

State v. Reid, \_\_\_\_ N.J. Super. \_\_\_\_ (App. Div. 2007).

The following summary is not part of the opinion of the court. Please note that, in the interest of brevity, portions of the opinion may not have been summarized.

We held that an internet subscriber has an expectation of privacy in information on file with the internet provider identifying her as the user associated with an anonymous "screen name." Since the police obtained that identifying information by means of an invalid subpoena, issued by a municipal court administrator and returnable on the date of issuance, the order suppressing the evidence obtained from the internet provider was affirmed.

The full text of the case follows.

\*\*\*\*\*

NOT FOR PUBLICATION WITHOUT THE  
APPROVAL OF THE APPELLATE DIVISION

SUPERIOR COURT OF NEW JERSEY  
APPELLATE DIVISION  
DOCKET NO. A-3424-05T5

STATE OF NEW JERSEY,

Plaintiff-Appellant,

v.

SHIRLEY REID,

Defendant-Respondent.

**APPROVED FOR PUBLICATION**

**January 22, 2007**

**APPELLATE DIVISION**

Submitted November 28, 2006 - Decided

January 22, 2007

Before Judges Kestin, Weissbard and Graves.

On appeal from Superior Court of New  
Jersey, Law Division, Cape May County,  
Ind. No. 05-02-0121.

Robert L. Taylor, Cape May County  
Prosecutor, attorney for appellant  
(J. Vincent Molitor, Assistant Prosecutor,  
of counsel and on the brief).

Barry, Corrado, Grassi, & Gibson, attorneys  
for respondent (Joseph C. Grassi, on the brief).

The opinion of the court was delivered by  
WEISSBARD, J.A.D.

The State appeals, pursuant to leave granted, from an order suppressing evidence obtained from Comcast Internet Service, the internet service provider (ISP) for defendant Shirley Reid. The evidence consisted of information on file with Comcast that identified defendant as the user of a coded screen name.<sup>1</sup> Addressing an issue of first impression, we conclude that defendant had an expectation of privacy under our State Constitution with respect to this identifying information that permitted her to challenge the manner in which it was obtained by the police. Since we also conclude that the method used by the police was unlawful, we affirm the order of suppression.

We take the following facts from defendant's brief.<sup>2</sup> On August 27, 2004, Patrolman Charles Fitzmaurice of the Lower Township Police Department handled a walk-in complaint by Timothy Wilson regarding theft via computer. Wilson, the owner of Jersey Diesel, told police someone had broken into his computer system on August 24,

---

<sup>1</sup> "A 'screen name' is an identity created by a user and may or may not have any correlations with the user's real name." Thomas K. Clancy, Symposium: The Search and Seizure of Computers and Electronic Evidence: The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, 75 Miss. L.J. 193, 251 (2005).

<sup>2</sup> In violation of our rules, R. 2:6-2(a)(4), defendant has provided no appendix reference in support of these facts. Nevertheless, since they appear to have come from discovery provided by the State, and because the State has not objected to them, we accept them as accurate background for the purposes of this opinion.

2004, and changed his shipping address and password for all of his suppliers. The shipping address was changed to a non-existent address.

During his conversation with the patrolman, Wilson mentioned that Shirley Reid, an employee who had been out on disability leave, could have made the changes to his account. Wilson said Reid reported for work on August 24 and was not happy with the decision to place her on light duty. An argument ensued between Wilson and Reid, and Reid left the premises. Wilson added that Reid was the only person in the company that knew the company password and ID.

Wilson learned through one of his suppliers that changes had been made to his password and shipping address. As a result, he started to investigate the changes. He discovered the changes were made by someone with an Internet Provider address that was owned by Comcast. Wilson then contacted Comcast to determine the name of the person responsible and was informed that a subpoena was required before Comcast would release any information.

