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 interests of brevity, portions of any opinion may not have been summarized).

State of New Jersey v. Shirley Reid (A-105-06)

Argued October 22, 2007 -- Decided April 21, 2008

Rabner, C.J., writing for a unanimous Court.

This case involves multi-digit numbers called IP addresses that Internet Service Providers (ISPs) assign to subscribers for use in accessing Internet websites. Websites may collect the numbers, but with the technology available today only the ISP that assigned the address can translate it into the name of an actual user. In this context, the Court considers whether Internet subscribers have a reasonable expectation of privacy in their identities while accessing Internet websites.

On August 27, 2004, Jersey Diesel's owner, Timothy Wilson, was informed by a supplier that Jersey Diesel's shipping address and password had been changed on the supplier's website. Specifically, the supplier's information technology specialist determined that on August 24, 2004, someone had accessed the website, used Jersey Diesel's username and password to sign on, changed Jersey Diesel's address to a non-existent address, and changed the password. The supplier's website captured the user's IP address, which was registered to Comcast. Although Wilson contacted Comcast and requested the subscriber information for the IP address so that he could identify the person who made the unauthorized changes, Comcast declined to respond without a subpoena.

Wilson reported the incident to the Lower Township Police Department and suggested that Shirley Reid, an employee who had been on disability leave, could have made the changes. Reid had returned to work on the morning of August 24, argued with Wilson, and left. According to Wilson, Reid was the only employee who knew the company's computer password and ID.

On September 7, 2004, a subpoena duces tecum issued by the Lower Township Municipal Court was served on Comcast. The subpoena sought all information pertaining to the IP address identified by the supplier for the appropriate time period on August 24th. The subpoena was captioned "Timothy C. Wilson, Plaintiff, vs. Shirley Reed [sic], Defendant," although no such case was pending. On September 16, 2004, Comcast responded and identified Reid as the subscriber of the IP address. Comcast also provided Reid's address, telephone number, type of service provided, IP assignment, account number, e-mail address, and method of payment.

On February 22, 2005, the Cape May County Grand Jury returned an indictment charging Reid with second-degree computer theft. Reid moved to suppress the evidence. The trial court granted the motion. The court identified various flaws in the subpoena and noted that the procedure followed by the police was unauthorized. The court also concluded that Reid had an expectation of privacy in her Internet subscriber information on file with Comcast, therefore the subpoena violated Reid's right to be free from unreasonable searches and seizures.

In a published opinion, the Appellate Division affirmed. 389 N.J. Super. 563 (2007). The panel found the subpoena invalid because it was not issued in connection with any judicial proceeding, was returnable the same day it was issued, and involved an indictable offense outside the jurisdiction of the Municipal Court. The panel also concluded that Reid had a protected privacy interest under the State Constitution in the information provided by Comcast and, as a result, the method used by the police to obtain the information warranted suppression.

HELD: Pursuant to Article I, Paragraph 7, of the New Jersey Constitution, the Court holds that citizens have a reasonable expectation of privacy in the subscriber information they provide to Internet service providers. Accordingly, the motion to suppress by defendant Reid was properly granted because the police used a deficient municipal subpoena. Law enforcement officials can obtain subscriber information by serving a grand jury subpoena on an Internet service provider without notice to the subscriber. The State may seek to reacquire the information with a proper grand jury subpoena because records of the information existed independently of the faulty process

used by the police, and the conduct of the police did not affect the information.

1. Both the Fourth Amendment to the United States Constitution and Article I, Paragraph 7, of the New Jersey Constitution protect the right of the people to be secure against unreasonable searches and seizures. Federal case law interpreting the Fourth Amendment has found no expectation of privacy in Internet subscriber information. On multiple occasions, however, this Court has held that the New Jersey Constitution affords greater protection than the Fourth Amendment. In State v. Hunt, 91 N.J. 338 (1982), this Court concluded that telephone toll billing records are protected and explained that citizens are entitled to assume that the numbers they dial in the privacy of their home will be recorded solely for the telephone company's business purposes. Similarly, in State v. McAllister, 184 N.J. 17 (2005), the Court held that the New Jersey Constitution provides bank account holders a reasonable expectation of privacy in their bank records. (Pp. 12—15).

2. It is well-settled under New Jersey law that disclosure to a third-party provider, as an essential step to obtaining service altogether, does not upend the privacy interest at stake. In order to access the Web, individuals must obtain an IP address from an ISP. Users make disclosures to ISPs for the limited goal of using the technology and not to promote the release of personal information to others. IP address information can be used to track a person's Internet usage, revealing intimate details about his or her personal affairs. Because current technology renders the user's identity anonymous to all except the ISP, users have reason to expect that their actions are confidential when they surf the Web from the privacy of their homes. Therefore, the Court holds that Article I, Paragraph 7, of the New Jersey Constitution protects an individual's privacy interest in the subscriber information that he or she provides to an ISP. (Pp. 15—21).

