

SYLLABUS

(This syllabus is not part of the opinion of the Court. 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 Supreme Court. Please note that, in the interest of brevity, portions of any opinion may not have been summarized.)

State v. Gary Lunsford (075691) (A-61-14)

Argued February 29, 2016 – Decided August 1, 2016

RABNER, C.J., writing for a majority of the Court.

In this appeal, the Court addresses the standard that should apply when the State seeks telephone billing records in connection with a criminal investigation.

The police arrested defendant Gary Lunsford after they executed a search warrant at his home based on suspected criminal activity involving transactions in controlled dangerous substances (CDS). As part of its continuing investigation, the Monmouth County Grand Jury issued a subpoena duces tecum to a wireless telephone service provider requesting subscriber information associated with defendant's cell phone number, which was the contact for the controlled drug buys that led to defendant's arrest. The subpoena sought customer and billing records, as well as call-detail records, which identify the phone numbers of all incoming and outgoing calls as well as the date, time, and duration of those calls (collectively "telephone billing records" or "telephone toll records").

Defendant filed a motion to quash, which the trial court granted, stating that, under State v. Hunt, 91 N.J. 338 (1982), a communications data warrant (CDW), which is the equivalent of a search warrant, is needed to obtain telephone billing records. The Attorney General, who superseded the Monmouth County Prosecutor's Office to litigate the constitutional question raised by the trial court's decision, sought leave to appeal, which the Appellate Division denied. The Court granted leave to appeal. 223 N.J. 159 (2015).

HELD: As a long-standing feature of New Jersey law, telephone billing records are entitled to protection from government access under the State Constitution. Because they reveal details of one's private affairs that are similar to what bank and credit card records disclose, these areas of information should receive the same level of constitutional protection and be available based on a showing of relevance. Direct judicial oversight of the process is required to guard against the possibility of abuse, and in order to obtain a court order requiring production of telephone billing records, the State must present specific and articulable facts to demonstrate that the records are relevant and material to an ongoing criminal investigation.

1. In a series of decisions, the Court has recognized a constitutionally protected right to privacy in various types of personal information. In doing so, the Court has parted company with federal law and relied on the State Constitution. Early case law gave little attention to the question of the appropriate level of protection to safeguard an individual's privacy interest. Later decisions addressed the issue by balancing individual privacy rights with society's interest in investigating and halting criminal activity. The Court examines these cases in order to reconcile the tensions that have developed over time in this area of law. (pp. 9-10)

2. In State v. Hunt, the Court held that defendant had a protectable privacy interest in telephone billing records under the State Constitution, and thereby departed from federal law, which did not recognize a privacy interest in such information. Although the Court did not address the specific procedure required for the State to obtain the information, the Court stated that judicial sanction or a judicial proceeding is necessary. After the decision in Hunt, the Attorney General consistently sought a warrant in order to obtain telephone billing records. Years later, the Court extended the State constitutional protections to billing records for a hotel-room phone, and determined that such records are subject to seizure only on a showing of probable cause and the issuance of a warrant. (pp. 10-16)

3. The Court has also recognized a protectable privacy interest in other information. More particularly, the Court has held that account holders have a reasonable expectation of privacy in their bank and credit card records. The Court rejected the position that a showing of probable cause and a search warrant are necessary to obtain these records, and held that a grand jury subpoena, based on a relevancy standard, is sufficient to protect an individual's

privacy interest in view of law enforcement's legitimate investigatory needs. Similarly, the Court has held that a grand jury subpoena sufficiently protects the privacy interest in utility records and the subscriber information that individuals supply to an internet service provider. However, in State v. Earls, 214 N.J. 564 (2013), the Court returned to the question of privacy in the context of cell-phone location information. There, the Court held that tracking one's location through a cell phone is a more intrusive and revealing invasion into an individual's privacy, and therefore requires that police obtain a warrant based on a showing of probable cause to acquire cell-phone location information. (pp. 16-26)

4. Telephone billing records reveal information about the account holder even though they do not disclose the contents of any communications. Bank account records and credit card statements disclose actual content. All of these records can reveal comparable information, and create similar expectations of privacy. However, the courts have afforded different levels of protection when production of the information is sought. Bank records can be obtained through a grand jury subpoena, upon a finding that the records are relevant. To obtain telephone billing records, the law requires that law enforcement meet a higher threshold and demonstrate probable cause, even though bank records arguably reveal more information than telephone billing records. To address these inconsistent standards, the Court must reconcile an individual's privacy concerns with valid law enforcement aims, including the practical impact of requiring a search warrant based on probable cause. (pp. 26-29)

5. A requirement that the State demonstrate that telephone billing records are relevant to an ongoing criminal investigation in order to obtain the records protects individual privacy rights at stake, and recognizes society's legitimate interest in investigating criminal activities. To require a showing of probable cause would be contrary to both the traditional authority of the grand jury and society's legitimate interest in having officials promptly investigate and interrupt criminal activity. The Legislature previously unanimously amended N.J.S.A. 2A:156A-29(e) of the New Jersey Wiretapping and Electronic Surveillance Control Act (Wiretap Act) to require service providers to disclose telephone records to law enforcement in response to a grand jury subpoena, which requires only a showing that the documents are relevant to the investigation. Because the amendment conflicts with the standard set forth in Hunt and other case law, it has not been followed. However, the amendment reflects the Legislature's view of the protection that a reasonable expectation of privacy requires in this area and is entitled to respectful consideration. Still, the judicial branch has the obligation and the ultimate responsibility to interpret the meaning of the Constitution and the protections it requires. In the end, the Court is guided by the language and history of the New Jersey Constitution. (pp. 29-34)

6. To obtain telephone billing or toll records, the State must apply for a court order under N.J.S.A. 2A:156A-29(e) of the Wiretap Act. As the statute requires, the State must demonstrate specific and articulable facts showing that there are reasonable grounds to believe that the records sought are relevant and material to an ongoing criminal investigation. The requested records must cover a finite period of time which does not extend beyond the date of the order. Judicial review of such ex parte applications will guard against abuse and root out bulk requests for information that are not connected to a criminal investigation. In this matter, the Court affirms the trial court's decision to quash the grand jury subpoena for telephone billing records, and notes that the State may apply for a court order to obtain those records in this case, consistent with the principles discussed in this opinion. (pp. 36-37)

The judgment of the trial court is **AFFIRMED**.

JUSTICE LaVECCHIA, CONCURRING IN PART and DISSENTING IN PART, joined by **JUDGE CUFF (temporarily assigned)**, concurs in the judgment to the extent that it affirms the trial court's decision to quash the grand jury subpoena for telephone billing records. Justice LaVecchia dissents from the portion of the judgment that permits the State to apply for a court order to obtain those records based on the new procedures that the Court outlines in its opinion. Justice LaVecchia expresses the view that State v. Hunt established a warrant requirement for police access to telephone billing records, and that precedent should control this case under a consistent line of cases addressing access by law enforcement to private telephone records.

JUSTICES PATTERSON, FERNANDEZ-VINA and SOLOMON join in CHIEF JUSTICE RABNER's opinion. JUSTICE LaVECCHIA filed a separate, concurring and dissenting opinion in which JUDGE CUFF (temporarily assigned) joins. JUSTICE ALBIN did not participate.

STATE OF NEW JERSEY,

Plaintiff-Appellant,

v.

GARY LUNSFORD,

Defendant-Respondent.

Argued February 29, 2016 - Decided August 1, 2016

On appeal from the Superior Court, Appellate Division.

Ronald Susswein, Assistant Attorney General, argued the cause for appellant (John J. Hoffman, Acting Attorney General of New Jersey, attorney; Mr. Susswein, Claudia Joy Demitro, Ian C. Kennedy, and Jane C. Schuster, Deputy Attorneys General, of counsel and on the briefs).

Dean I. Schneider argued the cause for respondent (Schneider Freiburger, attorneys).

Kevin H. Marino argued the cause for amicus curiae Association of Criminal Defense Lawyers of New Jersey (Marino, Tortorella & Boyle, attorneys; Mr. Marino, John D. Tortorella, and Erez J. Davy, on the brief).

Frank L. Corrado argued the cause for amici curiae American Civil Liberties Union of New Jersey, Brennan Center for Justice, Electronic Frontier Foundation and Office of the Public Defender (Edward L. Barocas, Legal Director, attorney; Mr. Corrado, Alexander R. Shalom, Rubin M. Sinins, and Annabelle M. Steinhacker, on the brief).

CHIEF JUSTICE RABNER delivered the opinion of the Court.

For more than three decades, this Court has departed from federal law and recognized that, under the New Jersey Constitution, individuals have a reasonable expectation of privacy in information they provide to phone companies, banks, and Internet service providers in order to use commercial services. The Court has consistently applied that principle to protect personal information from unrestricted government access. No party in this appeal seeks to disturb that precept, which is a bedrock feature of New Jersey law.

