

New Jersey Constitution's Privacy Right Protects Subscriber Information Held by ISPs

Under the New Jersey Constitution, customers of Internet service providers have a reasonable expectation of privacy in their subscriber information, the New Jersey Supreme Court held April 21 (*New Jersey v. Reid*, N.J., No. A-105, 4/21/08).

ISPs, Not Government, to be Affected by Holding

The way government accesses Internet subscriber information is not expected to change in light of *New Jersey v. Reid*, but the court's holding that users had a reasonable right of privacy in their subscriber data may alter the way service providers store information and make it accessible, privacy lawyers speculated after the decision came down.

Mark Zwillinger, partner at Sonnenschein Nath & Rosenthal in Washington, D.C. and chair of the firm's Internet, Communications & Data Protection Group, told BNA April 23 that the decision will not tangibly change law enforcement's access to or collection of subscriber information.

"The main significance of this case is that it offers a suppression remedy in New Jersey," Zwillinger said. "Aside from that, the case should not change much, and it is not indicative of any real shift on the privacy landscape," he said.

The Fourth Amendment does not extend a reasonable expectation of privacy to the kinds of personal information protected here, but federal statute still requires a properly issued subpoena before an ISP is required to disclose the kind of information at stake in this case.

At 18 U.S.C. § 2703(c)(2), the Stored Communications Act, within the Electronic Communications Privacy Act of 1986, requires a "provider of electronic communication service" or "remote computing service," which includes ISPs, to provide a subscriber's complete information—including name, address, billing and payment status—to the government "when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1)." Paragraph (1) includes warrants and subscriber consent.

At subsection (d), the statute goes on to say that a court order will only be proper if only if the governmental entity offers "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

Albert Gidari Jr., a partner at Perkins Coie in Seattle, said that these federal provisions dulled the impact of the court's decision.

"New Jersey is among a handful of states that provide online users more protection than the federal Stored Communications Act," Gidari said. "The decision of course does not bind federal officers who will still be able to get the information on a lower standard— specific and articulable facts under 18 USC § 2703(d)."

But even if the decision does not change the information's accessibility, it may still be significant for consumers because it may affect the way ISPs like Comcast treat sensitive personal information before the police are ever involved, Lothar Determann, a partner at Baker & McKenzie in San Francisco and professor at University of San Francisco School of Law, suggested.

"Once the courts say that individuals have reasonable expectation of privacy in personal information stored with an ISP, the ISPs may change the way they handle sensitive data," Determann told BNA April 25.

"The decision has potential implications in a number of areas where governments and companies have been accessing live or stored communications based on the assumption that the data subjects do not have a reasonable expectation of privacy," Determann said, and listed employee monitoring, e-mail filtering technology, security checks, and Web access restrictions among activities that ISPs may need to reassess in light of the holding.

ISPs struggle to balance cooperation with law enforcement and protection of consumer interests as it is, Determann said, and the court's readjustment of consumer privacy rights may throw those scales off, even if just temporarily.

The court said New Jersey's state constitutional privacy right is more expansive than the Fourth Amendment, and will extend to identifying information known only to Internet service providers. In order to access this identifying information, law enforcement must obtain a grand jury subpoena, the court said.

The court analogized Internet subscriber information to both telephone billing records and bank account information in reaching its conclusion. The Internet, like phone calls and banking, is an "essential activity" that demands a reasonable expectation of privacy for participants, the court said.

State Constitution Offended by Municipal Subpoena.

Article 1, Paragraph 7 of the New Jersey Constitution provides that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrant shall issue except upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the papers and things to be seized."

The court said that the state of New Jersey violated this provision when it issued a subpoena duces tecum on an ISP, seeking the identity of an Internet user identified only by Internet protocol address.

That IP address had been logged as visiting a corporate distribution Web site at the time that site was received an account modification request. The distributor grew suspicious when the user logged into a major account, changed the shipping address to a nonexistent combination of numbers and streets, and reformulated the password. The distributor called the account holder to verify the changes, and disclosed the IP address.

The account holder took the IP address to the police, claiming that the changes to the account had been made by an unauthorized outside party.

Local law enforcement determined that Comcast owned the ISP, served a municipal subpoena seeking the user's identifying information. Comcast identified the user as the defendant, Shirley Reid, a disgruntled employee of the account holder.