3. In State v. McAllister, the Court concluded that the constitutional protection against improper government intrusion is satisfied by the issuance of a grand jury subpoena providing that the bank records bear some possible relationship to the grand jury investigation. The Court adopts the same standard for the records at issue in this matter. As in McAllister, the Court also declines to adopt a requirement that notice be provided to account holders whose information is subpoenaed. Unscrupulous individuals aware of subpoenas could delete or damage files on their home computers and thereby effectively shield them from legitimate investigations. (Pp. 21—25).

4. Here, the subscriber information was suppressed because the police department used a defective municipal subpoena. Evidence discovered, directly or indirectly, as a result of a constitutional violation must be suppressed. However, unlike a confession coerced from a defendant in violation of that individuals constitutional rights, Comcast's records existed independently of the faulty process the police followed. Moreover, evidence of Reid's knowledge of the company's password, her argument with Wilson, as well as the supplier's information about the IP address used to access its website remains untainted by the results of the defective municipal subpoena. Because the subscriber information attached to that particular IP address bore some possible relationship to the investigation underway, the State may attempt to reacquire Comcast's records with a proper grand jury subpoena limited to seeking subscriber information for the IP address in question. (Pp. 25—29).

5. The trial court properly suppressed the subscriber information obtained, and the State may not proceed with the pending indictment absent proof that the indictment has a sufficient basis without relying on the suppressed evidence. Alternatively, the State may move to dismiss the pending indictment, re-serve a proper grand jury subpoena on Comcast, and seek a new indictment. (P. 29).

The judgment of the Appellate Division is **MODIFIED and AFFIRMED** and the matter is **REMANDED** to the Law Division for further proceedings consistent with this opinion.

JUSTICES LONG, LaVECCHIA, ALBIN, WALLACE, RIVERA-SOTO and HOENS join in CHIEF JUSTICE RABNER's opinion.

SUPREME COURT OF NEW JERSEY
A-105 September Term 2006

STATE OF NEW JERSEY,

Plaintiff-Appellant,

v.

SHIRLEY REID,

Defendant-Respondent.

Argued October 22, 2007 – Decided April 21, 2008

On appeal from the Superior Court, Appellate Division, whose opinion is reported at 389 N.J. Super. 563 (2007).

Steven A. Yomtov, Deputy Attorney General, argued the cause for appellant (Anne Milgram, Attorney General of New Jersey, attorney).

Joseph C. Grassi argued the cause for respondent (Barry, Corrado, Grassi & Gibson, attorneys; Mr. Grassi and Frank L. Corrado, of counsel and on the briefs).

Rubin M. Sinins argued the cause for amicus curiae Association of Criminal Defense Lawyers of New Jersey (Javerbaum Wurgaft Hicks Kahn Wikstrom & Sinins, attorneys).

Grayson Barber submitted a brief on behalf of amici curiae American Civil Liberties Union of New Jersey, Electronic Frontier Foundation, Electronic Privacy Information Center, Freedom To Read Foundation, Privacy Rights Clearinghouse and New Jersey Library Association (Ms. Barber, attorney; Ms. Barber and Edward L. Barocas, on the brief).

CHIEF JUSTICE RABNER delivered the opinion of the Court.

Modern technology has raised a number of questions that are intertwined in this case: To what extent can private individuals "surf" the "Web" anonymously? Do Internet subscribers have a reasonable expectation of privacy in their identity while accessing Internet websites? And under what circumstances may the State learn the actual identity of Internet users?

In this case, defendant Shirley Reid allegedly logged onto an Internet website from her home computer. The site belonged to a company that supplied material to her employer's business. While on the supplier's website, Reid allegedly changed her employer's password and shipping address to a non-existent address.

Whenever an individual logs onto an Internet website, that user's identity is revealed only in the form of a unique multi-digit number (an "IP address") assigned by the user's Internet Service Provider ("ISP"). A website may collect that number, but only a service provider can translate it into the name of an actual user or subscriber.

Here, the supplier's website captured a 10-digit IP address, and the supplier told Reid's employer what had occurred. The employer, in turn, reported the IP address to local authorities. They issued a deficient municipal subpoena

to Comcast, the service provider, and Comcast revealed that the IP address was assigned to Shirley Reid.

Reid is now under indictment for second-degree computer theft. She successfully moved to suppress the subscriber information obtained via the municipal subpoena.

We now hold that citizens have a reasonable expectation of privacy, protected by Article I, Paragraph 7, of the New Jersey Constitution, in the subscriber information they provide to Internet service providers -- just as New Jersey citizens have a privacy interest in their bank records stored by banks and telephone billing records kept by phone companies. Law enforcement officials can satisfy that constitutional protection and obtain subscriber information by serving a grand jury subpoena on an ISP without notice to the subscriber.

Because the police used a deficient municipal subpoena to obtain protected subscriber information in this case, defendant's motion to suppress was properly granted. However, records of the protected subscriber information existed independently of the faulty process the police used, and the conduct of the police did not affect that information. As a result, the State may seek to reacquire the subscriber information with a proper grand jury subpoena.