The case was turned over to Lower Township detectives. On September 7, 2004, Detective Robert Smith went to Lower Township Municipal Court to obtain a subpoena duces tecum. Elizabeth Byrne, the Court Administrator of Lower Township Municipal Court, issued the subpoena to Comcast Internet Service. The subpoena read as follows:

The State of New Jersey, To: COMCAST INTERNET  
SERVICE

You are hereby commanded to attend and give  
testimony before the Lower Township Municipal Court at 401  
Breakwater Road, Erma, New Jersey on the 7TH day of

SEPTEMBER, 2004, At 3:00 o'clock P.M., on the part of LOWER TOWNSHIP POLICE DEPARTMENT in the entitled action, and that you have and bring with you and produce at the same time and place, the following: **Any 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. This information pertains to Comcast case #: NA338384.**

Failure to appear according to the command of this Subpoena will subject you to a penalty, damage in a Civil Suit and punishment for contempt of Court.

Elizabeth Byrne, Court Administrator  
Lower Township Municipal Court

Detective Smith then faxed the subpoena to Shamma Austin, a Comcast employee.

On September 16, 2004, Comcast responded to the subpoena and provided information which implicated Reid. An arrest warrant was issued on September 29, and on October 8, Reid was arrested. She was subsequently charged in a single-count indictment with computer related theft, in violation of N.J.S.A. 2C:20-25b.

In an oral opinion, the motion judge found that defendant had a reasonable expectation of privacy in her internet subscriber information on file with Comcast and that the procedure used to obtain that information was "unauthorized in its entirety." As a result, the use of the subpoena to obtain this constitutionally protected information violated defendant's right to be free from unreasonable searches and seizures. The judge did not indicate whether it was defendant's state or federal right that was violated.

We deal first with the procedure utilized by the police. The subpoena issued by the Court Administrator was not in connection with any judicial proceeding; indeed, it was made returnable the same day it was issued. Clearly, it was utilized simply as a device to obtain the desired information. And while a court clerk may issue a subpoena,

R. 1:9-1, the crime under investigation here involved an indictable offense, not within the jurisdiction of the Municipal Court. See R. 7:7-8. In any event, it is a prerequisite for the valid issuance of a subpoena that the body before which it is returnable at least be in session on the return date. See State v. Hilltop Private Nursing Home, Inc., 177 N.J. Super. 377, 396 (App. Div. 1981); State v. Stelzner, 257 N.J. Super. 219, 235-36 (App. Div.), certif. denied 130 N.J. 396 (1992). Our Rules give neither the police nor prosecutors a general investigative subpoena power, independent of a grand jury or other judicial proceeding then in session. See Matter of Nackson, 221 N.J. Super. 187, 205 (App. Div. 1998) (citing Hilltop, supra, 177 N.J. Super. at 389-90), aff'd 114 N.J. 527 (1989); In the Matter of a Grand Jury Subpoena, \_\_\_ N.J. Super. \_\_\_ (App. Div. 2006) (slip op. at 8). The subpoena at issue in this case clearly violated these precepts and was invalid. The State's reliance on State v. Dyal, 97 N.J. 229 (1984), is misplaced. While Dyal held that in a drunk driving prosecution the police could obtain hospital records as part of their investigation, and could do so even when no case was yet pending, id. at 240-41, the Court held that the proper procedure was for the police to present "an application for a subpoena before a judicial officer, generally a municipal court judge having jurisdiction in the municipality where the records are located." Id. at 240. Thus, Dyal provides no support for the validity of the subpoena issued here to Comcast Internet Service. As we stated in another context, but in words applicable here, "the subpoena power is a significant one which must be exercised in good faith and in strict adherence to the rules to eliminate potential abuses." Cavallaro v. Jamco Prop. Mgmt., 334 N.J. Super. 557, 569 (App. Div. 2000); see also Crescenzo v. Crane, 350 N.J. Super. 531 (App. Div.), certif. denied, 174 N.J. 364 (2002).

Yet, despite the invalidity of the subpoena, the judge's ruling might still be subject to reversal if defendant had no privacy interest in the information obtained from Comcast. If there were no constitutionally protected privacy interest, it would not matter how the police obtained the information. Thus, we turn to that issue.