As a general rule, the greater the degree of intrusion into one's private matters by the government, the greater the level of protection that should apply. This appeal asks the Court to revisit the standard that should apply to telephone billing records sought in connection with a criminal investigation. The appeal also highlights inconsistencies in New Jersey's case law on privacy which have developed over time.

Telephone billing records, bank and credit card records, and Internet subscriber information can all reveal intimate details about a person's life. The level of detail disclosed across all of those areas is relatively similar. Yet our case law has set different standards that law enforcement officers must meet to obtain information from those sources. Earlier

decisions, with little analysis, required officials to seek a search warrant supported by probable cause to get access to telephone billing records; among other things, those records disclose the telephone numbers dialed to and from a particular phone but not the content of any conversations. To get access to bank records, though, which reveal the actual content of transactions, officials need only use a grand jury subpoena. A subpoena can be used if the documents are relevant to an ongoing criminal investigation, a lower threshold than probable cause.

When the Court's decisions in the area of privacy rights are read together, they reveal internal inconsistencies. We now attempt to resolve that tension in the law. Because telephone billing records reveal details of one's private affairs that are similar to what bank and credit card records disclose, we conclude that both areas of information should receive the same level of constitutional protection and be available if they are relevant to an ongoing criminal investigation. More intrusive records, like cell-phone location information, are entitled to greater protection and continue to require a search warrant.

To guard against the possibility of abuse in this sensitive area, however, we retain direct judicial oversight of the process and require the State to obtain a court order before it can ask a service provider to turn over telephone billing records. A judge may enter an order if law enforcement

officials offer specific and articulable facts to demonstrate that telephone billing records are relevant and material to an ongoing criminal investigation. See N.J.S.A. 2A:156A-29(e). We believe that this approach not only resolves the tension in existing case law, but also strikes an appropriate balance between legitimate privacy rights of individuals and society's valid interest in investigating and preventing crime.

We therefore agree with the trial court's decision to quash the grand jury subpoena the State served in this case, and direct that the State may apply for a court order to obtain the telephone billing records it seeks.

I.

The police arrested defendant Gary Lunsford after they executed a search warrant at his home on May 15, 2014. As part of a continuing investigation, the Monmouth County Grand Jury issued a subpoena duces tecum on June 19, 2014 to Cellco Partnership, doing business as Verizon Wireless. The subpoena required Verizon to produce telephone records and global positioning system (GPS) data associated with defendant's cell-phone number; the number was the contact for controlled drug buys that provided the basis for the search warrant.

Six weeks later, the grand jury recalled the subpoena and issued a new one that omitted the request for GPS data -- to comply with State v. Earls, 214 N.J. 564 (2013), which requires

a search warrant for cell-phone location information. The new subpoena sought subscriber information for the cell phone, namely, billing and customer records, as well as call-detail records for the two weeks leading up to defendant's arrest. Call-detail information includes the phone numbers dialed out from defendant's cell phone, the phone numbers dialed in to that phone, and the date, time, and duration of those calls. That information is often referred to as "telephone billing records" or "telephone toll records."

The State alerted defense counsel that it was seeking telephone billing records to give defendant the opportunity to move to quash the subpoena. Defendant filed a motion to quash, and the trial court granted the motion on January 16, 2015. In a written opinion, the trial court explained that under State v. Hunt, 91 N.J. 338 (1982), a communications data warrant, the equivalent of a search warrant, is needed to obtain telephone toll records.

The Attorney General, who superseded the Monmouth County Prosecutor's Office to litigate the constitutional question this case raises, sought leave to appeal. The Appellate Division denied the request. The State then filed a motion for leave to appeal with this Court, which we granted. 223 N.J. 159 (2015).

II.

The Attorney General does not dispute that telephone billing records are entitled to protection under the State Constitution. He argues instead that a grand jury subpoena, based on a relevancy standard rather than probable cause, is sufficient to safeguard the privacy rights at stake.

For support, the Attorney General traces the evolution of privacy rights under the State Constitution from Hunt, which addressed telephone billing records, to the present. He asserts that although Hunt found that customers enjoy a reasonable expectation of privacy in telephone billing records, the opinion did not address whether a grand jury subpoena would adequately protect that right. By contrast, the Attorney General contends, more recent case law relating to the privacy rights in bank records, State v. McAllister, 184 N.J. 17 (2005), Internet subscriber information, State v. Reid, 194 N.J. 386 (2008), and cell-phone location information, Earls, supra, 214 N.J. 564, “strongly suggest . . . that a grand jury subpoena is all that is needed.” According to the Attorney General, bank and Internet subscriber records can reveal intimate details about a customer’s private life that compare to the level of information disclosed in telephone billing records; as a result, those areas should be treated similarly under the law. The Attorney

General, therefore, argues that this Court should reconcile Hunt with its more recent opinions.

The Attorney General contends that the grand jury subpoena process works well to protect State constitutional privacy rights, that the law in other jurisdictions does not support sustaining a warrant requirement, and that the legitimate needs of law enforcement offer further support for the use of grand jury subpoenas to obtain telephone billing records. In particular, the Attorney General notes that a probable cause standard delays prosecutors from gathering toll records at an early stage in a criminal investigation and, as a result, lengthens the amount of time needed to conduct criminal investigations.

Defendant argues that Hunt not only found a reasonable expectation of privacy under the State Constitution in telephone billing records but that it also imposed a warrant requirement for the police to obtain those records. Because call-detail records can "paint a picture" of defendant's private life, he maintains that Hunt was correctly decided and should not be overturned. Defendant adds that the Attorney General has not presented any special justification to overturn Hunt.

Defendant also argues that the grand jury subpoena process, guided by a relevancy standard with no judicial oversight, does not adequately protect a citizen's privacy rights. Defendant

claims that a warrant requirement is the only way to guarantee the needed level of protection.

We granted amicus curiae status to (1) the American Civil Liberties Union of New Jersey, the Brennan Center for Justice, the Electronic Frontier Foundation, and the Office of the Public Defender (collectively, the ACLU), which submitted a joint brief, and (2) the Association of Criminal Defense Lawyers of New Jersey (ACDL).

Amici expand upon the arguments defendant raises. They contend that Hunt expressly and correctly imposed a warrant requirement and should not be overturned. The ACLU argues that telephone billing records, particularly when collected in bulk, can reveal intimate private information that only a warrant can adequately protect. The ACDL, likewise, highlights the expansive range of information that call-detail records can reveal. The ACDL also stresses that telephone billing records are quite revealing in the aggregate and pose particular concerns for whistleblowers, journalists, people who seek confidential advice on health issues, and others.

In addition, amici argue that the Attorney General has misread this Court's rulings on privacy. They contend that the privacy interest in telephone billing records recognized in Hunt is of the highest order, and that just because tracking an individual's movements may be more invasive than obtaining

telephone toll, bank, or ISP (Internet service provider) records, it does not logically follow that telephone billing records merit less protection than cell-phone location data or should be treated the same as bank or ISP records.

Finally, amici argue that the grand jury process is controlled by the prosecutor and does not adequately protect the privacy interests involved.

III.

Over the years, this Court has recognized a constitutionally protected right to privacy in various types of information: telephone toll records, bank records, subscriber information provided to an Internet Service Provider, and cell-phone location data. See Hunt, supra, 91 N.J. 338; McAllister, supra, 184 N.J. 17; Reid, supra, 194 N.J. 386; Earls, supra, 214 N.J. 564. In doing so, the Court has parted company with federal law and relied on the State Constitution.¹

Beyond the threshold question of whether a privacy right exists lies another inquiry: what level of protection is appropriate to safeguard an individual's privacy interest? Early case law gave little attention to the second question.

¹ The United States Constitution guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" U.S. Const. amend. IV. Article I, Paragraph 7 of the New Jersey Constitution contains nearly identical language.

Later decisions, dating back a decade, examined the issue by balancing both individual privacy rights and society's interest in investigating and halting criminal activity. Today, we are called upon to assess and reconcile the tension that has developed over time in this area.

A.

The Court's 1982 decision in Hunt marks an important point in the chronology. The case arose out of an investigation into an illegal sports gambling operation. Hunt, supra, 91 N.J. at 341. During the investigation, an informant told the State Police that the defendant conducted a daily gambling business over two telephone lines. Ibid. A detective asked the telephone company for telephone billing records for both numbers for a two-month period, and the company complied. Ibid. The State Police later obtained court orders for a pen register and a wiretap. Id. at 342.

Hunt analyzed with care whether the defendant had a "protectible interest" in telephone billing records under the Federal and State Constitutions. Id. at 342-43. The Court quoted Justice Stewart's observation that a list of dialed telephone numbers "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life." Id. at 347 (quoting Smith v.