I.

A.

Some background information about computers and the Internet may assist in evaluating the issues presented. The Internet is a global network of computers that allows for the "sharing" or "networking" of information to and from remote locations. See Harry Newton, Newton's Telecom Dictionary 502 (23rd ed. 2007). Users of the Internet can send electronic mail, share files, and explore or "surf" the World Wide Web ("Web"), a graphical computer-based information network. Id. at 502-03. While surfing the Web, a user can visit and interact with sites maintained by businesses, educational institutions, governments, and individuals, which cover almost every conceivable topic.

An individual customer must select an Internet Service Provider like Comcast, AOL, or Verizon, in order to connect to the Internet. See, e.g., id. at 107. To sign up for service, a customer must disclose personal information including one's name, billing information, phone number, and home address.

To interact with other computers also attached to the Internet, a computer must be assigned an Internet Protocol address, or IP address. Id. at 342. An IP address is a string of up to twelve numbers separated by dots -- for example, 123.45.67.89. Ibid. In certain situations, a computer is

assigned a permanent IP address, called a static IP address. Ibid. Most often, when an individual connects to the Internet, his or her Internet Service Provider dynamically assigns an IP address to the computer, which can change every time the user accesses the Internet. Ibid. In other words, the "dynamic" IP address assigned to the computer can be different for each Internet session. Ibid.

The American Registry for Internet Numbers (ARIN) is in charge of assigning IP addresses within North America. See http://www.arin.net/index.shtml. Anyone acquiring an IP address must register and provide ARIN certain contact information, which ARIN makes publicly available. Ibid. However, most Internet users do not obtain IP addresses directly from ARIN; they instead "lease" an IP address from a service provider like Comcast, which is the actual, named registrant. See RIR Comparative Policy Overview (2008), http://www.nro.net/documents/nro47.html (last visited April 16, 2008) (linked to ARIN website).

When an Internet user surfs the Web, sends e-mail, or shares a file, any site the user connects to can collect certain information, including the user's IP address. See Newton, supra, at 506. However, the sites ordinarily cannot identify the name of an individual user. Only the ISP can match the name of the customer to a dynamic IP address.

Recently, IP Address Locator Websites have become available to the general public.[1] Such websites operate similarly to a reverse phone directory: they permit a person to type in an IP address and obtain the name and location of the registrant for that address. Once again, because most Internet users access the Internet via third-party service providers like AOL, Comcast, Yahoo, and others, Address Locator Websites typically reveal the name and location of the service provider -- such as Comcast -- but not information about the individual user.

Thus, even with the advent of IP Address Locator Websites, most users continue to enjoy relatively complete IP address anonymity when surfing the Web.

B.

The facts of this case are not in dispute. On August 27, 2004, Timothy Wilson, the owner of Jersey Diesel, reported to the Lower Township Police Department that someone had used a computer to change his company's shipping address and password for its suppliers. The shipping address was changed to a non-existent address.

In response to a question by the police, Wilson explained that Shirley Reid, an employee who had been on disability leave,

[1] Websites providing this service include: GeoBytes IP Address Locator Tool, http://www.geobytes.com/IpLocator.htm; IP-address.com, http://www.ip-adress.com/ipaddresstolocation/; and IP Address Location, http://www.ipaddresslocation.org/.

could have made the changes. Reid returned to work on the morning of August 24, had an argument with Wilson about her temporary light duty assignment, and left. According to Wilson, Reid was the only employee who knew the company's computer password and ID.

Wilson learned of the changes through one of his suppliers, Donaldson Company, Inc. Both the password and shipping address for Jersey Diesel had been changed on Donaldson's website on August 24, 2004. According to an information technology specialist at Donaldson, someone accessed their website and used Jersey Diesel's username and password to sign on at 9:57 a.m. The individual changed the password and Jersey Diesel's shipping address and then completed the requests at 10:07 a.m.

Donaldson's website captured the user's IP address, 68.32.145.220, which was registered to Comcast. When Wilson contacted Comcast and asked for subscriber information associated with that address -- so that he could identify the person who made the unauthorized changes -- Comcast declined to respond without a subpoena.

On September 7, 2004, a subpoena duces tecum issued by the Lower Township Municipal Court was served on Comcast. The subpoena sought "[a]ny and all information pertaining to IP Address information belonging to IP address: 68.32.145.220, which occurred on 08/24/04 between 8:00 a.m. and 11:00 a.m.

EST." The subpoena was captioned "Timothy C. Wilson, Plaintiff, vs. Shirley Reed [sic], Defendant," although no such case was pending.

Comcast responded on September 16, 2004 and identified Reid as the subscriber of the IP address. In addition, Comcast provided the following information: Reid's address, telephone number, type of service provided, IP assignment (dynamic), account number, e-mail address, and method of payment.

An arrest warrant was issued on September 29, 2004, and Reid was arrested ten days later. On February 22, 2005, the Cape May County Grand Jury returned an indictment charging Reid with second-degree computer theft, in violation of N.J.S.A. 2C:20-25(b).

