State v. Simmons (2010-066)

2011 VT 69

[Filed 23-Jun-2011]

2011 VT 69

No. 2010-066

State of Vermont	Supreme Court
v.	On Appeal from District Court of Vermont, Unit No. 1, Windham Circuit
Graham Simmons	November Term, 2010

Katherine A. Hayes, J. (motion to suppress); Karen R. Carroll, J. (final judgment)

David W. Gartenstein, Windham County Deputy State's Attorney, and Eric W. Gentino, Law Clerk (On the Brief), Brattleboro, for Plaintiff-Appellee.

Allison N. Fulcher of Martin & Associates, Barre, for Defendant-Appellant.

PRESENT: Reiber, C.J., Dooley, Johnson, Skoglund and Burgess, JJ.

¶ 1. **BURGESS, J.** Defendant Graham Simmons appeals from the Windham District Court's denial of his motion to suppress evidence of a purloined computer and other stolen items discovered in the execution of a search warrant at his residence. Probable cause supporting the warrant was obtained through inquest subpoenas requiring production of internet addresses and indentifying data from internet service providers. Defendant challenges the subpoena of internet records as a warrantless search in violation of Chapter I, Article 11 of the Vermont Constitution, and also complains that the warrant was invalidly based on information from an unknown tipster whose reliability was not reasonably established. We note that defendant failed to properly preserve the first point and hold that the trial court's refusal to suppress was not plain error. We also determine that the informant's input and credibility was ultimately irrelevant to issuing the warrant. Accordingly, the judgment is affirmed.

¶ 2. In 2008, two of defendant's neighbors on Hi Lo Biddy Road in Putney reported break-ins and stolen property, including two laptop computers. A State Police detective received a tip from an anonymous informant that a man named "Graham," who lived on the same street as the victims, had one of the computers and was using it to access his neighbor's wireless internet network. The detective looked through public records and learned that one Graham Simmons with previous larceny and fraud convictions lived on Hi Lo Biddy Road. The detective also learned from defendant's next door neighbor—one of the break-in victims—that she subscribed to Verizon internet services and had a wireless network in her home for her personal use.

¶ 3. The detective looked for defendant on the social networking website MySpace.com and located a MySpace profile for a "Graham Simmons" living in Putney, accompanied by a picture resembling the photograph of defendant on record with the Department of Motor Vehicles. The detective then served an inquest subpoena[1] on MySpace to obtain defendant's internet protocol (IP) address—a code identifying the computer network from which defendant accessed his MySpace account. The records from MySpace indicated that shortly after defendant's neighbor's computer was stolen, defendant logged onto his MySpace account more than 100 times over the course of a week. Each log on originated from the same IP address, identified as a Verizon internet service address.

¶ 4. The detective secured another inquest subpoena, this time for Verizon's records concerning the same IP address. Verizon disclosed records indicating that the only person authorized to use the internet connection identified by that IP address was defendant's neighbor,

mentioned above. Though the neighbor had not given defendant permission to use her Verizon wireless connection, defendant had clearly done so.

¶ 5. Based on this evidence of unauthorized network access in apparent violation of 13 V.S.A. § 4102 (criminalizing knowing and intentional unauthorized access to computer networks and systems), the detective applied for and was issued a warrant to search for computers at defendant's Hi Lo Biddy Road address. The resulting search turned up a laptop computer with a serial number matching the laptop stolen from the neighbor's residence. The police also noted that several other objects in plain view resembled other items reported as stolen from defendant's neighbors. Based on these observations, the police secured defendant's residence while the detective obtained another search warrant to seize the other suspected stolen property. During the second search, the police found a small bag of marijuana. After his arrest, defendant admitted that he burglarized two of his neighbors' residences and accessed the internet using his neighbor's wireless signal without permission. Defendant was charged with four counts of burglary under 13 V.S.A. § 1201(a), possession of marijuana under 18 V.S.A. § 4230(a)(1), and unauthorized access to a network under 13 V.S.A. § 4102.

¶ 6. Defendant moved to suppress the evidence. Contending that the IP address was private information, defendant argued that issuing subpoenas to MySpace and Verizon without probable cause was an invalid search in violation of the Fourth Amendment of the Federal Constitution and of Chapter 1, Article 11 of the Vermont Constitution. Defendant claimed the subpoenas allowed essentially a warrantless search of his home in violation of his reasonable expectation of privacy, which he analogized to a warrantless search of his unopened mail. As we understand his point below, defendant maintained that probable cause for the warrants to physically search his house was derived from information obtained unconstitutionally from MySpace and Verizon. Thus the evidence gathered from those searches must be excluded as fruit of the poisonous tree under Wong Sun v. United States, 371 U.S. 471 (1963).