Maryland, 442 U.S. 735, 748, 99 S. Ct. 2577, 2584, 61 L. Ed. 2d 220, 231 (1979) (Stewart, J., dissenting)).

Hunt noted that federal case law did not recognize a "legitimate expectation of privacy in information voluntarily turned over to third parties," id. at 343-44, a principle commonly referred to as the "third-party doctrine." As a result, individuals have no expectation of privacy under federal law in pen register information (a list of local and long distance numbers dialed), ibid. (citing Smith, supra, 442 U.S. at 740, 99 S. Ct. at 2580, 61 L. Ed. 2d at 226-27), or in financial information that customers convey to banks, id. at 344 n.1 (citing United States v. Miller, 425 U.S. 435, 442, 96 S. Ct. 1619, 1623, 48 L. Ed. 2d 71, 79 (1976)).

The Hunt Court observed that New Jersey had followed a different approach and afforded "the utmost protection" against tapping phones to hear "telephonic communications." Id. at 345. The Court also emphasized that telephone customers -- in 1982 -- placed calls "from a person's home or office, locations entitled to protection" under the Federal and State Constitutions. Id. at 347.

The Court specifically rejected the third-party doctrine. Hunt explained that telephone callers are entitled to assume that not only the words they utter but also the numbers they dial in private "will be recorded solely for the telephone

company's business purposes." Ibid. The Court added, "[i]t is unrealistic to say that the cloak of privacy has been shed because the telephone company and some of its employees are aware of" billing records. Ibid. The Court therefore concluded that toll billing records were "part of the privacy package" and were entitled to protection under the State Constitution. Id. at 347-48.

The bulk of the Court's thoughtful analysis focused on whether to diverge from federal law and recognize a privacy interest in telephone billing records. The opinion devoted little attention to the steps law enforcement officials must take to obtain protected billing records. At one point, the decision observed that allowing "seizures" of telephone billing records "without warrants can pose significant dangers to political liberty." Id. at 347. The passage was a prelude to a brief discussion of an actual abuse that had occurred: the FBI obtained toll billing records for columnist Jack Anderson after he wrote a "column embarrassing to former Vice President Agnew"; a source whose telephone number appeared in the records then lost his job as a city attorney. Ibid.

Two paragraphs later, the opinion cited state court decisions that followed or departed from the federal third-party doctrine. Id. 348. After siding with the latter group, the paragraph concluded, "[t]hus we are satisfied that the police

wrongfully obtained the toll billing records of the defendant Hunt in that they were procured without any judicial sanction or proceeding." Ibid. (emphasis added). The Court did not elaborate on the meaning of the phrase.

In reaching its conclusion, the Court in Hunt did not mention its earlier decision in In re Addonizio, 53 N.J. 107 (1968). In that ruling, the Court addressed a defendant's effort to set aside grand jury subpoenas served on a bank and a brokerage firm for his account records. The defendant attempted to assert a claim under the Fourth Amendment. Id. at 131. Chief Justice Weintraub rejected the argument and distinguished Brex v. Smith, 104 N.J. Eq. 386 (Ch. 1929). In that case, "the prosecutor, without any judicial process, called upon banks to deliver" certain account records. Addonizio, supra, 53 N.J. at 134 (emphasis added). "It is enough to say," the Addonizio Court explained, that "a grand jury subpoena would be something else." Ibid.² Hunt did not consider the issue or cite Addonizio.

² Grand jury investigations, in practice, are directed by the prosecutor, who ordinarily proposes witnesses to be called and issues subpoenas in the grand jury's name. See In re Grand Jury Subpoena Issued to Galasso, 389 N.J. Super. 281, 293 (App. Div. 2006). But "[t]he grand jury is a judicial, investigative body, serving a judicial function; it is an arm of the court, not a law enforcement agency or an alter ego of the prosecutor's office." In re Grand Jury Appearance Request by Loigman, 183 N.J. 133, 141 (2005). The grand jury also operates under the authority of the Judiciary. See McAllister, supra, 184 N.J. at

Justice Pashman authored a concurring opinion in Hunt which pointedly addressed the risk of abuse: "What is missing from the majority opinion is a full appreciation of the danger of political abuse posed by unlimited police access to knowledge of whom private citizens are calling and therefore of the importance of the warrant requirement as a check on this potential for abuse." Hunt, supra, 91 N.J. at 351 (Pashman, J., concurring). The concurrence also directly stated that "police [must] obtain a warrant before seizing toll billing records." Id. at 352. Because "[t]here is no danger that billing records will be destroyed . . . during the time needed to get a warrant," Justice Pashman wrote, the requirement "is at most a minimal burden that in no way intrudes upon legitimate police activity." Ibid.

By contrast, the references to warrants in the majority opinion offer little analysis and are not as explicit. Viewing the opinion as a whole, it appears that the parties and the Court focused on whether New Jersey should recognize a privacy interest in telephone billing records under the State

42-43 (noting Supreme Court's supervisory authority over grand juries); State v. Murphy, 110 N.J. 20, 31-33 (1998) (discussing statutory responsibility of Court to promulgate rules and regulations governing State grand juries); N.J.S.A. 2B:22-5 (authorizing Chief Justice to designate judges to "maintain judicial supervision over the grand jury").

Constitution. Indeed, the majority opinion framed the issue in the case in just that way. See id. at 342-43 ("The key questions are whether an individual has a protectible interest in [toll billing] records under the Fourth Amendment to the Federal Constitution or Article I, par. 7 of the New Jersey Constitution."). It is not possible to tell if the advocates even argued about what level of protection that right would require.

The Attorney General explains that, in response to Hunt, the State took a cautious approach and consistently sought warrants to obtain telephone toll records.

State v. Mollica, 114 N.J. 329 (1989), decided seven years after Hunt, cemented a warrant requirement for telephone billing records. Mollica considered whether to extend State constitutional protections to billing records for a hotel-room telephone. In the case, anonymous sources told the FBI that an individual had operated an illegal bookmaking enterprise from hotel rooms in Atlantic City. Id. at 335. Without a search warrant, federal agents obtained the suspect's telephone records from the hotel. Ibid. The FBI later turned the records over to state officials, who used the information to get a search warrant. Id. at 335-36. The defendants, in turn, challenged the search and claimed it was based on an unconstitutional

seizure of their hotel-room telephone billing records. Id. at 336.

The Court found no basis to distinguish between the expectation of privacy in billing records for a home telephone and a phone in a hotel room. Id. at 342. The “broader view of . . . privacy that surrounds the use of a telephone” applied in both settings and called for protection under the State Constitution. Id. at 344-45.

The Court next turned to the process required and briefly concluded, “[i]t therefore follows ineluctably that the official seizure of hotel-telephone billing or toll records relating to a guest’s use of a hotel-room telephone is subject to the requirements of antecedent probable cause and the issuance of a search warrant” under the State Constitution. Id. at 345 (citation omitted). For support, the Mollica Court cited only the passage in Hunt that noted the police wrongfully obtained billing records because they were procured “without any judicial sanction or proceeding.” Ibid. (quoting Hunt, supra, 91 N.J. at 348).

The next link in the chain is McAllister, which addressed bank records in 2005. This time, the Court undertook a deliberative, two-part analysis: it first considered whether account holders have a reasonable expectation of privacy in their bank records, and then assessed what level of protection

should apply to that information. McAllister, supra, 184 N.J. at 19.

At the outset, the Court recounted New Jersey's departure from the third-party doctrine. Under federal law, records that customers voluntarily convey to banks enjoy no Fourth Amendment protection. See Miller, supra, 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71. By contrast, Brex and Addonizio took a more restrictive approach. McAllister, supra, 184 N.J. at 28. Brex "recognized that account holders expect their banks to keep their records confidential, even in the face of a government official's formal request," and Addonizio, four decades later, "implicitly recognized" that interest. Id. at 26-28.

The McAllister Court then directly addressed the privacy interest in bank records. Id. at 29. The Court began by noting how revealing the records are:

Bank records, like long distance billing records, differ from other documents that memorialize an individual's affairs. On their face, bank records are simply a collection of numbers, symbols, dates, and tables. They are a veritable chronicle of the mundane: the payment of a nominal ATM fee, the automatic deposit of a paycheck, the monthly interest earned on a savings account. However, when compiled and indexed, individually trivial transactions take on a far greater significance. "In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography."

[Id. at 30-31 (quoting Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1975)).]

