THE SUPREME COURT OF NEW HAMPSHIRE

Cheshire
No. 2010-455

THE STATE OF NEW HAMPSHIRE

v.

JAMES W. MELLO

Argued: April 13, 2011
Opinion Issued: May 26, 2011

Michael A. Delaney, attorney general (Thomas E. Bocian, assistant attorney general, on the brief and orally), for the State.

Wilson, Bush, Durkin & Keefe, P.C., of Nashua (Charles J. Keefe on the brief and orally), for the defendant.

DUGGAN, J. The defendant, James W. Mello, appeals his conviction following a bench trial on four counts of delivery of child pornography. See RSA 649-A:3, I(a), II(a) (2007) (amended 2008). He argues that the Superior Court (Arnold, J.) erred in denying his motion to suppress evidence derived from a search warrant issued by the Keene District Court, which authorized a search for information held by an out-of-state corporation. We affirm.

The record supports the following facts. As an aid to the investigation of crimes related to the sexual exploitation of children, Detective James

McLaughlin of the Keene Police Department placed a profile on an Internet social networking site. The profile indicated that he was a fourteen-year-old boy and included a photograph of a boy who was approximately that age. In October 2008, the defendant added McLaughlin's fictitious profile to his friend list on the social networking site. The defendant's profile on the site included several photographs of nude male children, some of which were pornographic in nature. McLaughlin and the defendant subsequently engaged in several e-mail and real-time chat exchanges between October 12 and October 15. Many of these exchanges were sexually explicit in nature and the defendant sent numerous pornographic images depicting male children to McLaughlin by e-mail and real-time chat.

Using the defendant's e-mail address, "wildbill0911," McLaughlin determined the defendant's corresponding Internet Protocol (IP) address. McLaughlin's check of the IP address also identified the subscriber's location as Nashua and his Internet service provider as Comcast, a New Jersey based corporation. On October 20, 2008, McLaughlin obtained a search warrant authorizing a search for subscriber information associated with the defendant's IP address. The warrant stated that Comcast was in possession of that information. The Keene District Court issued the warrant and McLaughlin faxed it to Comcast. Comcast responded by faxed letter and provided the subscriber's name, address, telephone number, type of service, account number, account status, IP assignment, e-mail user IDs, and method of payment.

Based upon this information, McLaughlin applied for and received an additional warrant to search the defendant's home for certain computer-related equipment. McLaughlin and the Nashua Police Department executed the warrant and seized evidence that led to the indictment of the defendant on four counts of delivery of child pornography.

The defendant subsequently filed a motion to suppress all evidence obtained as a result of the initial search warrant. He contended that the district court exceeded the scope of its jurisdiction by issuing a warrant for evidence held by an out-of-state corporation. The trial court denied the motion because the defendant did not have a reasonable expectation of privacy in the information obtained from Comcast.

On appeal, the defendant argues that the warrant to obtain his subscriber information was issued in violation of his rights under the Fourth Amendment to the Federal Constitution and Part I, Article 19 of the State Constitution. We first address the defendant's claim under our State Constitution and cite federal cases for guidance only. State v. Ball, 124 N.H. 226, 231-33 (1983). We review the superior court's order on a motion to suppress de novo, except as to any controlling facts determined by the superior court in the first instance. State v. Goss, 150 N.H. 46, 47 (2003).

The defendant contends that the district court did not have the authority to issue a search warrant to a corporation outside of New Hampshire. At oral argument, the State conceded that the search warrant was defective. We agree that the district court did not have jurisdiction to issue a warrant to an out-of-state corporation. Accordingly, we take this opportunity to outline some of the proper procedures for obtaining records and evidence located outside of New Hampshire.

For example, the legislature has provided two mechanisms for obtaining such evidence, neither of which was followed in this case. See RSA 7:6-b (2003); RSA ch. 613 (2001). The first method pertains only to records held by a "communications common carrier," see RSA 7:6-b, defined as "a person engaged in providing communications services to the general public through transmission of any form of information between subscribers by means of wire, cable, radio or electromagnetic transmission, optical or fiber-optic transmission, or other means which transfers information without physical transfer of medium." RSA 570-A:1, IX (2001). Upon written demand of the attorney general, or his designee, that he "has reasonable grounds for belief that the service furnished to a person or to a location by such communications common carrier has been, is being, or may be used for an unlawful purpose," the carrier must provide certain identifying information, including the name and address of the subscriber. RSA 7:6-b, I, III.

