s). However, when a government entity[13] seeks to compel disclosure of the contents of electronic communications without providing notice to the subscriber or customer, the significance of the distinction between ECS and RCS providers erodes.

[13] One distinction between the federal and state statutes pertains to the nature of the entity that is compelling disclosures. While the SCA broadly concerns records sought by any "governmental entity," 18 U.S.C. § 2703(c)(B), the NJWESCA is limited to "[a] law enforcement agency, but no other governmental entity." N.J.S.A. 2A:156A-29(a). As the governmental entities here were both law enforcement agencies, this distinction is immaterial in these cases.

Under subsection (a) of 18 U.S.C. § 2703, "governmental entit[ies] may require the disclosure by a provider of [ECS] of the contents of a wire or electronic communication, that is in electronic storage in an [ECS] for one hundred and eighty days or less, only pursuant to a warrant . . . issued using State warrant procedures," in state court matters. 18 U.S.C. § 2703(a). For communications in storage longer than that, subsection (b), pertaining to RCS providers, controls. Similarly, under subsection (b), without notice, disclosure is only available "if the governmental entity obtains a warrant . . . in the case of a State court, issued using State warrant procedures." 18 U.S.C. § 2703(b)(1)(A). In language more direct than the federal statute, but amounting to the same thing, the New Jersey statute provides that, with respect to both ECS and RCS providers, "[a] law enforcement agency . . . may require the disclosure by a provider . . . of the contents of an electronic communication without notice to the subscriber or the customer if the law enforcement agency obtains a warrant." N.J.S.A. 2A:156A-29(a). Unlike the federal statute, there is no qualifier in the text of the NJWESCA requiring that the electronic communication, the disclosure of which is compelled under the search warrant, be "in electronic storage." Ibid.

III.

A.

The State's Contentions of Error

With that understanding of the federal and state laws in this area, we turn to the State's contentions on appeal.

On appeal from both orders, the State principally argues that the judges erred by mistakenly holding that the compelled disclosures of the contents of prospective communications from electronic storage after initial transmission would constitute "interceptions" under the wiretap acts. In the State's view, "an interception occurs only when the content of the communication is acquired contemporaneously with its transmission," in "real-time," which does not apply to the searches and seizures here. These prospective electronic communications are not contemporaneous with transmission, the State notes, since the CDWs required them to be sent to the State every fifteen minutes "as part of the snapshot of the user's account--a process wholly unrelated to the messages' transmission." The wiretap acts are not concerned with the "acquisition of electronic communications from storage, no matter how brief that storage may be," under the State's construction.

The State maintains that because no wiretap order was needed, the issue was governed by the SCA and by the NJWESCA's warrant provisions applicable to electronically stored information. Congress intended for the SCA to apply to the acquisition of the contents of any communications obtained from electronic storage, regardless of whether the coming to rest of the communications in storage occurred "before or after the issuance of process." The SCA requires only a search warrant based on probable cause to compel disclosure of "a communication that has come to rest in storage . . . so long as the temporary, intermediate storage is 'incidental to'--i.e., not an essential part of--the communication's transmission from its point of origin to its point of reception." Because Congress, and our own Legislature, determined the "acquisition of electronic communications from electronic storage does not implicate the same privacy concerns as the real-time interception," those legislative judgments should be respected.

The Atlantic judge, per the State, "mistakenly focused on the timing of the acquisition vis-à-vis the issuance of the CDW" in "conclud[ing] that the acquisition of any communication transmitted after the issuance of the CDW[] . . . '[wa]s tantamount to eavesdropping,'" and thereby required a wiretap order. In so holding, the judge failed to recognize the contemporaneity

component of the wiretap acts, instead focusing on the fact that the CDW sought prospective communications, which was irrelevant. Where there was no anticipated interception contemporaneous with transmission, no wiretap order was needed.