Reid moved to suppress the evidence obtained via the municipal court subpoena. On September 22, 2005, the trial court granted Reid's motion. The court identified various flaws with the municipal court subpoena and noted that the procedure followed by the police was "unauthorized in its entirety." The court also concluded that Reid had an expectation of privacy in her Internet subscriber information on file with Comcast. Therefore, the trial court held that the subpoena violated Reid's "right to be free from unreasonable searches and seizures" and was unconstitutional.

The Appellate Division, in a published opinion, affirmed the order of suppression. State v. Reid, 389 N.J. Super. 563 (App. Div.), appeal granted, 190 N.J. 250 (2007). First, the panel found the subpoena invalid for a number of reasons: it was not issued in connection with any judicial proceeding; was returnable the same day it was issued; and involved an indictable offense outside the jurisdiction of the Municipal Court. Id. at 568. Next, the panel concluded that Reid had a protected privacy interest under the State Constitution in the subscriber information obtained from Comcast. As a result, the method the police used to obtain that information warranted suppression.

The panel reasoned that "New Jersey appears to have recognized a right to what has been called 'informational privacy.'" Id. at 570. Quoting from a law review article, the court adopted the following formulation of that right:

> [informational privacy] encompasses any information that is identifiable to an individual. This includes both assigned information, such as a name, address, or social security number, and generated information, such as financial or credit card records, medical records, and phone logs . . . . [P]ersonal information will be defined as any information, no matter how trivial, that can be traced or linked to an identifiable individual.

> [Ibid. (quoting Elbert Lin, Prioritizing Privacy: A Constitutional Response to the Internet, 17 Berkeley Tech. L.J. 1085, 1096-97 (2002)).]

In support of this precept, the panel cited to State v. Hunt, 91 N.J. 338 (1982), State v. Hempele, 120 N.J. 182 (1990), and State v. McAllister, 184 N.J. 17 (2005).

The panel concluded that information on file with Comcast concerning the identity of Internet users fell within the protected privacy right. Accordingly, that information could "only be obtained by law enforcement through some means of proper judicial process." Reid, supra, 389 N.J. Super. at 575.

On March 15, 2007, this Court granted the State's motion for leave to appeal. 190 N.J. 250 (2007).

II.

The State contends that there is no reasonable expectation of privacy in subscriber information provided to one's ISP. The State submits that State v. Evers, 175 N.J. 355 (2003), has already resolved that question. Because no constitutional violation occurred, the State asserts that suppression of the evidence obtained through the invalid municipal court subpoena is not required.

If the Court were to recognize a privacy interest, the State argues that a grand jury subpoena would be legally sufficient to gain access to subscriber information, consistent

with the holdings in McAllister, supra, 184 N.J. 17, and State v. Domicz, 188 N.J. 285 (2006). Notice to a subscriber should not be required, the State maintains, because that would "severely impede investigations into criminal activity." The State also points to New Jersey's Wiretapping and Electronic Surveillance Control Act, N.J.S.A. 2A:156A-1 to -34 -- and to N.J.S.A. 2A:156A-29 in particular -- as authority for the use of grand jury or trial subpoenas to obtain ISP subscriber information.

Reid asks us to affirm the Appellate Division's holding and find a constitutional right of privacy in internet subscriber information. Reid argues that Evers, supra, did not settle the issue. In addition, Reid submits that suppression is the proper remedy for a violation of her constitutional right.

Reid also urges this Court to require notice to the Internet user whenever the government, using judicial process, seeks subscriber information from an ISP. The State could avoid the notice requirement in a given case if it were able to justify an exception to that rule.

We granted amicus curiae status to the Association of Criminal Defense Lawyers of New Jersey (ACDL) as well as the American Civil Liberties Union of New Jersey (ACLU). (The ACLU submitted a brief on behalf of itself and the Electronic Frontier Foundation, Electronic Privacy Information Center,

Freedom to Read Foundation, Privacy Rights Clearinghouse, and New Jersey Library Association.)

All amici contend that there is a reasonable expectation of privacy under the New Jersey Constitution with regard to ISP subscriber information. They also argue for contemporaneous notice to the Internet user when the government seeks such information. In case of a violation of the constitutionally protected privacy right, they argue that suppression is required. They submit that statutory civil remedies are insufficient to protect an individual's right of privacy.

III.

We first consider the existence of a New Jersey citizen's privacy interest in Internet subscriber information.

A.

Both the Fourth Amendment to the United States Constitution and Article I, Paragraph 7, of the New Jersey Constitution protect, in nearly identical language, "the right of the people to be secure . . . against unreasonable searches and seizures."