Alternatively, RSA chapter 613 provides a uniform method, which has been adopted by all fifty states and the District of Columbia, for requesting the appearance of an out-of-state witness in New Hampshire. This uniform statute provides that a New Hampshire court may summons a material out-of-state witness in any grand jury investigation or criminal prosecution that has commenced or is about to commence by issuing a certificate under the seal of the court requesting the presence of that witness. RSA 613:3, I. That certificate must then be presented to a court in the county in which the witness is found. Id. Thus, in this case, the State could have requested a New Hampshire court to summons Comcast's keeper of records to New Hampshire. We also note that these two examples do not foreclose the possibility that there may be other permissible means for obtaining evidence from an out-of-state corporation.

Nonetheless, the defective warrant infringed upon the defendant's constitutional rights only if the effort to obtain evidence constituted a search in the constitutional sense. See State v. Valenzuela, 130 N.H. 175, 181-82 (1987). The defendant asserts that a search took place because he had a subjective expectation of privacy in the subscriber information that society is prepared to recognize as reasonable. The State argues that the defendant did not have a reasonable expectation of privacy because he voluntarily conveyed the information to Comcast.

"Our State Constitution protects all people, their papers, their possessions and their homes from unreasonable searches and seizures." Goss, 150 N.H. at 48 (quotation omitted). We have recognized that an expectation of privacy plays a role in the protection afforded under Part I, Article 19. State v. Robinson, 158 N.H. 792, 796 (2009). In Goss, we adopted a two-part analysis for determining whether there is a reasonable expectation of privacy: "first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable." Goss, 150 N.H. at 49 (quotations omitted).

The State does not dispute that the defendant had a subjective expectation of privacy in his subscriber information. Accordingly, we need only decide whether the defendant's subjective expectation of privacy was one that society would be prepared to recognize as reasonable.

We have previously held that a defendant has no reasonable expectation of privacy in business records containing information voluntarily provided to a public utility. State v. Gubitosi, 152 N.H. 673, 677-79 (2005); Valenzuela, 130 N.H. at 183; see also Smith v. Maryland, 442 U.S. 735, 743-45 (1979). In Valenzuela, we relied upon a series of United States Supreme Court "agent-informer" cases and determined that the government's use of a pen register to record outgoing telephone numbers dialed by the defendant was not a search within the meaning of Article 19. Valenzuela, 130 N.H. at 188-89. These "agent-informer" cases have consistently held that information revealed by a defendant to a government informant or agent is admissible even if the informant or agent conceals his true identity. Hoffa v. United States, 385 U.S. 293, 302 (1966); Lewis v. United States, 385 U.S. 206, 210-11 (1966); United States v. White, 401 U.S. 745, 752 (1971). We explained in Valenzuela that in making a record of a decoded signal sent from the defendant's phone to the telephone company, "the registers did no more than record voluntary communications from the defendant to the telephone company." Valenzuela, 130 N.H. at 183. We also specifically distinguished these communications to the company from the contents of communications transmitted over the company's lines, addressed to recipients of completed calls. Id.

We confronted a similar issue more recently in Gubitosi, where we specifically declined the defendant's invitation to overrule Valenzuela. Gubitosi, 152 N.H. at 678. There, we determined that just as a defendant has no protected privacy interest in a record of his outgoing phone calls, there is no reasonable expectation of privacy in a record of a defendant's cell phone calls "recorded for billing purposes and retained by [the telephone company] in the ordinary course of its business." Id. at 677-78.

Likewise, we see no meaningful distinction between obtaining telephone numbers recorded in the ordinary course of business by a telephone company and the procurement of a customer's basic subscriber information from an

Internet service provider. As in Valenzuela and Gubitosi, the defendant voluntarily provided the information to Comcast, which recorded it in the ordinary course of business for billing purposes and used it to provide the defendant with Internet service. Having voluntarily provided this information in order to use Comcast's service, the defendant cannot now claim a privacy interest in it. See Valenzuela, 130 N.H. at 188 (explaining that once a defendant voluntarily discloses information to another he cannot claim a degree of privacy protection against the government because it would result in "a kind of evidentiary copyright"). Accordingly, we join the overwhelming majority of federal and state courts that have addressed this issue and conclude that a defendant has no reasonable expectation of privacy in subscriber information voluntarily provided to an Internet service provider. See, e.g., United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008), cert. denied, 131 S. Ct. 440 (2010); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001); United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007); State v. Delp, 178 P.3d 259, 264-65 (Or. Ct. App. 2008); Hause v. Com., 83 S.W.3d 1, 12 (Ky. Ct. App. 2002).

Our conclusion is bolstered by Comcast's customer privacy policy, which specifically reserves the right to disclose subscriber information to "comply with law." The defendant contends that this exception to the privacy policy is inapplicable because Comcast responded to a defective warrant. We are unpersuaded by this distinction because Comcast undoubtedly believed that it was disclosing the defendant's information in order to "comply with law."