The Court also explained that “bank customers voluntarily provide their information to banks, but they do so with the understanding that it will remain confidential.” Id. at 31. The Court therefore held that the State Constitution “recognizes an account holder’s interest in the privacy of his or her bank records.” Id. at 32-33.³

Next, McAllister analyzed the level of protection needed to safeguard that privacy interest “in view of law enforcement’s legitimate investigatory needs.” Id. at 33. The Court rejected the ACDL’s position that probable cause was required. See id. at 24, 33. In doing so, the Court relied on Addonizio, which explained “that grand juries have never been bound only to investigate charges that were already supported by probable cause.” Id. at 33 (citing Addonizio, supra, 53 N.J. at 124). The McAllister Court quoted Chief Justice Weintraub, who had observed that “the probable cause required for a search warrant

³ Nowhere does McAllister suggest that customers have a reduced expectation of privacy because of federal reporting requirements for certain large cash transactions. See post at ___-___ (slip op. at 13-14). Nor would that logically follow. To the extent that account holders realize that a cash transaction of more than \$10,000 should result in the filing of a currency transaction report, how would that affect their reasonable expectation of privacy in the countless non-cash transactions that appear in their bank statements? McAllister specifically focused on the latter, more revealing, transactions.

is foreign to this scene [A grand jury's] power to investigate would be feeble indeed if [it] had to know at the outset everything needed to arrest a man or to invade his home." Id. at 33-34 (quoting Addonizio, supra, 53 N.J. at 126).

McAllister affirmed "the expansive investigatory power of grand juries," id. at 34, "bounded by relevancy and safeguarded by secrecy," id. at 42, and held that a grand jury subpoena based on a relevancy standard was adequate to protect an individual's privacy interest in bank records, id. at 36. A showing of probable cause, ordinarily required for a search warrant, was not required. Ibid.

Notably, McAllister contains but a single substantive reference to Hunt. McAllister simply states that because Hunt did not involve a grand jury subpoena, the opinion did not "require[] a different result in this appeal." Id. at 36.⁴

State v. Domicz, 188 N.J. 285 (2006), followed soon after McAllister. In Domicz, the Court held that a grand jury

⁴ The Court in McAllister declined to require the State to give notice to the target of the grand jury's investigation and invited the Criminal Practice Committee to further study "the benefits and burdens of enhanced protections for bank records." Id. at 42-43. The Criminal Practice Committee later surveyed prosecutors and defense counsel and concluded that the subpoena process, without notice, struck "a fair balance between an account holder's right to privacy and the legitimate needs of law enforcement to investigate alleged criminal activity." Report of the Supreme Court Criminal Practice Committee 2007-2009 Term at 133-34 (Feb. 17, 2009).

subpoena was sufficient to protect any privacy interest in an individual's utility records. Id. at 299-301. In its analysis, the Court underscored how revealing bank records are:

Bank records may reveal all types of household items purchased and possessed by a person, such as furniture, artwork, and electronic equipment. Through check and debit card payments, those records may disclose what a person eats and drinks, what newspapers and magazines he reads, and even where he vacations. Bank records also may indicate the amount of a person's utility and telephone bills.

[Id. at 299-300.]

By contrast, utility records expose far less "about a person's private life and activities within the home." Id. at 299. The Court thus found no basis to treat "utility records differently from bank records." Ibid. It upheld the use of a grand jury subpoena to obtain utility records and did not require the police to secure a warrant. Id. at 300-01.

Reid, supra, decided in 2008, drew on similar themes and followed the same two-part approach. In that case, someone had accessed a company's website and fraudulently changed the company's shipping address. 194 N.J. at 392. A supplier captured the user's Internet Protocol (IP) address and reported it to the owner of the company; the owner later relayed the IP address to the police. Ibid. The police issued a deficient subpoena to Comcast, the service provider to which the address

was registered, to obtain information about the IP address. Id. at 392-93. In response, Comcast identified the defendant as the subscriber of the IP address and provided subscriber information including her name, address, telephone number, and other account details. Id. at 393.

The Court again departed from the federal third-party doctrine and held that subscriber information that individuals provide to an Internet service provider is entitled to protection under the State Constitution. Id. at 399. The Court explained that

ISP records share much in common with long distance billing information and bank records. All are integrally connected to essential activities of today's society. Indeed, it is hard to overstate how important computers and the Internet have become to everyday, modern life. Citizens routinely access the Web for all manner of daily activities: to gather information, explore ideas, read, study, shop, and more.

. . . .

In addition, while decoded IP addresses do not reveal the content of Internet communications, subscriber information alone can tell a great deal about a person. With a complete listing of IP addresses, one can track a person's Internet usage. "The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's . . . fantasies, her health concerns, and so on." Daniel Solove, The Future of Internet Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1287 (2004). Such information can reveal intimate details about one's personal affairs in the same way

disclosure of telephone billing records does. Although the contents of Internet communications may be even more revealing, both types of information implicate privacy interests.

[Id. at 398-99.⁵]

The Court went on to consider “the type of protection ISP subscriber information should receive in the face of legitimate investigative needs.” Id. at 402. The Court revisited Addonizio, McAllister, and Domicz and concluded, “we see no material difference between bank records and ISP subscriber information and decline to treat them differently.” Id. at 404. In both cases, the Court held, “a grand jury subpoena based on a relevancy standard is sufficient to meet constitutional concerns.” Ibid. The Court did not rely on, or even refer to, Hunt in that discussion.

In 2013, the Court returned to the question of privacy in the context of cell-phone location information. Earls, supra, 214 N.J. 564. In Earls, the police obtained an arrest warrant for the defendant because of his role in a series of residential burglaries. Id. at 570-71. Law enforcement began looking for the defendant and an ex-girlfriend, whom the defendant allegedly

⁵ The subpoena in Reid sought subscriber information, not the subscriber’s Internet search or browsing history. The State has not argued in this appeal that a grand jury subpoena would be sufficient to obtain the latter kind of information, which would directly reveal content.

threatened after he learned about her cooperation in the investigation. Ibid. The police contacted T-Mobile, a cell-phone service provider, which provided information on three occasions -- without a warrant -- about the location of a cell phone believed to be used by the defendant. Id. at 571-72. That information led to the defendant's arrest. Id. at 572.

The Court noted that a cell phone automatically registers or identifies itself with the nearest cell site every seven seconds, even when no calls are made. Id. at 576-77. With existing technology in 2013, "cell-phone providers [could] pinpoint the location of a person's cell phone with increasing accuracy," and in some areas could even locate users within individual floors and rooms inside buildings. Id. at 577.

The Court reviewed federal law and considered United States v. Knotts, 460 U.S. 276, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983), and United States v. Karo, 468 U.S. 705, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984), which together "found no reasonable expectation of privacy in the monitoring of tracking devices in public, as opposed to private, areas." Earls, supra, 214 N.J. at 580-81. Earls also discussed a more recent decision, United States v. Jones, 565 U.S. ___, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012), in which a majority of the United States Supreme Court held that the installation of a GPS

tracking device on a car constituted a trespass on private property and required a warrant. Earls, supra, 214 N.J. at 582.

Justice Alito, who concurred with three other Justices, would have analyzed the case under a reasonable-expectation-of-privacy framework. Jones, supra, 565 U.S. at ___, 132 S. Ct. at 963-64, 181 L. Ed. 2d at 933-34 (Alito, J., concurring). He observed that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable"; "[b]ut the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Id. at ___, 132 S. Ct. at 964, 181 L. Ed. 2d at 934 (citation omitted). Justice Sotomayor, who joined the majority opinion, also concurred separately. She agreed with Justice Alito's views on longer term tracking and added that "even short-term [GPS] monitoring . . . will require particular attention." Id. at ___, 132 S. Ct. at 955, 181 L. Ed. 2d at 925. Both concurrences addressed GPS monitoring and the details it revealed, not toll billing records. See, e.g., ibid. (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail.").

Earls reasoned from the concurring opinions in Jones as well as settled state law. It reiterated that all three types of information discussed in Hunt, McAllister, and Reid can be

very revealing, and compared them to cell-phone location data.

Earls, supra, 214 N.J. at 585.

Using a cell phone to determine the location of its owner can be far more revealing than acquiring toll billing, bank, or Internet subscriber records. It is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources. It also involves a degree of intrusion that a reasonable person would not anticipate. See Jones, supra, 565 U.S. at ___, 132 S. Ct. at 964, 181 L. Ed. 2d at 934 (Alito, J., concurring). Location information gleaned from a cell-phone provider can reveal not just where people go -- which doctors, religious services, and stores they visit -- but also the people and groups they choose to affiliate with and when they actually do so. That information cuts across a broad range of personal ties with family, friends, political groups, health care providers, and others. See id. at ___, 132 S. Ct. at 955-56, 181 L. Ed. 2d at 925 (Sotomayor, J., concurring). In other words, details about the location of a cell phone can provide an intimate picture of one's daily life.

[Id. at 586 (emphasis added).]

The Court concluded that cell-phone users have a reasonable expectation of privacy in the location of their cell phones, which is entitled to protection under the State Constitution. Id. at 587-88. The sentence underscored in the above passage, though, does not resolve this appeal because it does not differentiate among telephone billing, bank, and Internet records; it merely notes that tracking one's location through a

cell phone is more revealing than the other three kinds of information.