Federal case law interpreting the Fourth Amendment has found no expectation of privacy in Internet subscriber information. See Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001); Freedman v. America Online, Inc., 412 F. Supp. 2d 174, 181 (D. Conn. 2005); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005); United States v. Cox, 190 F. Supp. 2d

330, 332 (N.D.N.Y. 2002); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kans. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 508-09 (W.D. Va. 1999), aff'd, 225 F.3d 656 (4th Cir. 2000), cert. denied, 531 U.S. 1099, 121 S. Ct. 832, 148 L. Ed. 2d 714 (2001). Those decisions draw on settled federal law that a person has no reasonable expectation of privacy in information exposed to third parties, like a telephone company or bank. See Smith v. Maryland, 442 U.S. 735, 742, 99 S. Ct. 2577, 2581, 61 L. Ed. 2d 220, 227 (1979) (finding no privacy interest in telephone numbers dialed); United States v. Miller, 425 U.S. 435, 442, 96 S. Ct. 1619, 1624, 48 L. Ed. 2d 71, 79 (1976) (finding no privacy interest in bank records). The logic of those precedents extends to subscriber information revealed to an ISP.

Our inquiry does not end there because "despite the congruity of the language," the search and seizure protections in the federal and New Jersey Constitutions "are not always coterminous." Hunt, supra, 91 N.J. at 344. Indeed, on multiple occasions this Court has held that the New Jersey Constitution "affords our citizens greater protection against unreasonable searches and seizures" than the Fourth Amendment. State v. Novembrino, 105 N.J. 95, 145 (1987) (finding that Article I, Paragraph 7, unlike Fourth Amendment, does not provide good-faith exception to exclusionary rule); see also Planned

Parenthood of Cent. N.J. v. Farmer, 165 N.J. 609, 629 (2000) (noting New Jersey's "long-standing history" of commitment to protection of privacy rights); Doe v. Poritz, 142 N.J. 1, 89-90 (1995) (noting "a constitutional right of privacy in . . . the disclosure of confidential or personal information").

During the past twenty-five years, a series of New Jersey cases has expanded the privacy rights enjoyed by citizens of this state. In 1982, this Court concluded in Hunt, supra, that telephone toll billing records are "part of the privacy package." 91 N.J. at 347. In language that resonates today on the subject of computers, the Court observed that "[t]he telephone has become an essential instrument in carrying on our personal affairs." Id. at 346. Moreover, a list of telephone numbers dialed in the privacy of one's home "'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, supra, 442 U.S. at 748, 99 S. Ct. at 2584, 61 L. Ed. 2d at 231 (Stewart, J., dissenting)).

Finding that Article I, Paragraph 7, of the New Jersey Constitution provides more protection than federal law affords, this Court concluded that a person "is entitled to assume that the numbers he dials in the privacy of his home will be recorded solely for the telephone company's business purposes." Id. at

345, 347. The Court rejected the underpinnings of federal case law by explaining that

> [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 this information. . . . This disclosure has been necessitated because of the nature of the instrumentality, but more significantly the disclosure has been made for a limited business purpose and not for release to other persons for other reasons.
>
> [Id. at 347.]

More recently, in McAllister, supra, this Court held that the New Jersey Constitution provides bank account holders a reasonable expectation of privacy in their bank records. 184 N.J. at 32-33. As in Hunt, the Court noted that bank accounts "have become an indispensable part of modern commerce" for our citizens. Id. at 31. Like long distance billing records, bank records reveal a great deal about the personal affairs, opinions, habits, and associations of depositors. Id. at 30-31. The Court also noted that, although bank customers voluntarily provide information to banks, "they do so with the understanding that it will remain confidential." Id. at 31. The disclosure is done to facilitate financial transactions, not to enable banks to broadcast the affairs of their customers.

B.

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.

Individuals need an ISP address in order to access the Internet. However, when users surf the Web from the privacy of their homes, they have reason to expect that their actions are confidential. Many are unaware that a numerical IP address can be captured by the websites they visit. More sophisticated users understand that that unique string of numbers, standing alone, reveals little if anything to the outside world. Only an Internet service provider can translate an IP address into a user's name.

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.

The State compares IP addresses to the return addresses found on the outside of envelopes, which carry no privacy protection. But there is an important difference: letter writers choose to include their address on an envelope. They may also opt for anonymity and list no return address. Internet users have no such choice because they must have an IP address to access a website. In addition, the string of numbers that comprises an IP address and can be collected by a website is both less revealing and less public than a name or street address posted on an envelope.

It is well-settled under New Jersey law that disclosure to a third-party provider, as an essential step to obtaining service altogether, does not upend the privacy interest at stake. See McAllister, supra, 184 N.J. at 31; Hunt, supra, 91 N.J. at 347. In the world of the Internet, the nature of the technology requires individuals to obtain an IP address to access the Web. Users make disclosures to ISPs for the limited goal of using that technology and not to promote the release of

personal information to others. Under our precedents, users are entitled to expect confidentiality under these circumstances.[2]

For all of those reasons, we find that Article I, Paragraph 7, of the New Jersey Constitution protects an individual's privacy interest in the subscriber information he or she provides to an Internet service provider.[3]

This Court's decision in Evers does not hold otherwise. In Evers, a deputy sheriff in California was investigating the use of child pornography on the Internet. He connected to AOL, entered a chat room whose name suggested sexual activity involving children, and sent an e-mail that allowed other AOL subscribers interested in the subject matter to communicate with him. Evers, supra, 175 N.J. at 365. He received responses from ninety-eight different screen names, including one response containing images of a nude female child in a sexually

---

[2] Users, of course, may waive their expectation of confidentiality in any number of ways. People routinely identify themselves on a website when they make a purchase or complete a survey. Likewise, employees often waive any privacy interests in their use of work-related computers as a condition of employment. No such waiver occurred here.