Nonetheless, the defendant asks us to recognize a privacy interest in his subscriber information based upon our decision in Goss that an individual has a reasonable expectation of privacy in sealed garbage bags left in front of a residence for collection. Goss, 150 N.H. at 49-50. He contends that Goss stands for the proposition "that by exposing information to a third party, when one does not expect it to be revealed to anyone else in the ordinary course, that one does not lose an expectation of privacy in that information."

The defendant reads Goss too broadly. While the defendant correctly points out that we construed our State Constitution to provide greater protection than the Federal Constitution, we explicitly relied upon the fact that people do not voluntarily expose the contents of their sealed trash bags to the public when they leave those bags out for regular collection. Goss, 150 N.H. at 49. Additionally, in Gubitosi, we rejected the defendant's similar reliance upon Goss to contend that he had a reasonable expectation of privacy in his telephone billing records because they "only contain information that he voluntarily conveyed to [the phone company] in order to make use of its telephone service." Gubitosi, 152 N.H. at 679. Likewise, as we have already determined, the defendant here voluntarily provided his subscriber information to Comcast, and in doing so, lost any reasonable expectation of privacy in that information. Accordingly, Goss is distinguishable from the facts of this case.

The defendant also points us to the New Jersey Supreme Court's decision in State v. Reid, 945 A.2d 26 (N.J. 2008), which, contrary to the majority of jurisdictions, recognized a reasonable expectation of privacy in Internet subscriber information. Reid, 945 A.2d at 33-34. The court in Reid began its analysis by recognizing that federal courts, relying upon "settled federal law that a person has no reasonable expectation of privacy in information exposed to third parties, like a telephone company or bank," have found no expectation of privacy in Internet subscriber information. Id. at 31. Nonetheless, the court reached a different conclusion based upon its own case law, which recognizes a reasonable expectation of privacy in telephone billing and bank records. Id. at 32.

Despite our previous reliance upon "settled federal law" recognizing no reasonable expectation of privacy in information voluntarily exposed to third parties, the defendant urges us to adopt the reasoning of Reid. He contends that our State Constitution, like New Jersey's State Constitution, provides greater privacy protection than the Federal Constitution. While Part I, Article 19 does offer greater protection than the Fourth Amendment in some circumstances, see Goss, 150 N.H. at 49; State v. Sterndale, 139 N.H. 445, 449 (1995) (refusing to adopt an automobile exception to the warrant requirement), our law regarding information voluntarily exposed to third parties is in line with the protection afforded under the Fourth Amendment and diverges significantly from New Jersey law, see Valenzuela, 130 N.H. at 182-84 (relying upon the "well-settled" and "inescapable" United States Supreme Court precedent that individuals have no reasonable expectation of privacy in information voluntarily exposed to third parties); Gubitosi, 152 N.H. at 677 (noting that we relied upon Smith v. Maryland, 442 U.S. 735 (1979), in Valenzuela to determine that an individual has no legitimate expectation of privacy in phone numbers dialed to make outgoing calls). Accordingly, we do not find Reid persuasive and decline to follow it.

We recognize how intertwined and essential computers and the Internet have become to everyday, modern life. See Reid, 945 A.2d at 33. Citizens routinely access the Internet for a wide range of daily activities, such as gathering information, communicating, shopping, banking, and more. We are also cognizant that many users conduct some of their most private affairs over the Internet because of the anonymity that it offers. Nonetheless, as we similarly recognized in Valenzuela more than twenty years ago, while individuals may have a reasonable expectation of privacy in the contents of their communications, i.e., the content of e-mails and the specific content viewed over the Internet, they have no such privacy interest in information voluntarily disclosed to an Internet service provider in order to gain access to the Internet. See Valenzuela, 130 N.H. at 183; cf. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("When the government obtains the to/from addresses of a person's e-mails or the IP addresses of websites visited, it does

not find out the contents of the messages or know the particular pages on the websites the person viewed. At best, the government may make educated guesses . . . ."); United States v. Hernandez, 313 F.3d 1206, 1209-10 (9th Cir. 2002) ("Although a person has a legitimate interest that a mailed package will not be opened and searched en route, there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior." (citations omitted)).

Because the Federal Constitution is no more protective of the defendant than the State Constitution under these circumstances, Goss, 150 N.H. at 49, we reach the same conclusion under the Federal Constitution.

Affirmed.

DALIANIS, C.J., and HICKS, CONBOY and LYNN, JJ., concurred.