Earls also separately considered what level of protection the privacy right required. The Court noted that, "[a]s a general rule, the more sophisticated and precise the tracking, the greater the privacy concern." Id. at 587. "Because of the nature of the intrusion, and the corresponding, legitimate privacy interest at stake," the Court held that the "police must obtain a warrant based on a showing of probable cause" to get tracking information through a cell phone, unless exigent circumstances or another exception to the warrant requirement applies. Id. at 588. Earls did not rely on Hunt to support that holding.

B.

The above survey reveals that our jurisprudence is not internally consistent. Telephone billing records -- a list of phone numbers dialed out of and in to a phone, along with the time and duration of those calls -- are, of course, quite revealing. That is why they are entitled to protection under the State Constitution, even though they do not disclose the contents of any communications.

Amici argue that telephone billing records are "content-laden" and "suggestive" of content, particularly when they are aggregated. But are telephone billing records more revealing

than bank records, which reveal actual content? Bank records contain not only a tally of dates and dollar amounts; they also include copies of actual checks that disclose who was paid, for how much, often for what services, and when. The contents of a checkbook can expose the doctors we use, the political parties and religious groups we contribute to, and payments to intimate associates that are meant to be kept private. Credit card statements offer similar details. Also, as Reid explained, ISP subscriber information can disclose comparable personal details; if matched to an IP address, the information can help track a person's Internet usage. Reid, supra, 194 N.J. at 398.

All three areas -- telephone billing records, bank records, and Internet subscriber information -- are less intrusive than a device that permits 24/7 tracking. Yet it is hard to differentiate among the three in terms of the reasonable expectation of privacy that attaches to each. Bank account records, credit card statements, and Internet subscriber information can be just as revealing as telephone billing information.

The ACDL argues that telephone billing records, which are expressed in a standardized format, are easy to aggregate and analyze, particularly in light of modern technology. The ACDL also contends that society's reliance on telecommunications has increased with the rise of mobile phones. But standardized bank

records can also be aggregated and analyzed. And just as mobile phones have arguably increased the amount of data available, the widespread replacement of cash with credit and debit cards and mobile payment systems has also added to society's trail of financial transactions. See Geoffrey R. Gerdes and Kathy C. Wong, Federal Reserve Bulletin, Recent Payment Trends in the United States A77 (Oct. 2008), <http://www.federalreserve.gov/pubs/bulletin/2008/pdf/payments08.pdf> (showing nearly three-fold increase in number of non-cash payments per person in United States from 1971 to 2006); Federal Reserve System, The 2013 Federal Reserve Payments Study 15 (2014), https://www.frbervices.org/files/communications/pdf/general/2013_fed_res_paymt_study_detailed_rpt.pdf (showing approximately 29-percent increase in total non-cash payments in United States from 2006 to 2012).

Bank records arguably reveal more to law enforcement than telephone billing records because of the actual content they contain. Yet our law has given greater protection to telephone billing records, which do not disclose content. In other words, if bank records are relevant to an investigation, law enforcement can seek them with a subpoena; to obtain telephone billing records, though, officers have been required to meet a higher threshold and show probable cause.

One reason for the disparate approach in our case law is the manner in which it developed. Hunt and Mollica did not consider legitimate investigative needs when they together imposed a warrant requirement to obtain telephone billing records. McAllister and Reid weighed that concern but did not wrestle with Hunt. This appeal requires that we do both. We are called on to analyze and reconcile different strands in the law -- to assess genuine privacy concerns as well as valid law enforcement aims across related areas.

To do that, in addition to evaluating how intrusive toll records can be, as Hunt did, we consider the practical impact of requiring a search warrant -- based on probable cause -- to obtain telephone toll records. Probable cause for a warrant requires proof "to believe that a crime has been or is being committed at a specific location or that evidence of a crime is at the place to be searched." State v. Evers, 175 N.J. 355, 381 (2003) (citations omitted). In the context of a warrant for telephone billing records, a judge must be convinced that there is probable cause to believe the records sought contain evidence of a crime -- not simply that the records are relevant to an ongoing criminal investigation. To amass enough evidence to meet the higher standard inevitably slows down investigations in the early stages, particularly in matters that involve more complex schemes. That approach runs counter to both the

traditional authority of the grand jury, see Addonizio, supra, 53 N.J. at 126, and society's legitimate interest in having officials promptly investigate and try to interrupt criminal activity.

To be sure, if the police choose to use highly intrusive techniques, like obtaining cell-phone location information, they must establish probable cause notwithstanding the impact that standard may have on the pace of an investigation. But when the police request less intrusive information, a relevance standard can protect valid privacy concerns and allow appropriate investigations to proceed.⁶

⁶ The dissent focuses on pen registers. Unlike toll billing records, which present a list of phone numbers dialed after the fact, a pen register tracks each call as it is made. Law enforcement officials who monitor a pen register get real-time information about all local and long distance numbers dialed, including calls that are not completed. See State v. Feliciano, ___ N.J. ___, ___ (2016) (slip op. at 4 n.1). Pen registers thus disclose current activity, around the clock, in a manner that reveals more than toll billing records.

A number of jurisdictions, in fact, require law enforcement to meet a heightened standard to obtain a pen register, as compared to toll billing records. See, e.g., State v. Thompson, 760 P.2d 1162, 1168 (Idaho 1988) (pen register), Idaho Code Ann. § 19-3004A (2016) (billing records); In re Original Investigation, Special Grand Jury, 402 N.E.2d 962, 964 (Ind. 1980) (pen register), In re Order for Ind. Bell Tel. to Disclose Records, 409 N.E.2d 1089, 1090-91 (Ind. 1980) (billing records), overruled in part on other grounds by S.H. v. State, 984 N.E.2d 630 (Ind. 2013); Dist. Attorney for Plymouth Dist. v. New England Tel. & Tel. Co., 399 N.E.2d 866, 868-70 (Mass. 1980) (pen register), Commonwealth v. Vinnie, 698 N.E.2d 896, 909-10 (Mass.), cert. denied, 525 U.S. 1007, 119 S. Ct. 523, 142 L. Ed. 2d 434 (1998) (billing records); Mont. Code Ann. § 46-4-403

C.

We are not the only state to consider the standard the police must satisfy to obtain telephone billing records. In the three decades since Hunt and Mollica, however, only a handful of states have imposed a probable cause requirement.

Federal law permits law enforcement to obtain telephone billing records with a grand jury or trial subpoena or an appropriate administrative subpoena. See 18 U.S.C.A. § 2703(c)(2). That standard remains in place after Riley v. California, ___ U.S. ___, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014).

Defendant relies on Riley and contends that it requires the use of a search warrant to access telephone connection records. Riley, however, involved a warrantless search of the contents of a smartphone seized incident to an arrest. As the United States Supreme Court explained, a search of a modern cell phone can reveal vast amounts of private personal information, “from the mundane to the intimate”: photographs, text messages, one’s Internet browsing history, calendar, personal contacts, historic location information, various apps, and more. Id. at ___, 134

(2016) (pen register), Hastetter v. Behan, 639 P.2d 510, 512-13 (Mont. 1982) (billing records); Commonwealth v. Mellili, 555 A.2d 1254, 1258-59 (Pa. 1989) (pen register), 18 Pa. Cons. Stat. § 5743 (2016) (billing records); but see Hunt, supra, 91 N.J. at 344.

S. Ct. at 2489-91, 189 L. Ed. 2d at 446-48. Because smartphones contain and may reveal "the privacies of life," the Court held that law enforcement officers must get a warrant before they may search the contents of a cell phone seized incident to arrest.

Id. at ___, 134 S. Ct. at 2494-95, 189 L. Ed. 2d at 452

(citation omitted). Riley did not address telephone billing records and did not alter the prevailing federal standard to obtain that information.