As to the Mercer judge, despite "correctly recogniz[ing]" that Facebook was not even capable of granting "the State real-time access to a user's communications," the judge nevertheless "mistakenly concluded" that the contemporaneity requirement could be "satisfied by the acquisition of a communication from electronic storage, potentially as long as fifteen minutes later." Instead of "looking at the transmission from the point of origin to the point of reception"—the State's interpretation of the wiretap acts—the judge instead looked to the transmission from Facebook to law enforcement in deciding the contemporaneity requirement was satisfied.

B.

The Turnover of Stored and Prospectively Stored Electronic Information Is Not An "Interception"

The nature of the arguments raised by the State requires us to consider the intention of the Legislature when it enacted the NJWESCA in order to determine

if the subject CDWs' requirement for transmittal of prospective electronically stored information violated the Legislature's will. We conclude it did not.

"The overriding goal" of statutory interpretation "is to determine . . . the intent of the Legislature, and to give effect to that intent." State v. Hudson, 209 N.J. 513, 529 (2012). "The inquiry thus begins with the language of the statute, and the words chosen by the Legislature should be accorded their ordinary and accustomed meaning." Ibid. Courts should "apply to the statutory terms the generally accepted meaning of the words used by the Legislature," Patel v. N.J. Motor Vehicle Comm'n, 200 N.J. 413, 418 (2009), "read . . . in context with related provisions so as to give sense to the legislation as a whole." DiProspero v. Penn, 183 N.J. 477, 492 (2005).

"If the language leads to a clearly understood result, the judicial inquiry ends without any need to resort to extrinsic sources." Hudson, 209 N.J. at 529. "In other words, extrinsic aids may not be used to create ambiguity when the plain language of the statute itself answers the interpretative question; however, when the statutory language results in more than one reasonable interpretation, then resort may be had to other construction tools . . . in the analysis." Id. at 529-30. When "the Legislature's intent is clear from the statutory language," courts should "apply the law as written." Shelton v. Restaurant.com, Inc., 214

N.J. 419, 429 (2013). However, "extrinsic evidence may be considered when 'a plain reading of the statute leads to an absurd result or if the overall statutory scheme is at odds with the plain language.'" Hardy ex rel. Dowdell v. Abdul-Matin, 198 N.J. 95, 101 (2009) (quoting DiProspero, 183 N.J. at 493).

With these guiding principles in mind, we turn to the NJWESCA requirements for wiretaps. Again, the state and federal Acts preclude the intentional or purposeful interception of any electronic communication, as well as the intentional or purposeful "disclos[ure]" or "use[ ]" of "the contents of any" electronic communication while "knowing . . . that the information was obtained through the interception." 18 U.S.C. § 2511(1); N.J.S.A. 2A:156A-3. The key to whether the electronic communications sought through the CDWs are subject to a wiretap's requirements is: whether the CDWs ordered communications to be "intercept[ed]." Ibid. We conclude they did not.

As already noted, an "[i]ntercept," is "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." 18 U.S.C. § 2510(4); N.J.S.A. 2A:156A-2(c). Although this definition "does not explicitly require that the acquisition of a communication occur contemporaneously with the transmission of the communication . . . courts interpreting this language have uniformly

concluded that an intercept requires contemporaneity." Luis v. Zang, 833 F.3d 619, 627 (6th Cir. 2016); see also Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' under the [Federal Wiretap Act] must occur contemporaneously with transmission."); accord Boudreau v. Lussier, 901 F.3d 65, 77-78 (1st Cir. 2018); Szymuszkiewicz, 622 F.3d at 705-06; 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, 461-62 (5th Cir. 1994); United States v. Reyes, 922 F. Supp. 818, 836 (S.D.N.Y. 1996).

Here, just like we did when we considered the information from Twitter that the State sought through a CDW in In re CDWs, "[w]e [again] agree with the State and the overwhelming federal precedent that holds interception, as defined by the [NJWESCA] and the federal act, contemplates the acquisition of the communication contemporaneously with its transmission." 448 N.J. Super. at 485-86 (emphasis added) (citations omitted). As in that case, "[i]n this case, the State does not seek to access the electronic communications in transmission. Rather, the State seeks to access the electronic communications already in 'electronic storage' on [Facebook's] servers," and those that will be. Ibid.