The precise question we confront has been uniformly answered in the negative by the federal courts, all of which have held that internet subscribers have no right of privacy under the Fourth Amendment with respect to identifying information on file with their internet service providers. See Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000), aff'd, 106 Fed. Appx. 688 (10th Cir. 2004); United States v. Hambrick, 55 F. Supp. 2d 504 (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); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002). This result followed inexorably from Supreme Court precedent which "consistently has held 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, 442-43, 96 S. Ct. 1619, 1624, 48 L. Ed. 2d 71, 78-79 (1976); United States v. Payner, 447 U.S. 727, 731-32, 100 S. Ct. 2439, 2444, 65 L. Ed. 2d 468, 474 (1980).<sup>3</sup>

---

<sup>3</sup> Two states have likewise found no expectation of privacy in internet subscriber information, relying solely upon federal case law. Hause v. Commonwealth, 83 S.W.3d 1, 25-29 (Ky. Ct. App. 2001); In re Forgione, 908 A.2d 593, 607-08 (Conn. Super. Ct. 2006).

However, the right to privacy of New Jersey citizens under our State Constitution has been expanded to areas not afforded such protection under the Fourth Amendment. While ten states have explicit rights to privacy in their state constitutions, Lin, Prioritizing Privacy: A Constitutional Response to the Internet, 17 Berkeley Tech. L.J. 1085, 1129-30 (2002), New Jersey is among the few states to have found an implied right to privacy in its state charter.<sup>4</sup> Lin, supra, at 1141-42; see Doe v. Poritz, 142 N.J. 1, 89 (1995). Of these, only New Jersey appears to have recognized a right to what has been called "informational privacy." Id. at 1130, 1141-42, 1154; Doe, supra, 142 N.J. at 89-90. Informational privacy has been variously defined as "shorthand for the ability to control the acquisition or release of information about oneself," Lin, supra, at 1095 n.42 (quoting A. Michael Froomkin, The Death of Privacy?, 52 Stan. L. Rev. 1461, 1463 (2000)), or "an individual's claim to control the terms under which personal information . . . is acquired, disclosed, and used." Ibid. (quoting Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193, 1205 (1998)). In general, 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."

---

<sup>4</sup> New Jersey was one of the earliest states to grant recognition to a substantive right of privacy, not long after such a right was first espoused in the seminal article by Warren and Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890). See Vanderbilt v. Mitchell, 72 N.J. Eq. 910 (E. & A. 1907); see also McGovern v. Van Riper, 137 N.J. Eq. 24, 32-33 (Ch. 1945); Frey v. Dixon, 141 N.J. Eq. 481, 483 (Ch. 1948).

[Id. at 1096-97.]

We adopt this formulation.

In State v. Hunt, 91 N.J. 338 (1982), the Court found a reasonable expectation of privacy in long distance call records maintained by the phone company, rejecting federal and state decisions to the contrary that had followed the reasoning of Smith v. Maryland, supra. Id. at 344-48. The Court held that not only the content of phone calls, but also the numbers dialed in the privacy of the home, are entitled to protection from unfettered governmental intrusion. The Court was "persuaded that the equities so strongly favor protection of a person's privacy interest that we should apply our own standard rather than defer to the federal provision." Id. at 345-46. More recently, in State v. McAllister, 184 N.J. 17 (2005),<sup>5</sup> the Court held that under the search and seizure guarantee of our State Constitution, Art. I par. 7, a citizen has a "reasonable expectation of privacy in his or her bank records, even when those records are in the possession of the bank." Id. at 29. In reaching that conclusion, the Court again rejected federal law, specifically United States v. Miller, supra, and United States v. Payner, supra, as well as state cases following the federal lead. Id. at 24-32. Bank records, like long distance phone billing records, reveal much about the personal affairs of the account holder, entitling those records to protection from unfettered government intrusion. McAllister, supra, 184 N.J. at 30-33. Nevertheless, those records may be obtained by a valid grand jury subpoena duces tecum. Id. at 35-37. Indeed, even a

---

<sup>5</sup> Subsequent to Hunt, but before McAllister, the Court had extended state constitutional protection to the contents of garbage left for pickup by the waste-hauler, State v. Hemptele, 120 N.J. 182 (1990), rejecting federal law to the contrary. Id. at 191-212. See California v. Greenwood, 486 U.S. 35, 108 S. Ct. 1625, 100 L. Ed. 2d 30 (1988).

validly issued administrative subpoena might be used to obtain those same records. Id. at 36 n.1. While McAllister has significant bearing on the issue before us, the records obtained by the State in that case went far beyond the limited identification information sought from, and provided by, Comcast in this case.