[3] We decline to adopt the "informational privacy" standard outlined by the Appellate Division. See Reid, supra, 389 N.J. Super. at 570. The contours and breadth of the standard are not entirely clear, and we need not address those issues in resolving the narrower constitutional question before us. See Bell v. Twp. of Stafford, 110 N.J. 384, 389 (1988) (court should not reach constitutional issues unless absolutely imperative to dispose of the litigation). The privacy right established here pertains to subscriber information held by an ISP.

provocative position. That response was also sent to fifty other users. Ibid.

The deputy obtained a search warrant to learn the identities associated with the ninety-eight screen names and served the warrant on AOL's corporate headquarters in Dulles, Virginia. AOL, in turn, provided names and billing addresses for the requested screen names. Ibid. Because the person who sent the pornographic images resided in Nutley, New Jersey, the deputy forwarded the information to the Nutley Police Department. The Department acquired a warrant to search defendant's house. Id. at 366.

Evers claimed he had a reasonable expectation of privacy in the contents of the e-mail of the nude girl. This Court quickly dispensed with his argument, noting that Evers had forwarded the e-mail to fifty-one recipients at his peril that one of them would disclose his wrongdoing. Id. at 370.

The Court next asked whether defendant had a privacy interest in the subscriber information stored at AOL headquarters in Virginia. Ibid. Without reaching the substantive question under New Jersey law, the Court acknowledged that "[n]o purpose would be served by applying New Jersey's constitutional standards to people and places over which the sovereign power of the state has no power or control." Id. at 371 (citing State v. Mollica, 114 N.J. 329, 347 (1989)).

As a result, the Court declined to hold, as a matter of New Jersey law, that defendant had a privacy right in the subscriber information at AOL headquarters in Virginia, sought by a California law enforcement officer. Ibid. Because no privacy right existed under federal law, for reasons discussed above, the Court concluded that defendant had no privacy interest in the subscriber information. Id. at 374. Viewed in its entire context, Evers saved for another day the issue we now address.

The New Jersey Wiretapping and Electronic Surveillance Control Act ("Wiretap Act"), N.J.S.A. 2A:156A-1 to -34, offers additional support for concluding that internet users have a reasonable expectation of privacy in their own subscriber information kept by an ISP. The Wiretap Act provides for disclosure of subscriber information, including name, address, telephone number, and means of payment, only when a law enforcement agency obtains "a grand jury or trial subpoena or when the State Commission of Investigation issues a subpoena." N.J.S.A. 2A:156A-29(f). The Legislature's decision to protect disclosure of ISP information absent a subpoena is consistent with the privacy protection we recognize today.

One additional point bears mention about the right to privacy in ISP subscriber information: the reasonableness of the privacy interest may change as technology evolves. A reasonable expectation of privacy is required to establish a

protected privacy interest. Hempele, supra, 120 N.J. at 200. As discussed in section I(A), supra, Internet users today enjoy relatively complete IP address anonymity when surfing the Web. Given the current state of technology, the dynamic, temporarily assigned, numerical IP address cannot be matched to an individual user without the help of an ISP. Therefore, we accept as reasonable the expectation that one's identity will not be discovered through a string of numbers left behind on a website.

The availability of IP Address Locator Websites has not altered that expectation because they reveal the name and address of service providers but not individual users. Should that reality change over time, the reasonableness of the expectation of privacy in Internet subscriber information might change as well. For example, if one day new software allowed individuals to type IP addresses into a "reverse directory" and identify the name of a user -- as is possible with reverse telephone directories -- today's ruling might need to be reexamined.

C.

We turn next to the type of protection ISP subscriber information should receive in the face of legitimate investigative needs. The Appellate Division found that "some

means of proper judicial process" was necessary but did not specify what level. Reid, supra, 389 N.J. Super. at 575.

Reid argues that, at a minimum, a valid grand jury subpoena issued on notice to the subscriber is required. The ACDL submits that a grand jury subpoena with contemporaneous notice is required. The ACLU contends that the State should satisfy a heightened standard in criminal cases either by obtaining judicial approval or giving notice to the target of the investigation so that the target can challenge a subpoena. All three argue that subscriber information is deserving of greater protection than bank records. They all also cite to a standard in the civil arena for discovery of information held by an ISP.[4] In addition, all three argue that an individual subscriber has a greater incentive than an ISP in challenging a request by the State for subscriber information.