A large majority of states use the same type of standard and allow law enforcement to obtain telephone billing information based on some form of a relevancy standard.⁷

⁷ See Henderson v. State, 583 So. 2d 276, 291-92 (Ala. Crim. App. 1990); Ariz. Rev. Stat. § 13-3018 (2016); State v. Hamzy, 709 S.W.2d 397, 398-99 (Ark. 1986); Conn. Gen. Stat. § 54-47aa (2016); Del. Code Ann. tit. 11, § 2423(c) (2016); Gibbs v. State, 479 A.2d 266, 272 (Del. 1984); Fla. Stat. Ann. § 934.23(4) (2016); Figueroa v. State, 870 So. 2d 897, 901 (Fla. Dist. Ct. App. 2004); Kesler v. State, 291 S.E.2d 497, 504 (Ga. 1982); Idaho Code Ann. § 19-3004A (2016); People v. DeLaire, 610 N.E.2d 1277, 1282-83 (Ill. App. Ct.), appeal denied, 616 N.E.2d 340 (Ill. 1993); In re Order for Ind. Bell Tel. to Disclose Records, 409 N.E.2d 1089, 1090 (Ind. 1980); State v. Schultz, 850 P.2d 818, 829-30 (Kan. 1993); State v. Marinello, 49 So. 3d 488, 507-10 (La. Ct. App. 2010), cert. denied, 61 So. 3d 660 (La. 2011); Me. Rev. Stat. Ann. tit. 5, § 200-B(2) (2016); Md. Code Ann., Crim. Proc. § 15-108(a) (2016); Mass. Ann. Laws ch. 271, § 17B (2016); Commonwealth v. Vinnie, 698 N.E.2d 896, 909-10 (Mass. 1998); Minn. Stat. Ann. § 388.23 (2016); Fraise v. State, 17 So. 3d 160, 163-64 (Miss. Ct. App. 2009) (non-narcotics case); Hastetter v. Behan, 639 P.2d 510, 511 (Mont. 1982); Neb. Rev. Stat. Ann. § 86-2,106 (2016); State v. Knutson, 852 N.W.2d 307, 319-20 (Neb. 2014), cert. denied, ___ U.S. ___, 135 S. Ct. 1505, 191 L. Ed. 2d 442 (2015); N.H. Rev. Stat. Ann. § 7:6-b (2016); State v. Gubitosi, 886 A.2d 1029, 1034-36 (N.H. 2005); People v. Di Raffaele, 433 N.E.2d 513, 516 (N.Y. 1982);

Five states require a showing of probable cause. In three states, the rule is imposed by statute;⁸ in two, it is based on case law that interprets the state's constitution.⁹

In 2006, the New Jersey Legislature unanimously amended the Wiretap Act to require service providers to disclose telephone records to law enforcement in response to a grand jury subpoena. See L. 2005, c. 270 (codified as amended at N.J.S.A. 2A:156A-

N.C. Gen. Stat. § 15A-298 (2016); N.D. Cent. Code Ann. § 51-34-04 (2016); State v. Lind, 322 N.W.2d 826, 836-37 (N.D. 1982); State v. Neely, 2012-Ohio-212, ¶¶ 16-26 (Ohio Ct. App. 2012); State v. Johnson, 131 P.3d 173, 183-84 (Or. 2006); 18 Pa. Cons. Stat. Ann. § 5743 (2016); State v. McGoff, 517 A.2d 232, 234 (R.I. 1986); State v. King, 772 S.E.2d 189, 197 (S.C. Ct. App. 2015); Tenn. Code Ann. § 24-7-116 (2016); Tex. Code Crim. Proc. Ann. art. 18.21, Sec. 5 (2016); Utah Code Ann. § 77-23b-4 (2016); Am. Fork City v. Smith, 258 P.3d 634, 636 (Utah Ct. App. 2011); Va. Code Ann. § 19.2-70.3 (2016); State v. Clark, 752 S.E.2d 907, 921 (W. Va. 2013); Saldana v. State, 846 P.2d 604, 611-12 (Wyo. 1993); see also Williams v. Commonwealth, 213 S.W.3d 671, 683 (Ky. 2006) (embracing third-party doctrine generally); State v. Plunkett, 473 S.W.3d 166, 175-76 (Mo. Ct. App. 2015) (same); State v. Rolfe, 825 N.W.2d 901, 910 (S.D. 2013) (following third-party doctrine for ISP records); State v. Simmons, 27 A.3d 1065, 1070 n.5 (Vt. 2011) (noting no history of rejecting third-party doctrine); but see Miss. Code. Ann. § 41-29-536 (2016) (probable cause standard for narcotics cases). The State canvassed other Attorneys General and represents that prosecutors in New Mexico use subpoenas to obtain telephone billing records.

⁸ Cal. Penal Code § 1524.3 (2016); Mich. Comp. Laws Serv. § 767A.3 (2016); Wis. Stat. Ann. § 968.375 (2016).

⁹ See People v. Corr, 682 P.2d 20, 26-28 (Colo. 1984); State v. Eisfeldt, 185 P.3d 580, 585 (Wash. 2008). The State represents that prosecutors in Alaska and Nevada use search warrants to obtain telephone billing records; notwithstanding the authority cited above in note 7, prosecutors in South Carolina and Wyoming reportedly do so as well.

29(f) (2006)). The provision mirrors federal law. See 18 U.S.C.A. § 2703(c)(2). Because the amendment conflicts with the standard set in Hunt and Mollica, it has not been followed. It nevertheless reflects the Legislature's view of what a reasonable expectation of privacy in this area calls for, and is entitled to respectful consideration. See Reid, supra, 194 N.J. at 401 (noting Legislature's determination to protect against disclosure of ISP information).

The judicial branch, of course, has the obligation and the ultimate responsibility to interpret the meaning of the Constitution and the protections it requires. Asbury Park Press, Inc. v. Woolley, 33 N.J. 1, 12 (1960). Although the actions of other states may be informative, in the end we are guided by the language and history of the New Jersey Constitution.

D.

We pause to underscore what this case is not about: the collection of bulk data from telephone service providers for large numbers of customers, over an extended period of time, by an agency that does not conduct criminal investigations. Much has been written about the recent efforts of the National Security Agency (NSA) to collect large amounts of telephone metadata on an ongoing basis. The Second Circuit recently found that the NSA's program exceeded the scope of what Congress had

authorized and violated the Patriot Act. See ACLU v. Clapper, 785 F.3d 787, 826 (2d Cir. 2015). New Jersey's Attorney General stresses that the NSA program presents a "markedly different" practice that is "completely distinct" from the grand jury subpoena process.

We do not address or sanction the NSA's practice in this opinion. The subpoena at the center of this appeal seeks two weeks of telephone billing records, for a single phone line, in connection with an ongoing criminal investigation. That is not the same as an effort by a non-law enforcement agency, acting outside the criminal arena, to obtain, aggregate, and retain bulk data about the use of telephone facilities by a large number of individuals.

E.

We continue to believe that telephone billing records, bank records, and ISP subscriber information disclose private information that is entitled to constitutional protection. Our law, therefore, does not allow police officers simply to contact a service provider and ask for those records.

As we have noted before, the greater the degree of intrusion into an individual's personal affairs, the greater the privacy concern. See Earls, supra, 214 N.J. at 587. We find that all three types of records reveal comparable amounts of private information and are similarly intrusive. Indeed, the

language in Hunt, McAllister, and Reid contains similar themes and examples of the types of personal information that may be disclosed. See Hunt, supra, 91 N.J. at 347; McAllister, supra, 184 N.J. at 30-31; Reid, supra, 194 N.J. at 398-99. Because the privacy concerns in all three areas are similar, the records should receive comparable levels of protection. See Reid, supra, 194 N.J. at 404 ("[Records that] reveal comparably detailed information about one's private affairs . . . are entitled to comparable protection under our law.").

Defendant does not acknowledge the inconsistency in our case law. For that reason, he views the State's petition as an effort to overturn Hunt. This appeal, however, viewed in the context of three decades of jurisprudence, is about reconciling and restoring consistency to a challenging area of law, which we have attempted to do.

Looking at the full spectrum of cases the Court has decided in recent decades, we conclude that the relevance standard adopted in McAllister and Reid appropriately protects individual privacy rights in telephone billing records and at the same time recognizes society's legitimate interest in investigating criminal activities.

We also appreciate the possibility for abuse in this sensitive area. Hunt, supra, addressed that issue decades ago, 91 N.J. at 347, and it remains a concern today. We therefore

retain direct judicial oversight as part of the process to obtain telephone billing records.

We direct that, going forward, the State must apply for a court order under N.J.S.A. 2A:156A-29(e) to obtain telephone billing or toll records. In accordance with that statute, law enforcement must demonstrate "specific and articulable facts showing that there are reasonable grounds to believe that" the records sought are "relevant and material to an ongoing criminal investigation." N.J.S.A. 2A:156A-29(e). The requested records must cover a finite period of time which does not extend beyond the date of the order.

Judicial review of ex parte applications of this type will help guard against abuses in general and root out bulk requests for information that are unconnected to a criminal investigation. In addition, a judge may quash or modify an order "if the information or records requested are unusually voluminous," among other reasons. Ibid.

IV.

For the reasons stated above, we affirm the trial court's decision to quash the grand jury subpoena for telephone billing records. The State may apply for a court order to obtain those records in this case, consistent with the principles discussed above.

JUSTICES PATTERSON, FERNANDEZ-VINA and SOLOMON join in CHIEF JUSTICE RABNER's opinion. JUSTICE LaVECCHIA filed a separate, concurring and dissenting opinion in which JUDGE CUFF (temporarily assigned) joins. JUSTICE ALBIN did not participate.