The only case to touch on the question presented here is State v. Evers, 175 N.J. 355 (2003), a decision not cited by either party to this appeal. There, a California law enforcement officer investigating internet child pornography sent a California search warrant by mail to America Online, Inc. (AOL) headquarters in Virginia seeking "account information concerning screen name BTE324." AOL's response yielded the name, address, and telephone number of Elayne Evers, other screen names associated with her account, the method of accessing the Internet, and additional basic account information. Id. at 371.

The information provided by AOL revealed that the account holder lived in New Jersey and led to the indictment of the defendant, William Evers, in this State. Evers moved to suppress evidence seized in a search of his home in New Jersey based on an argument that the affidavit in support of the New Jersey warrant contained information obtained unlawfully by the California authorities. Id. at 365-69. At issue was whether Evers had a reasonable expectation of privacy in his internet account information under either federal or state law. Id. at 370. In regard to the State constitutional claim, the Court said:

No 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. See State v. Mollica, 114 N.J. 329, 347, 554 A.2d 1315 (1989) (holding "protections afforded by the constitution of a sovereign entity control the actions only of

the agents of that sovereign entity"). Article I, Paragraph 7 of our State Constitution protects the rights of people within New Jersey from unreasonable searches and seizures by state officials, and its jurisdictional power extends to agents of the state who act beyond the state's borders in procuring evidence for criminal prosecutions in our courts. Our State Constitution has no ability to influence the behavior of a California law enforcement officer who does not even know that New Jersey has an interest in a matter he is investigating. Therefore, we decline to hold that defendant had a right of privacy protected by Article I, Paragraph 7 in the subscriber information at AOL headquarters in Virginia.

[Id. at 371.]

While the language in the final sentence could be understood to mean that there is no right to privacy in the account information at issue here,<sup>6</sup> we read that language, as limited by the preceding sentence, to mean only that no such right of privacy would be recognized under the circumstances there presented, where the information was obtained by an officer from another jurisdiction without any involvement by New Jersey officials. As a result, the issue remains open as a matter of State constitutional law.

Id. at 371-74.

The judge, in granting defendant's motion to suppress, found support in State v. Domicz, 377 N.J. Super. 515 (App. Div. 2005), rev'd, 188 N.J. 285 (2006). One of the issues presented in that case was the obtaining of defendant's electrical use records by means of subpoena. The subpoena also sought records of "other similarly-sized homes for comparison purposes." Id. at 533. After a careful analysis of our case law establishing greater protection for New Jersey citizens under our State Constitution than accorded under the Fourth Amendment, id. at 534-38, we concluded "that there is a

---

<sup>6</sup> One commentator has read Evers in this expansive manner. Clancy, supra, 75 Miss. L.J. at 226 n.100.

legitimate expectation of privacy in electrical usage records maintained by a power company." Id. at 538. We were unpersuaded by contrary decisions in Alaska, Colorado and Idaho under their respective state constitutions. Id. at 539. We rejected the State's arguments that the fact that the records were maintained by a third-party precluded a legitimate expectation of privacy, id. at 540, referencing the Court's decisions in Hempele, supra, and Hunt, supra, as well as our opinion in McAllister, 366 N.J. Super. 251 (App. Div. 2004), which was subsequently affirmed by the Court, as discussed earlier. Id. at 540-42. We also concluded that electrical usage records, just like garbage (Hempele) and telephone records (Hunt) revealed intimate details of activities taking place within the home. Id. at 542-45. Finally, we rejected the State's reliance on State v. Jones, 179 N.J. 377 (2004) and State v. Sullivan, 169 N.J. 204 (2001), cases also relied on by the State in this appeal. While it is true that the Court in Sullivan, supra, 169 N.J. at 209, mentioned in passing that a police officer had corroborated an informant's tip by reviewing utility records that identified the owner of certain premises, the opinion did not, as we noted in Domicz, explain "by what authority the police officer was permitted to examine the utility records." 377 N.J. Super. at 545. Indeed, as the Court explained in Jones, supra, 179 N.J. at 391, the officer in Sullivan did no more than ascertain whether the telephone number listed to the apartment in a multi-unit building where controlled narcotic purchases were made matched the phone number provided by the informant. Concluding our analysis of Jones and Sullivan, we stated:

Moreover, there is a distinct difference between a warrantless review of utility records to ascertain the name of an occupant of property, on the one hand, and a review of records relating to the usage of power, on the other. See Commonwealth v. Duncan, 572 Pa. 438, 817 A.2d 455, 459 (Pa.2003); cf., Hiibel v. Sixth Judicial Dist. Ct., 542 U.S. 177,

124 S.Ct. 2451, 159 L. Ed. 2d 292 (2004). For present purposes, we need not determine whether a warrantless search of such records--for the sole purpose of identifying the owner of property--runs afoul of either the Fourth Amendment or Article I, paragraph 7. Here, the subpoena utilized by Detective Peacock compelled a greater disclosure of information than that which occurred in Sullivan.

[Domicz, supra, 377 N.J. Super. at 545-46.]

Our decision in Domicz was reversed on numerous grounds. State v. Domicz, 188 N.J. 285 (2006). Concerning the utility records, although the Court seemed to question our conclusion that there is a legitimate expectation of privacy in electrical usage records, id. at 298-300, it ultimately held that, even assuming such an expectation of privacy, the records were properly obtained by a grand jury subpoena, as was the case with the bank records in McAllister. Id. at 301. Thus, the Court's disposition ultimately provides no definitive answer to the question before us.<sup>7</sup>

Writing on a nearly clean slate, we conclude that defendant had a reasonable expectation of privacy in her ISP account information obtained by Detective Smith from Comcast by means of the invalid subpoena. We do so treading the State constitutional path illuminated by the Court in cases such as McAllister, Hunt and Hempele, decisions which are highly protective of an individual's right to privacy even when the information sought is, of necessity, in the hands of a third-party. As the Court said in Doe, supra, 142 N.J. at 89-90, "[w]e have found a constitutional right of privacy in many contexts, including the disclosure of confidential or personal information" (citations omitted).

---

<sup>7</sup> The information at issue here was not exposed to public view, rendering the extensive discussion of such material in Doe, supra, 142 N.J. at 79-87, largely irrelevant.

By her use of an anonymous ISP address, 68.32.145.220, or "screen name," defendant manifested an intention to keep her identity publicly anonymous. She could have used her own name or some other ISP address that would have readily revealed her identity, but she did not. Having chosen anonymity, we conclude that defendant manifested a reasonable expectation of privacy in her true identity, known only to Comcast. Defendant's interest in anonymity is both legitimate and substantial, see Doe, supra, 142 N.J. at 87, and the data on file with Comcast fell within the concept of informational privacy, which we have earlier endorsed.

Just as technological developments once made "the telephone an essential instrument in carrying on our personal affairs," Hunt, supra, 91 N.J. at 338, so have further developments made the personal computer an essential component of modern life, entitling individuals to at least the same degree of privacy with respect to its use as accorded to other forms of personal communication. See Clancy, supra. While not sacrosanct, that information concerning the identity of an internet user can only be obtained by law enforcement through some means of proper judicial process. This is not an onerous burden to place on law enforcement. Just as with telephones or bank records, computers cannot be used with impunity for unlawful purposes. When there is probable cause to believe unlawful use has occurred, law enforcement has the tools to respond.

In this case, we need not address whether defendant's reasonable expectation of privacy would be infringed if the officers, knowing of her identity, merely asked Comcast to verify that the named individual was in fact the user of that provider's services, i.e., that Shirley Reid maintained an account with them. That information might then have

been used to support the issuance of process to discover the ISP address utilized by defendant. As noted, we do not need to resolve that issue because the information sought here was not limited to a verification of defendant's status as an account holder. Rather, here, the police unlawfully obtained the identity of defendant as the user of an ISP address which did not of itself reveal her identity.

Because defendant had a right of privacy in the subscriber information obtained by the invalid subpoena, that evidence was properly suppressed by Judge Alvarez.

Affirmed.

I hereby certify that the foregoing  
is a true copy of the original on  
file in my office.

  
CLERK OF THE APPELLATE DIVISION