[4] Defendant and amici argue that the State should at least be required to satisfy the standard set forth in Dendrite Int'l, Inc. v. John Doe No. 3, 342 N.J. Super. 134 (App. Div. 2001). Dendrite was a civil defamation action in which a corporation sued John Doe defendants for posting a message on an ISP's bulletin board. Plaintiff sought discovery compelling the ISP to disclose the defendants' identities. Id. at 140. In affirming the trial court's denial of the discovery request, the Appellate Division provided guidance to courts seeking to strike a balance between the First Amendment right to anonymous speech and a defamation claimant's reputational and proprietary interests. Id. at 141-42. We express no view today on the appropriate standard for disclosure of ISP subscriber information in civil cases, and we decline to import Dendrite's holding to the grand jury context.

Recent case law informs our discussion. In McAllister, supra, this Court concluded that issuance of a grand jury subpoena to obtain bank records, upon a showing of relevance, satisfies the constitutional protection against improper government intrusion. 184 N.J. at 36. The Court further found that notice to the account holder was not constitutionally required. Id. at 37. The same principles apply here.

In McAllister, the Court rejected arguments similar to those advanced in this case. In declining to adopt a heightened standard of probable cause to support the issuance of a grand jury subpoena, the Court found guidance in the words of Chief Justice Weintraub, writing in In re Addonizio, 53 N.J. 107 (1968). He declared that "the 'probable cause' required for a search warrant is foreign to [the grand jury] scene." Id. at 126. His explanation rings true today:

> [A grand jury's] power to investigate would be feeble indeed if the grand jury had to know at the outset everything needed to arrest a man or to invade his home. Nor would it serve the public interest to stay a probe until the grand jury reveals what it has or what it seeks. Such disclosures could defeat the inquiry and impede the apprehension of the culprit. This is one of the reasons why the law cloaks the grand jury investigation with secrecy.
>
> [Ibid.]

Since Addonizio, "New Jersey courts have consistently affirmed the expansive investigatory power of grand juries."

McAllister, supra, 184 N.J. at 34. That power rests on the grand jury's ability to issue subpoenas to gather information -- a power that must always be exercised in good faith and in accordance with established rules to avoid possible abuses. Under those rules, grand jury subpoenas may be issued based on a relevancy standard: the documents must "bear some possible relationship, however indirect, to the grand jury investigation." Ibid. (quoting In re Grand Jury Subpoena Duces Tecum, 167 N.J. Super. 471, 473 (App. Div. 1979) (per curiam)).

More recently, in Domicz, supra, this Court determined that acquiring electric utility records with a grand jury subpoena was proper under our Constitution. 188 N.J. at 297. The Court noted that "whatever privacy interest attached" to utility records, obtaining them through the use of a grand jury subpoena satisfies Article I, Paragraph 7, of the State Constitution. Id. at 297. Again, based on a relevancy standard, the Court declined to suppress the evidence obtained. Id. at 300.

Utility records expose less information about a person's private life than either bank records or subscriber information. But we see no material difference between bank records and ISP subscriber information and decline to treat them differently. They reveal comparably detailed information about one's private affairs and are entitled to comparable protection under our law.

In both cases, a grand jury subpoena based on a relevancy standard is sufficient to meet constitutional concerns.

In addition, as in McAllister, we decline to adopt a requirement that notice be provided to account holders whose information is subpoenaed. See 184 N.J. at 37-40. For obvious reasons, notice could impede and possibly defeat the grand jury's investigation. Particularly in the case of computers, unscrupulous individuals aware of a subpoena could delete or damage files on their home computer and thereby effectively shield them from a legitimate investigation. Banks maintain copies of the records they send their customers. But ISP providers do not have a back-up file of the information maintained on a home computer. As a result, notice could be even more damaging to an investigation in this arena.

As we noted in Addonizio and McAllister, "[o]ur grand jury process -- bounded by relevancy and safeguarded by secrecy -- conforms to our jurisprudence," and "[t]he New Jersey Constitution does not require more." McAllister, supra, 184 N.J. at 42 (citing Addonizio, supra, 53 N.J. at 126-28).

D.

The police in this case used a defective municipal subpoena to obtain Reid's ISP subscriber information from Comcast. We turn now to the consequences that flow from this violation of her rights.

Violations of constitutionally protected rights implicate the exclusionary rule. Under the exclusionary rule, the State may not introduce evidence obtained unlawfully by the police; evidence discovered, directly or indirectly, as a result of a constitutional violation must be suppressed. State v. Lee, 190 N.J. 270, 277-78 (2007) (citing Wong Sun v. United States, 371 U.S. 471, 487-88, 83 S. Ct. 407, 417, 9 L. Ed. 2d 441, 455 (1963)); State v. Hartley, 103 N.J. 252, 282-83 (1986) (citing Oregon v. Elstad, 470 U.S. 298, 308, 105 S. Ct. 1285, 1292, 84 L. Ed. 2d 222, 231 (1985)). The purpose of the rule is to deter police misconduct and encourage respect for protected rights. State v. Worthy, 141 N.J. 368, 385 (1995). As a result, the subscriber information obtained in this case, by way of a defective municipal court subpoena, was properly suppressed.[5]