SUPREME COURT OF NEW JERSEY
A-61 September Term 2014
075691

STATE OF NEW JERSEY,

Plaintiff-Appellant,

v.

GARY LUNSFORD,

Defendant-Respondent.

JUSTICE LaVECCHIA and JUDGE CUFF (temporarily assigned),
concurring and dissenting.

We concur in the judgment that affirms the trial court's decision to quash the grand jury subpoena for telephone billing records. We respectfully dissent from the portion of the Court's judgment that permits the State to apply for a court order to obtain those records based on the new procedures outlined in the Court's opinion.

This appeal is about where one puts one's marker on privacy. For the telephone billing records in issue in this matter, we place our marker where this Court placed it over thirty years ago in State v. Hunt, 91 N.J. 338 (1982). Hunt established a warrant requirement for police access to telephone billing records. The line of cases that began with Hunt and continued with State v. Mollica, 114 N.J. 329 (1989), and State

v. Earls, 214 N.J. 564 (2013), should, in our view, include this appeal as part of that chain.

I.

In Hunt, supra, this Court rejected United States Supreme Court precedent, believing that “[i]t is unrealistic to say that the cloak of privacy has been shed” because telephone billing records were disclosed to the telephone company and its employees. 91 N.J. at 347. Because of the wealth of information that they reveal, the Court said that telephone billing records are “part of the privacy package.” Ibid. As such, law enforcement could not obtain those records “without any judicial sanction or proceeding.” Id. at 348.

For us there can be no sincere question whether Hunt imposed a warrant requirement for access to telephone billing records that include information about calls sent, received, and the length of time spent on each such call. The Court unmistakably understood its own precedent as requiring a warrant and not something less. See Chief Justice Robert Wilentz, The New Constitution, 49 Rutgers L. Rev. 887, 888 (1997) (stating, in speech delivered at Princeton University in 1985, “[W]e held that the state’s obtaining a defendant’s telephone bills without a warrant (order by a judge) simply by asking the telephone company to turn the bills over, or obtaining them in some other way without a warrant, constituted an unreasonable seizure under

the New Jersey Constitution, rendering any evidence derived from those telephone bills inadmissible at trial").

If it is arguable, at all, from the very language of Hunt itself, any doubt about the judicial process that the Hunt Court had in mind was cleared up by Mollica. That opinion began with this sentence: "In this case federal law-enforcement officers without a search warrant obtained hotel billing records relating to the use of an occupant's room telephone." Mollica, supra, 114 N.J. at 334 (emphasis added). The Court asked whether Hunt's protection reached "transient accommodations, such as hotel rooms, and . . . hotel telephone toll records that are kept in the regular course of a hotel's business to reflect for billing purposes the use of hotel-room telephones by guests." Id. at 340-41.

The Court said that it did, declining "to endorse . . . a shallow constitutional distinction between a home on the one hand and motel rooms on the other." Id. at 342 (quoting People v. Oliver, 338 N.W.2d 167, 173 (Mich. 1983)). That the hotel staff in addition to the telephone company "creat[ed] an extra circle of persons who have access to toll records for business purposes, [did] not alter this perception." Id. at 343. Accordingly, this Court declared that government seizure of those records "is subject to the requirements of antecedent probable cause and the issuance of a search warrant." Id. at

345 (emphasis added). In making that pronouncement, Mollica cited to Hunt's language that telephone billing records were wrongfully obtained "without any judicial sanction or proceeding." Ibid. That, in our view, nullifies any argument that "judicial sanction or proceeding" means anything other than a warrant supported by antecedent probable cause.

The State now argues that the warrant requirement should be tossed aside. According to the State, the warrant requirement is too burdensome. After all, a federal statute allows federal officers to obtain telephone billing records on the strength of a grand jury subpoena, see 18 U.S.C.A. § 2703(c)(2), and so does a New Jersey statute that was designed to mimic the federal standard, see N.J.S.A. 2A:156A-29(f). Because federal authorities can obtain telephone billing records early in joint federal-state conspiracy investigations, and because those records will not be admissible in state court, the State contends that the option to prosecute any part of the case in state court is foreclosed. Our warrant requirement, in the State's view, serves as a roadblock to joint federal-state investigations.

The difficulty with the State's position is that it has been advanced before, thoroughly considered, and rejected. The warrant requirement was not some ill-considered aside by this Court. Writing for the Court in Mollica, Justice Handler was

expressly aware of the practical implications that follow from imposing a warrant requirement under Article I, Paragraph 7 when none is required under the Fourth Amendment. Ironically for the State, Mollica is "the seminal case" on the issue. Wayne A. Logan, Dirty Silver Platters: The Enduring Challenge of Intergovernmental Investigative Illegality, 99 Iowa L. Rev. 293, 311 (2013).

When states, like New Jersey, began to impose more protective procedures under their state constitutions, it constituted a twist on the old "silver platter" doctrine. Before the Fourth Amendment applied to the states, evidence would pass from state officers -- unburdened by the Fourth Amendment -- to federal authorities on a silver platter. Mollica, supra, 114 N.J. at 346-47. But as judicial federalism gained a foothold, "evidence [could] now flow to state officers from federal officers governed by more lenient standards." Id. at 351. The Mollica Court detailed the jurisdictional limits of a state constitution, which "ordinarily governs only the conduct of the state's own agents or others acting under color of state law." Id. at 345. Just as a state constitution does not constrain officers of other states, "state constitutions do not control federal action." Id. at 352. Thus, it does not offend the New Jersey Constitution when an officer of another jurisdiction transfers criminal evidence to New Jersey law

enforcement, so long as that out-of-state officer obtained the evidence lawfully and independent of New Jersey authorities. Id. at 353.

Applying those principles to the case at hand, the Mollica Court explained that the telephone billing records “were obtained by federal agents exercising federal authority in a manner that was in conformity with federal standards and consistent with federal procedures.” Id. at 354. Once legally seized, nothing prevented the federal agents from turning over the telephone record evidence to state authorities, even if its seizure violated state constitutional standards. Id. at 355. But that turnover was subject to a “vital” limitation: “When such evidence is sought to be used in the state, it is essential that the federal action deemed lawful under federal standards not be alloyed by any state action or responsibility.” Ibid.

Mollica’s holding and analysis remained tethered to Hunt’s warrant requirement, mindful of the burdens that the warrant requirement would impose on joint federal-state investigations. See id. at 356 (recognizing that “antecedent mutual planning, joint operations, cooperative investigations, or mutual assistance between federal and state officers may sufficiently establish agency and serve to bring the conduct of the federal agents under the color of state law”). Thus, when it comes to telephone billing records, our Court in Hunt and Mollica could

not have been clearer: A warrant supported by probable cause is required. And, equally clear is this: The Court knew precisely the burdens that a warrant requirement for telephone billing records would impose on joint federal-state investigations.

Mollica addressed the prime concern that, the State now asserts, renders the warrant requirement unworkable, namely that federal officers can obtain telephone billing records before their state counterparts. To us, Hunt resolved the issue. And Mollica reaffirmed it. Both treated the privacy interest in telephone billing information equally, and the privacy interests were not place-based. In each, the Court demanded a probable cause showing and review by a judicial officer before the State could trench on the private matters disclosed through the telephone billing records. Certainly, the warrant requirement and its probable cause standard might impede joint federal-state operations, but the privacy interest was great enough, in our Court's view, to justify that impediment.

That was our law, our proud law. The State's argument does not justify tossing aside the standard that has governed in this State for more than thirty years. In any case where this Court imposes a warrant requirement under Article I, Paragraph 7, and that requirement is lacking under federal law, federal law enforcement officers will be able to proceed more quickly than their New Jersey counterparts. Federal officers may choose not

to wait for a warrant, and that will mean that, in cooperative investigations, the seized evidence will be inadmissible in a New Jersey prosecution. That is a necessary and established consequence of doing business under a privacy-protective state constitution. The State's recycling of the same complaints about that consequence does little to advance its argument that Hunt is "unworkable in practice."

II.

The State also asserts that New Jersey is an outlier, a fringe jurisdiction. It argues that law enforcement can obtain telephone billing records almost everywhere else on the authority of a grand jury subpoena grounded in a relevancy finding, but we require a warrant.

In our view, that argument sets a false equivalency. The starting point for any nationwide comparison is not all fifty states but those states that have departed -- like we have -- from Fourth Amendment law that holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44, 99 S. Ct. 2577, 2582, 61 L. Ed. 2d 220, 229 (1979); see also United States v. Miller, 425 U.S. 435, 443, 96 S. Ct. 1619, 1624, 48 L. Ed. 2d 71, 79 (1976). Only about eleven states have done so. See Stephen E. Henderson, Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs

to Protect Third Party Information from Unreasonable Search, 55 Cath. U. L. Rev. 373, 376 (2006). It is thus entirely unsurprising that most states require only a grand jury subpoena. That simply mirrors the federal standard. In those states, there is no protectable privacy interest in telephone billing records under either the Fourth Amendment or the state constitution's search-and-seizure provision; accordingly, it should be easier for law enforcement to obtain those records.