One textual basis for this interpretation is that the ECPA defines "intercept" as applying to "electronic communications" but does not specifically mention communications in electronic storage. 18 U.S.C. § 2510(4). Since an "electronic communication" refers to "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part," § 2510(12) (emphasis added), "intercept . . . does not apply to the acquisition of electronic signals that are no longer being transferred." Luis, 833 F.3d at 627. Rather, "[o]nce the transmission of the communication has ended, the communication ceases to be a communication at all," and instead "becomes part of 'electronic storage[,]'" at which point "a person cannot 'intercept' the former communication because the term intercept . . . does not apply to electronic storage." Ibid.

An interception "must, in other words, catch the communication 'in flight' before the communication comes to rest and ceases to be a communication." Id. at 627-28. The upshot is that "[t]he level of protection provided stored communications under the SCA is considerably less than that provided communications covered by the [Federal] Wiretap Act[,]" and "the procedures law enforcement must follow to access the contents of stored electronic

communications" are likewise "considerably less burdensome and less restrictive than . . . under the Wiretap Act." Konop, 302 F.3d at 879.

As already mentioned, New Jersey courts have followed this federal precedent regarding the contemporaneity requirement of "intercept" when applying the NJWESCA. Finesmith, 408 N.J. Super. at 212; In re CDWs, 448 N.J. Super. at 485. Several other jurisdictions have as well. See, e.g., Sparks v. Indiana, 100 N.E.3d 715, 720 (Ind. Ct. App. 2018) (where woman discovered on boyfriend's Facebook account "a recording of a conversation that had already taken place," she "did not intercept a communication in transit," but "accessed a communication in storage," and therefore did not violate the Federal Wiretap Act); Ohio v. Poling, 938 N.E.2d 1118, 1123 (Ohio Mun. 2010) (woman's reading and copying of her daughter's received email messages was not an "interception" under the ECPA); Evans v. Evans, 610 S.E.2d 264, 271 (N.C. Ct. App. 2005) (holding extraction of emails stored on and recovered from hard drive of family computer were not "intercepted" contemporaneously with transmission); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 979 (M.D. Tenn. 2008) (finding persuasive an interpretation of "intercept" in Tennessee's Wiretap Act that "unless an e-mail is actually acquired in its split

second transmission over a computer network, it cannot be 'intercepted' as that term is reasonably understood").

To the extent that, in their rulings, the motion judges here held the compelled disclosures of prospective electronically stored communications authorized by the CDWs were "interceptions" under the NJWESCA, those interpretations of that statutory term misapprehended the transmission contemporaneity requirement set by the above precedents and were therefore incorrect.[14] In other words, because, the officers here would have no way to "catch the communication[s]" at issue "in flight," before they "c[a]me[] to rest" in electronic storage on Facebook's servers, the CDWs did not authorize the "interception" of any communications at all, and did not, in that respect, implicate the federal or state Acts. Luis, 833 F.3d at 627-28 (emphasis added); accord Finesmith, 408 N.J. Super. at 212.

Councilman and Szymuszkiewicz do not direct otherwise. Councilman was an appeal from the dismissal of an indictment charging an email provider's employee with intercepting, disclosing, and using the contents of electronic communications, and with "causing a person providing an [ECS] to divulge the

[14] Considering the warrants' language about transmissions through mirrored or ghost accounts accessible by law enforcement, we cannot criticize them for reaching their conclusions.

communications' contents to persons other than the addressees," contrary to 18 U.S.C. § 2511(1)(a) of the Federal Wiretap Act. Councilman, 418 F.3d at 71. To gain a commercial advantage, the defendant in Councilman directed the systems administrator of the email service to modify its mail-delivery agent program to copy messages from a specified domain before the messages reached the clients, and to then store them in a separate mailbox accessible to the defendant. Id. at 70-71. The litigation posture presented no occasion to address "whether the term 'intercept' applies only to acquisitions that occur contemporaneously with the transmission of a message from sender to recipient or, instead, extends to an event that occurs after a message has crossed the finish line of transmission." Id. at 80. Still, the panel noted it was "highly unlikely" that the defendant could show he had not "intercepted" the emails, because they were "acquired while they were still en route to the intended recipients." Ibid. (emphasis added).