Reid was arrested and charged with second-degree computer theft. She moved to suppress the evidence, arguing that its collection was an illegal search and seizure.

The New Jersey Supreme Court agreed, upholding the finding of the lower court.

'Informational Privacy' Right Recognized in New Jersey.

The search was illegal because New Jersey affords its citizens a reasonable expectation of privacy in the information that users provide to their ISPs, Chief Justice Stuart Rabner wrote, emphasizing that New Jersey's constitution provides more protection than does the United States Constitution.

Although "federal case law interpreting the Fourth Amendment has found no expectation of privacy in Internet subscriber information," the court said that "Article 1, Paragraph 7, of the New Jersey Constitution provides more protection than federal law affords."

The court affirmed the appellate court's determination that New Jersey vests in individuals a right of "informational privacy."

"Information privacy encompasses any information that is identifiable to an individual," the appellate panel said, concluding that "information on file with Comcast concerning the identity of Internet users fell within [that] protected privacy right."

Looking to New Jersey precedent, the supreme court agreed.

In *State v. Hunt*, 91 N.J. 338 (1982), the state supreme court held that citizens enjoyed a reasonable expectation of privacy in their telephone toll billing records. These records were "part of the privacy package," the *Hunt* court said, because a list of privately-dialed telephone numbers "could reveal the identities of the persons and places called, and thus reveal the most intimate details of a person's life."

The court similarly extended a reasonable expectation of privacy to bank account holders with respect to their

bank records in *State v. McAllister*, 184 N.J. 17 (2005). The *McAllister* court said that banking records reveal "a great deal" about the personal affairs of the owners, and held that although the owners voluntarily provide personal information to their banks, "they do so with the understanding that it will remain confidential."

This logic carried through, in the court's view, to an Internet context.

"ISP records share much in common with long distance billing information and bank records," the court said, as "[a]ll are integrally connected to essential activities of today's society."

Internet users, like telephone and bank users, reveal personal information for limited purposes, the court said, and that disclosure did not upend the privacy right at stake.

"Users make disclosures to ISPs for the limited goal of using that technology and not to promote the release of personal information to others," the court said. "Under our precedents, users are entitled to expect confidentiality under these circumstances."

Additional Support in State Wiretap Act.

The court said that the New Jersey Wiretapping and Electronic Surveillance Act, N.J.S.A. 2A:156A-1 to -34, lent further support to its conclusion.

The Wiretap Act provides for disclosure of subscriber information, including name, address, telephone number, and means of payment—exactly the information Comcast provided about Reid—*only* when a law enforcement agency obtains "a grand jury 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," the court said.

No Heightened Showing, Notice Requirements.

The court said that a showing of relevance was all that was required for the grand jury to issue a subpoena. Probable cause was too high a hurdle, the court said, relying again on the reasoning of *McAllister*.

The *McAllister* court said that a relevancy standard was all that was needed satisfy the constitution. "The 'probable cause' required for a search warrant is foreign to the grand jury scene," that court said, and this court agreed.

"[W]e see no material difference between bank records and ISP subscriber information and decline to treat them differently," the court said. "In both cases, a grand jury subpoena based on a relevancy standard is sufficient to meet constitutional concerns."

The court also rejected the arguments of amici, including the New Jersey chapter of the American Civil Liberties Union, that notice should be given to users before issuance of a subpoena.

Notice could thwart investigations because ISP information is not backed up the way bank and telephone provider information is. "[U]nscrupulous individuals aware of a subpoena could delete or damage files on their home computer and thereby effectively shield them from a legitimate investigation," the court said.

Records Can be Reproduced.

Although the court suppressed the evidence, it was clear that, with a proper subpoena, it could be reproduced, and the case could again proceed against Reid.

Unlike an improperly coerced confession, Comcast's records existed independently on the faulty process the police followed, the court said. "As a result, the records can be reliably reproduced and lawfully reacquired through a proper grand jury subpoena."

Steven A. Yomtov, New Jersey deputy attorney general, represented the State of New Jersey. Joseph C. Grassi and Frank L. Corrado of Barry, Corrado, Grassi & Gibson, Cape May, N.J., represented Shirley Reid.

Full text at http://pub.bna.com/eclr/a105_042108.pdf