¶ 7. The trial court denied the motion, concluding that defendant enjoyed no reasonable expectation of privacy in the subpoenaed information. The court found that the

MySpace privacy policy, posted online, plainly declared that its account information could be disclosed as it deemed necessary "to respond to a subpoena . . . whether or not a response is required by applicable law." The court also noted that the MySpace records were limited to the IP address and time-of-use data.

¶ 8. Applying settled Fourth Amendment precedent, the court agreed with the ruling in United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007)[2] that "internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access." Regarding the Verizon records that identified the IP address as belonging to defendant's neighbor, the court observed that defendant had no privacy interest in his neighbor's internet account.

¶ 9. Defendant's remaining argument on appeal is that suppression should have been granted because the State's subpoena to MySpace violated the state constitutional guarantees against warrantless searches in Article 11.[3] This argument is unavailing. First, defendant failed to properly preserve his state constitutional claim below. Second, the trial court did not commit plain error in denying the motion—it properly concluded that Vermont's Constitution affords no privacy protection in an internet service provider's subscriber address or use information disclosing noncontent data.[4] Concerning the claimed inadequacy of the informant's reliability, probable cause for the warrants did not depend on the tip. Accordingly, we affirm.

¶ 10. This court has consistently held that "it is the duty of the advocate to raise State constitutional issues, where appropriate, at the trial level." State v. Jewett, 146 Vt. 221, 229, 500 A.2d 233, 238 (1985). We considered a similar preservation question in State v. Maguire, where the defendant merely cited Article 11 in the introductory paragraph of a memorandum in support of his motion to suppress, but presented no analysis or application of that provision. 146 Vt. 49, 54, 498 A.2d 1028, 1031 (1985). Though the parties in Maguire stipulated that defendant's motions below raised a constitutional question, we still declined to address the issue on appeal because defendant offered "no analysis of the Vermont Constitution in comparison with the Federal Constitution and no showing of extraordinary circumstances that would justify our addressing this issue for the first time on appeal." Id.

¶ 11. Aside from a bald assertion that the evidence should be suppressed "pursuant to . . . the Vermont Constitution, Chapter 1, Article 11," defendant proffered no particular argument or analysis to the trial court as to why this should be so. Defendant correctly points out in his brief to this Court that Article 11 has been found to surpass protections afforded under the Fourth Amendment to the United States Constitution; however, he advanced no reason for expanded protection at the trial court. Nor does defendant demonstrate any extraordinary circumstances to prompt divergence from the customary consequence of nonpreservation of matters not raised below. See State v. Hunt, 150 Vt. 483, 494-95, 555 A.2d 369, 376-77 (1988) (holding that defendant's Article 11 claims, while fully briefed on appeal, were not preserved when not argued below, and no extraordinary circumstances justified appellate review of issues not first addressed to the trial court). Thus, defendant waived his Article 11 argument.

¶ 12. Despite defendant's failure to preserve his constitutional claim, we examine the claim for "plain error" in the court's ruling. See State v. Yoh, 2006 VT 49A, ¶ 36, 180 Vt. 317, 910

A.2d 853 (noting that when issue has been forfeited by failure to raise it below, Court may only consider it under plain error). Plain error lies "only in those rare and extraordinary cases where the error is both obvious and strikes at the very heart of the defendant's constitutional rights or results in a miscarriage of justice if we do not recognize it." State v. Campbell, 146 Vt. 25, 27, 497 A.2d 375, 377 (1985). There was no such obvious and fundamental error here.

¶ 13. As conceded by defendant, Federal courts consistently refuse to extend Fourth Amendment protection to noncontent internet identification and account data. See United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (noting that "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation"); cf. Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (holding, in the context of telephonic technology, that defendant had no expectation of privacy in pen register listing phone numbers dialed from his phone).

¶ 14. Nothing in our Article 11 rulings suggest that an internet subscriber address and frequency of use data, unembellished by any personal information, should be treated as private. Article 11 declares that "the people have a right to hold themselves, their houses, papers, and possessions, free from search and seizure." Vt. Const. ch. 1, art. 11. Absent exigent circumstances not at issue here, Article 11 prohibits a warrantless search of "only those areas or activities that a reasonable person would conclude are intended to be private." State v. Geraw, 173 Vt. 350, 352, 795 A.2d 1219, 1221 (2002).

¶ 15. "Under Article 11, the question of whether an individual has a legitimate expectation of privacy hinges on the essence of underlying constitutional values—including respect for both private, subjective expectations and public norms." State v. Bryant, 2008 VT 39, ¶ 11, 183 Vt. 355, 950 A.2d 467 (quotation omitted). "[I]n order to invoke Article 11 protection, a person must 'exhibit[] an actual (subjective) expectation of privacy . . . that society is prepared to recognize as reasonable.' " Id. (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). Given the necessary and willing exposure of an internet user's

access point identification and frequency of use to third party internet service providers, such information cannot reasonably be considered confidential, especially when a provider such as MySpace openly declares a policy of disclosure. The information appears no more private than a phone number and the number of calls made, or a street address or post office box and volume of mail, neither of which could plausibly be considered private.