Szymuszkiewicz, 622 F.3d at 704, also concerned arguments raised by a criminal defendant charged with violating 18 U.S.C. § 2511(1)(a) of the Federal Wiretap Act. The evidence demonstrated that the defendant created a "rule" on the wiretapping victim's computer, "implemented on the server side," pursuant to which, whenever the victim received an email, the message would first be

routed through the email provider's server, which "retained the message in its own files and dispatched two copies," one for the victim and one for the defendant, "within the same second." Ibid. (emphasis added). The court reasoned, "[t]he copying at the server was the unlawful interception, catching the message 'in flight.'" Ibid.

Here, unlike in Councilman and Szymuszkiewicz, the CDWs did not grant access to the contents of prospective communications on Anthony's and Maurice's Facebook accounts while they were either "en route," or "within the same second," that they were placed on Facebook's servers. Rather, police would not have access until, at earliest, fifteen minutes after any electronic communication's transmission. Though the CDWs compelled Facebook to disclose the entire stored contents of each target's Facebook account for thirty prospective days, that did not make the disclosures contemporaneous with transmission. Luis, 833 F.3d at 627. Rather, once the communications would come to "rest" on Facebook's servers, they would be in "electronic storage," and thereby subject not to the wiretap acts, but to the SCA and the provisions of the NJWESCA that mirror that statute. Ibid.

C.

Constitutional and Other Limitations on Duration

Our determination that a wiretap order was not necessary does not necessarily lead us to conclude that the CDWs issued in the present matters met the requirements of the state NJWESCA or the federal SCA or either the federal or New Jersey constitutions. Our consideration of those issues leads us to conclude that, while the CDWs complied with the NJWESCA to a point, an additional limitation had to be imposed on the duration of the warrants in order to pass constitutional muster and to be in compliance with our court rules.

At the outset, we observe that it cannot be disputed that there is no language in the NJWESCA that expressly bars the production of prospectively stored information by a provider such as Facebook. For that reason, before us, the parties engaged in textual arguments as to why we should or should not read into the Act grounds for allowing through a CDW the release of prospectively stored electronic information or bar its release.

Addressing the language of the applicable statutes, the crux of the textual dispute between Facebook and the State regarding the Federal SCA revolves around what "is" means in Congress's reference to an electronic communication "that is in electronic storage." The State contends that if Congress intended for

"the SCA to apply only to communications in storage at the time a warrant was issued," and not to communications yet to exist, it would have used the same verb tense in 18 U.S.C. § 2703(a) when referring to communications in shorter-term electronic storage, as it did later in the same paragraph when referring to communications in longer-term electronic storage. Specifically, Congress referred to a communication in storage for one hundred and eighty days or less as one "that is in electronic storage in an electronic communications system," while referring to a communication in longer-term storage as one "that has been in electronic storage." Ibid. (emphasis added).

The verb tense difference, the State posits, is because the present tense for short-term electronic storage "includes any communication that is in storage presently or in the future, without any limitation." By contrast, the present perfect tense for longer-term storage refers only to storage "completed by the present time." If Congress intended the SCA to apply only to communications in storage at the time when legal process is issued, as both judges essentially held, the present perfect tense would have sufficed for both shorter and longer-term stored electronic communications. Instead, Congress intended communications in shorter-term storage would include "communications that are in storage presently or come to be in storage in the future," while

communications in longer-term storage would include only communications whose storage had been complete longer than 180 days. In support, the State relies on the federal Dictionary Act's provision stating "unless the context indicates otherwise . . . words used in the present tense include the future as well as the present." 1 U.S.C. § 1. The State claims this proves Congress intended for the statute to apply prospectively to communications that have yet to exist when a warrant issues. Facebook contends the "context" here includes Congress's "comprehensive statutory scheme governing federal surveillance law," which contravenes the State's interpretation of the word "is," particularly because the SCA was intended to be retrospective while Titles I and III of the ECPA were intended to be prospective.