Once the comparison point is properly cut down, the analysis is more balanced. In some states, like ours, that have rejected the third-party doctrine, and have in turn found a protectable privacy interest in certain telephone records, a warrant supported by probable cause is required before the government can access such information. See, e.g., State v. Rothman, 779 P.2d 1, 7 (Haw. 1989) (recognizing expectation of privacy in "telephone numbers [persons] call on their private lines" and requiring government to obtain warrant before "tap[ping] . . . private telephones to obtain such information, or requir[ing] the telephone company to supply such information"); State v. Thompson, 760 P.2d 1162, 1167 (Idaho 1988) ("Since there was no warrant based on probable cause for the installation and use of the pen register in this case, the information obtained by its use should have been excluded from the determination of probable cause for the issuance of the

wiretap orders."); State v. Gunwall, 720 P.2d 808, 813 (Wash. 1986) (holding that Washington Constitution "prevent[s] the defendant's long distance home telephone records from being obtained from the phone company, or a pen register from being installed on her telephone connections, without a search warrant or other appropriate legal process first being obtained"). In others, however, a subpoena bounded by a relevancy standard may do the job, at least in the grand jury context. See People v. Mason, 989 P.2d 757, 761-62 (Colo. 1999).

In its rush to resolve what it views as a tension in our case law, the majority creates another one. Presumably after this appeal, the State will still use a communications data warrant to install a pen register or a trap-and-trace device so that it can track, in real time, calls made and received. Although some courts have recognized a distinction between real-time and historical data, we have not. See Hunt, supra, 91 N.J. at 344 ("The expectation of privacy in a pen register, both subjectively and objectively, is substantially similar to that in toll billing records."); see also People v. Larkin, 239 Cal. Rptr. 760, 762 (Ct. App. 1987) ("A pen register, providing information about outgoing and incoming calls, involves the same privacy rights as toll information in phone company records."); Stephen E. Henderson, Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest

of Us Too, 34 Pepp. L. Rev. 975, 1016 (2007) (“[T]he acquisition of telephone numbers dialed in real time via a pen register is equivalent to the acquisition of those numbers from a telephone company record. Therefore, the constitutional restraint on government access should be identical. Both processes acquire the same information, and it is no more invasive to have information captured in real time.”).

Even those federal courts that have avoided following Smith and Miller third-party-doctrine principles when it comes to location information require a warrant for such requests by law enforcement. See United States v. Graham, 796 F.3d 332, 345 (4th Cir. 2015) (holding that because users have a reasonable expectation of privacy in historical cell-site information, “[i]ts inspection by the government, therefore, requires a warrant, unless an established exception to the warrant requirement applies”).

Notably, this Court’s decision in Earls, supra, did not draw a distinction between a real-time request for cell-site information and historical data. 214 N.J. at 588. And such a distinction can prove highly superficial. For data to be historical, it need not be far removed in time. When a law enforcement officer requests a cellular provider to relay a target’s telephone records in hour-by-hour intervals, it is technically a request for historical records. Any delay -- no

matter how short -- can turn data into historical data. See State v. Perry, 776 S.E.2d 528, 535 (N.C. Ct. App. 2015) (calling location information "historical" when "evidence show[ed] AT&T emailed the delayed recorded information to [law enforcement] every fifteen minutes").

The incongruity we see in the outcome reached by the majority, at the State's urging, is that, under the majority's new holding, to follow a suspect's telephone activity as it happens requires a judicial warrant based on probable cause. But if the police want the suspect's telephone records two or three minutes after the call is completed, a warrant based on probable cause is not necessary. It is not the move from a warrant to a judicially reviewed subpoena that is the most troubling. After all, a subpoena is a commonly used device to request documents. It is the lessening of the standard from probable cause to relevancy. Now a watered-down grand jury subpoena will suffice for telephone billing records, so long as there is judicial oversight to ensure that a relevancy standard is met, somehow, for the particular investigation. Because relevancy sweeps broadly, particularly at the beginning stages of a criminal investigation, one must ask what exactly is the point then of an Article I, Paragraph 7 privacy interest. Relevance governs the breadth of a grand jury's subpoena power anyway. Pressler & Verniero, Current N.J. Court Rules, comment

2 on R. 1:9-2 (2015) ("With respect to grand jury investigations, relevance continues to constitute the standard for appropriate issuance of a subpoena duces tecum").

In reaching its conclusion, the majority places a good deal of weight on this Court's decision in State v. McAllister, 184 N.J. 17, 32-33 (2005), in which the Court recognized an Article I, Paragraph 7 privacy interest in bank records. That interest was protected by only a grand jury subpoena based on a relevancy standard. Id. at 36. Next in line was State v. Reid, 194 N.J. 386 (2008). There, the Court determined that subscriber information held by an Internet Service Provider was also protected by the New Jersey Constitution. Id. at 399. Pointing to McAllister, the Court said a grand jury subpoena was sufficient to protect that interest. Id. at 403-04.

From those cases, the majority sees a need to make our privacy law jurisprudentially consistent. Hunt, it says, is out of tune with the rest of our law. To accomplish that, the majority drops the level of protection for telephone records and says that for those records a relevancy standard is more than enough. Because McAllister and Reid held a grand jury subpoena sufficient, we should do the same here. We disagree.

In our view, the State benefited in McAllister from the reality of a reduced expectation of privacy that bank records have due to the well-known regulatory review and reporting

requirements on transactional behavior. 31 U.S.C.A. § 5313(a) grants the Secretary of the Treasury broad authority to prescribe when domestic financial institutions involved in monetary transactions must "file a report on the transaction." See also 31 C.F.R. § 1010.311 ("Each financial institution other than a casino shall file a report of each deposit, withdrawal, exchange of currency or other payment or transfer, by, through, or to such financial institution which involves a transaction in currency of more than \$ 10,000, except as otherwise provided[.]"). The Treasury Secretary may, moreover, "require any financial institution, and any director, officer, employee, or agent of any financial institution, to report any suspicious transaction relevant to a possible violation of law or regulation." 31 U.S.C.A. § 5318(g)(1); see also 31 C.F.R. § 1020.320(a)(1) (enforcing that requirement). The Court's lesser concern with bank customer privacy expectations and rights was registered by its willingness to allow subpoenas without prior notice to the target. McAllister, supra, 184 N.J. at 42.

That lesser concern with privacy rights is a far cry from the traditional respect shown to telephone records and suggests that bank records should be regarded as the outlier case, not Hunt or Mollica. Reid relied on McAllister in the new world of internet subscriber information. Given its limited scope -- the State concedes that a search warrant is required to gain access

to a full internet search history -- Reid should hardly be regarded as the "new" assessment of privacy rights historically respected in this State. Nothing in either McAllister or Reid suggests that we intended to turn the entirety of our privacy law on its head.

It is particularly perplexing that the Court holds as it does now, at a time when we are more dependent on our telephones than ever before. We are in contact all the time through cell phones. And the associational concerns that drove Hunt, and were present in Earls too, are no less weighty today. See Hunt, supra, 91 N.J. at 351-52 (Pashman, J., concurring); Earls, supra, 214 N.J. at 586. Our jurisprudence now protects, through a warrant requirement, the location of those phones but not who we are calling or who is calling us. The majority asserts that it is striving for consistency in our jurisprudence as justification for tossing aside Hunt and Mollica. To us, consistency is to be found in answering the question here in the same way we have dealt with the protection of privacy interests in telephone information in Hunt, Mollica, and Earls. A warrant issued on the basis of probable cause should remain the prerequisite to access telephone billing records. This case should have been an unremarkable application of a consistent line of cases addressing law enforcement access to private telephone records.

III.

In sum, even if we are an outlier compared to those jurisdictions that allow law enforcement access to telephone billing records through means short of a warrant issued on probable cause, that alone is not a reason to change our law. This Court has been a leader in privacy rights, proudly proclaiming that Article I, Paragraph 7 is not simply "a procedural matter" but "a reaffirmation of the privacy rights guaranteed to our citizens and of our duty as judges to secure them." State v. Eckel, 185 N.J. 523, 540 (2006). It did not bother us that we were an outlier in Hunt. And it did not bother us that we were an outlier in Mollica. Why then should it bother us now? So fixated on aligning our state jurisprudence with the federal standard, we fear the State, and now the majority, has sacrificed our law for the sake of that uniformity. We are unpersuaded that any legitimate basis for overturning our precedent -- for that is what is happening here no matter how the analysis is dressed up -- is present here.

Accordingly, we respectfully dissent.