¶ 16. Though Article 11 can afford greater protection against warrantless searches than is sometimes accorded by the Fourth Amendment, defendant presents no compelling reason to depart from federal case law as applied by the trial court in this instance. No "intimate details" of defendant's personal "activities, behavior, habits, and lifestyles" were shown to be at stake as in State v. Morris, where Article 11 protection was extended to closed trash bags that would have been subject to warrantless search under the Fourth Amendment. 165 Vt. 111, 116, 680 A.2d 90, 94 (1996). Nor are other circumstances put forth meriting distinction from federal law on this topic. Cf., e.g., State v. Neil, 2008 VT 79, ¶¶ 12, 15, 184 Vt. 243, 958 A.2d 1173 (limiting warrantless search otherwise permitted under Fourth Amendment, of closed container seized incident to arrest, where there are no exigent circumstances beyond the immediate fact of arrest); State v. Savva, 159 Vt. 75, 91, 616 A.2d 774, 783 (1991) (rejecting the per se "automobile exception" to the Fourth Amendment, and requiring a warrant under Article 11 to search a closed container within a vehicle stopped by police if time and circumstances reasonably allow for warrant to be obtained); State v. Kirchoff, 156 Vt. 1, 14, 587 A.2d 988, 996 (1991) (holding open fields, subject to warrantless search under Federal precedent, protected under Article 11 if posted against trespass). Defendant's analogies to a warrantless search of his home or mail are also unavailing. Such intrusions are incomparable to requesting and receiving, from a third party service provider, an IP address and the number of times the access was used.[5]

¶ 17. Lastly, we need not tarry long on the issue of the anonymous informant. Defendant's claim that the state needed to substantiate the tipster's reliability for purposes of probable cause is unfounded. It is evident that the tip only initiated the detective's inquiry into defendant's identity from public records and his published MySpace profile, which led, in turn, to the MySpace inquest subpoena seeking an IP address. None of these investigative steps required warrants or probable cause. See, e.g., 13 V.S.A. § 5131. As found by the trial court, the warrant application was supported by probable cause supplied from the records obtained from MySpace and Verizon, the neighbor's evidence and the detective's background information on illicit wireless access. Given the rest of this evidence and information, the informant's reliability and the provenance of his tip was irrelevant to probable cause for the warrant. Affirmed.

FOR THE COURT:

Associate Justice

[1] 13 V.S.A. § 5131 provides that "[u]pon the written application of the state's attorney, a judge of the superior court may institute and conduct an inquest upon any criminal matter under investigation by the state's attorney." In furtherance of the inquest, the "judge may issue necessary process to bring witnesses before [the court] to give evidence in any matter there under investigation." 13 V.S.A. § 5132.

[2] After the trial court's ruling, this decision was vacated by United States v. D'Andrea, ___ F.3d ___ (1st Cir. 2011).

[3] Defendant argues no Fourth Amendment violation now, and does not challenge the legality, under the state or Federal Constitution, of the subpoenaed production of Verizon records disclosing the ownership of the IP address as an independent violation of his privacy, except as a "tainted fruit" of the Myspace search. State v. Pitts, 2009 VT 51, ¶ 21, 186 Vt. 71, 978 A.2d 14 (quotation omitted). Further, defendant concedes here that Federal courts, so far, decline to recognize a protected Fourth Amendment privacy interest in the service provider information at issue in this case.

[4] "Noncontent data" in this context is defined as data that does not include information concerning the substance of internet communications. Cf. 18 U.S.C. § 2510(8) (Under Federal law criminalizing unauthorized interceptions of communication, " '[c]ontents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication.").

[5] The Oregon Supreme Court reached a similar conclusion under similar circumstances, ruling that where a third party lawfully possesses, ruling that, where a third party lawfully possesses "noncontent information . . . regarding [an individual's] Internet usage," the state's constitution did not protect such information against warrantless police examination. State v. Delp, 178 P.3d 259, 264-65 (Or. App. 2008).

Conversely, the New Jersey Supreme Court has ruled that a subscriber's name associated with an IP address is confidential, but for reasons undeveloped, or simply inapplicable, here. See State v. Reid, 945 A.2d 26 (N.J. 2008). The Reid decision was based, in part, on prior recognition of state constitutional privacy rights in matters disclosed to third parties, such as banks and telephone exchanges, whereas no such history precedes the instant case. Id. at 32-33. Moreover, despite the privacy retained in internet user identification, the Reid court opined that such information was still obtainable by police through properly issued subpoenas, rather than warrants based on probable cause. Id. at 36. Concerned with issues not raised here, Reid is ultimately irrelevant to our inquiry.