As to the NJWESCA, the language is broader than its federal counterpart, stating, in the future conditional tense, that "[a] law enforcement agency . . . may require the disclosure by a provider . . . of the contents of an electronic communication without notice to the subscriber or the customer if the law enforcement agency obtains a warrant." N.J.S.A. 2A:156A-29(a). Again, absent from that Act, is any qualifying language requiring that the electronic communications ordered to be disclosed by the search warrant to ever be "in electronic storage" in the past, the present, or the future. Inverting the statute

for illustrative purposes, the New Jersey Act simply states: "[I]f the law enforcement agency obtains a warrant," the agency "may require the disclosure . . . of the contents of an electronic communication." Ibid. Implicit in the absence of the "electronic storage" qualifier is that a warrant compels disclosure of the contents of the electronic communications specified in the warrant, regardless of whether they are "in electronic storage" when process is issued. Ibid.

By contrast, subsections (c)(1) and (c)(4) of the NJWESCA, concerning location information, provide, in the present perfect conditional tense, that when, among other possible statutory predicates, a "law enforcement agency" either "has obtained a warrant[,]" or, in the present tense, "believes in good faith that an emergency . . . requires disclosure without delay of information relating to the emergency[,]" the provider to whom the request is made "shall disclose," among other things, "the location information for a subscriber's . . . device." N.J.S.A. 2A:156A-29(c)(1), (4).

Implicit in the clause in (c)(4) that an officer's good-faith present belief in an "emergency" justifies disclosure of location information is that the relevant location information will be prospective to the issuance of process and as near to real-time as possible. After all, it would be illogical to construe (c)(4)

otherwise: allowing officers, during an ongoing emergency, to compel disclosure of only temporally distant, possibly stale location information.

Assuming then that the Legislature used the present perfect tense to allow the compelled disclosures of future communications in subsection (c), it would be incongruous if the same Legislature in the same statute used the future conditional tense to disallow disclosures of future communications in subsection (a). See Borough of N. Haledon v. Bd. of Educ. of Manchester Reg'l High Sch. Dist., Passaic Cnty., 305 N.J. Super. 19, 28 (App. Div. 1997) (discussing canon of statutory interpretation "that statutes dealing with the same subject matter ought to be construed together 'as a unitary and harmonious whole,' . . . so that each may be fully effective" (quoting Clifton v. Passaic Cnty. Bd. of Tax'n, 28 N.J. 411, 421 (1958))). It would also lead to an absurd inversion of the warrant preference, since officers could use (c)(4) to warrantlessly procure real-time location information based only on their subjective discretionary judgment that an emergency exists, but, under Facebook's construction of the NJWESCA as strictly retrospective from the vantage point of when the warrant issues, the officers could not obtain that same information with a warrant.

Similarly, focusing on the federal SCA, the entirety of § 2703 is written in the future conditional tense: i.e., only if something happens in the future

(e.g., police obtain a warrant) or something else may happen later (e.g., police may require disclosure of the contents of stored electronic communications). If "is" is at all ambiguous, the ordinary presumption is to read it to imply "is and will be." 1 U.S.C. § 1. Other than the atypical warrant procedures here, nothing else about the "context" in which "is" appears in § 2703(a) and (b)(1)(A) displaces this default rule. For these reasons, we conclude that neither the NJWESCA nor the SCA categorically bars the disclosure of prospective electronic communications not yet in storage when legal process issues.

Having determined that the NJWESCA does not prevent the turning over of prospectively stored electronic information, the question becomes for what period of time must the provider continue to turn that information over. It is undisputed that neither the federal nor the state Acts make any reference to such a limitation, nor is it disputed that to pass constitutional muster some reasonable limitation is required.