The subscriber information Comcast disclosed lies at the core of the indictment against Reid. Without it, she would not have been identified. It is therefore difficult in this case to see how the pending indictment can survive suppression. By

[5] The Wiretap Act does not provide an adequate remedy. Under the Act, an aggrieved person challenging the interception of content information -- such as the contents of an intercepted wire, electronic, or oral communication intercepted unlawfully -- may bring a motion to suppress. N.J.S.A. 2A:156A-21. But an aggrieved customer whose subscriber information was obtained without a grand jury subpoena, as required by N.J.S.A. 2A:156A-29, may only recover civil damages and attorney's fees. N.J.S.A. 2A:156A-32 & -34.

contrast, in Hunt, supra, introduction of the toll billing records was "too insignificant to have had any bearing" on the trial and was therefore harmless error. 91 N.J. at 350. In addition, the Court noted that if "subsequently obtained evidence was acquired from an independent source," or if the "causal connection between the illegal conduct and the discovery of the challenged evidence was 'so attenuated' that the taint was dissipated," the evidence could be admitted. Id. at 349 (citations omitted). As a result, evidence uncovered through court orders or search warrants that rested on other lawfully obtained information was not subject to suppression. Ibid.

Suppression under the circumstances present here does not mean that the evidence is lost in its entirety. Comcast's records existed independently of the faulty process the police followed. And unlike a confession coerced from a defendant in violation of her constitutional rights, the record does not suggest that police conduct in this case in any way affected the records Comcast kept. As a result, the records can be reliably reproduced and lawfully reacquired through a proper grand jury subpoena.

This outcome is readily apparent if viewed in the context of a motion to quash. Had Comcast sought to quash the municipal court subpoena, the trial court would have granted that relief for the same reasons it gave at the motion to suppress. At that

point, nothing would have prevented the police from seeking the subscriber information from Comcast a second time, this time armed with an appropriate grand jury subpoena. See State v. Bodtmann, 239 N.J. Super. 33, 46 n.10 (App. Div. 1990) (explaining that where grant of motion to suppress is not a ruling on the admissibility of blood alcohol test results obtained via subpoena, "the decision then would be tantamount to quashing the subpoena," in which case police could make application for new subpoena supported by objective facts known at or near time of event).

The record in this case includes a police report prepared before the police sought the defective municipal subpoena. According to the report, Reid's employer, Mr. Wilson, relayed to police that someone used a computer to change his company's password and shipping address with his suppliers, that Reid was the only employee who knew the password, and that he and Reid had argued earlier in the day before she walked out of the office. Further, before the municipal subpoena was obtained, Wilson's supplier relayed the specific IP address of the computer that had accessed the supplier's website and changed Wilson's company's username, password, and shipping address. Under any reasonable interpretation, the subscriber information attached to that particular IP address bore "some possible

relationship" to the investigation underway. See McAllister, supra, 184 N.J. at 34.

All of the above information remains untainted by the results of the defective municipal subpoena. Therefore, the State may attempt to reacquire Comcast's records with a proper grand jury subpoena limited to seeking subscriber information for the IP address in question.[6]

To recap, the trial court properly suppressed the subscriber information obtained, and the State may not proceed with the pending indictment absent proof that the indictment has a sufficient basis without relying on the suppressed evidence. Alternatively, the State may move to dismiss the pending indictment, re-serve a proper grand jury subpoena on Comcast, and seek a new indictment.

IV.

For the above reasons, we modify and affirm the judgment of the Appellate Division and remand to the Law Division for further proceedings consistent with this opinion.

JUSTICES LONG, LaVECCHIA, ALBIN, WALLACE, RIVERA-SOTO, and HOENS join in CHIEF JUSTICE RABNER's opinion.

---

[6] Reid and the amici curiae also raise questions about the breadth of the municipal court subpoena served on Comcast. Comcast provided only subscriber information in response, but Reid and the amici argue the subpoena sought additional information that would have required a court order under the Wiretap Act. In light of our ruling, we need not resolve that claim.

SUPREME COURT OF NEW JERSEY

NO. A-105 SEPTEMBER TERM 2006

ON APPEAL FROM Appellate Division, Superior Court

STATE OF NEW JERSEY,

Plaintiff-Appellant,

v.

SHIRLEY REID,

Defendant-Respondent.

DECIDED April 21, 2008

Chief Justice Rabner PRESIDING

OPINION BY Chief Justice Rabner

CONCURRING/DISSENTING OPINION BY

DISSENTING OPINION BY

CHECKLIST	MODIFY AND AFFIRM/ REMAND	
CHIEF JUSTICE RABNER	X	
JUSTICE LONG	X	
JUSTICE LaVECCHIA	X	
JUSTICE ALBIN	X	
JUSTICE WALLACE	X	
JUSTICE RIVERA-SOTO	X	
JUSTICE HOENS	X	
TOTALS	7	