These CDWs in these matters directed in nearly identical language that "execution of this [CDW] shall continue . . . provided that the USER NAME and/or USER ID remain the same," for thirty consecutive days. (Emphasis added). Although warrant procedures generally permit search warrants to constitutionally authorize police to search for and seize evidence that will be in

a specific place only "in the future," see, e.g., Illinois v. Gates, 462 U.S. 213, 225-26 (1983) (upholding a warranted seizure even though items were not at specified location until after warrant issued); State v. Earls, 214 N.J. 564, 588 (2013) (where the Court considered a series of continuous "24/7" intrusions through a tracking system and found that a warrant, an emergency, or some other warrant exception would all be sufficient to alleviate any privacy concerns associated with such ongoing searches and seizures); State v. Mier, 147 N.J. Super. 17, 20 (App. Div. 1977) ("There is no particular constitutional infirmity in the mere fact that a warrant is sought to search for contraband which has not as yet reached the destination described."), there is no state procedure that authorizes warrant execution periods as lengthy as in these CDWs.

Rule 3:5-5(a)'s Ten-Day Limit

Our procedures, to which again federal law defers, see SCA, § 2703(a) and (b)(1)(A) (authorizing the State to compel disclosures of electronic communications in electronic storage without notice to the subscriber or customer only to the extent warrants are "issued using State warrant procedures"), mandate a search warrant "must be executed within 10 days after its issuance." R. 3:5-5(a). Once executed during the ten-day period, any additional warrants must be issued only upon another demonstration of probable

cause. See Berger, 388 U.S. at 54 (rejecting "a series of intrusions, searches, and seizures pursuant to a single showing of probable cause").

Here, the CDWs' arbitrary inclusion of a thirty-day period for repeated execution of the same warrant invalidated the warrants, as the duration allowed law enforcement to accomplish what was tantamount to repeated intrusions based on a single showing of probable cause existing at a particular time. To be sure, the constitutional infirmity here was not that the warrants called for a wiretap or interception of simultaneous communications, but instead was founded upon the length and repeated nature of its execution without additional showings of probable cause.

The compelled disclosures of all prospective contents of electronic communications in a subscriber's social media account on an ongoing basis for more than four weeks authorizes multiple intrusions into private communications based on a single showing of probable cause, and therefore is contrary to the particularity requirement of the Fourth Amendment under Berger, 388 U.S. at 59. For that reason, the CDWs in their present form cannot be enforced as to prospectively stored electronic information.

In 2013, the New Jersey Supreme Court in Earls addressed the disclosure of cell phone users' location to law enforcement and observed that "Law and

practice have evolved in this area in response to changes in technology." 214 N.J. at 588. The same is true today as it relates to the evolving technology surrounding stored electronic information.

The Ten-Day Limitation

In formulating an acceptable constitutional solution to the disclosure of that information, we choose to apply a practical approach to the release of prospective electronically stored communications under a CDW. To remain within the parameters of state warrant procedure, the CDWs can be issued, assuming probable cause is once again established, and served on Facebook requiring that any information identified in the warrant and stored by Facebook during the period up to the day it is served with the warrant must be turned over. In addition, incorporating our state warrant procedures under Rule 3:5-5, going forward, if the State serves a CDW on Facebook for the disclosure of prospective electronic communications, no disclosures may be compelled beyond ten days from the issuance of the warrant. And, Facebook can comply with that requirement by producing the stored information on the day of or after the electronic communications have been stored.

Any further attempt to secure information from prospective time periods must be based upon new CDWs issued on new showings of probable cause. We

believe that this practical approach, which modifies the trial courts' dispositions, is consistent with the federal and state constitutions and our warrant procedures, comports with the applicable statutes, and fairly balances the interests of the parties before us.[15]

All other arguments raised in the parties' briefs either lack sufficient merit to warrant discussion, R. 2:11-3(e)(1)(E), or are unnecessary to reach in light of our disposition.

The orders appealed from are affirmed as modified, without prejudice to the State's ability to reapply to the trial courts for approval of warrants consistent with the limitations set forth in this opinion.

Affirmed as modified.

[15] Again, we are not addressing any claims that might be raised by the users of the Facebook accounts as to the scope of the CDWs as they are not before us nor are the users apparently even aware of the investigations.