In the Supreme Court of Georgia

Decided: November 5, 2012

S12A1190. REGISTE v. THE STATE.

MELTON, Justice.

Following the denial of his motion to suppress, Michael Jason Registe filed an application for an interlocutory appeal, which this Court granted. We asked the parties to specifically address "[w]hether the trial court erred by denying Registe's motion to suppress evidence regarding cellular phone?" For the reasons set forth below, we affirm.

In relevant part, the record shows that Registe has been indicted for the July 20, 2007 murder of two men who were shot in the head some time after borrowing a car from Lawrence Kidd. The next morning, Kidd told police that the victims were going to meet someone named "Mike," and Kidd provided Mike's cell phone number. Using this cell number, Detective R. Jackson faxed Cricket Communications, the cell service provider, the following message on July 21, 2007:

The Columbus Police Dept. is currently investigating a double

> homicide which occurred at approximately 2130 hours on 07-20-07. We have information that the victim last met with the owner of this phone (706-617-3602) which makes him a suspect at this time. Obviously this suspect presents an immediate danger to any law enforcement officer who may come into contact with this person. We are requesting information as to the owner of this phone as well as any calls to and from this number within a two hour period starting at 8:30 pm to 13:30 pm on 07-20-07 EST. Thank you for your cooperation.

Cricket Communications responded on July 22, 2007 with the requested information. Cricket reported that the account belonged to "Kareem Penn," an alias of Registe.

After cold calling numbers in the phone records provided by Cricket, the police spoke with Michael Brown, who stated he had picked up Registe at a time shortly after the shootings. Brown named others who had information. Combined, these individuals stated they had seen blood on Registe's clothing, and they named the hotel where Registe spent time. Through persons at the hotel and photo identification by Brown and his acquaintances, "Mike" was identified as Registe, and, on July 22, 2007, an arrest warrant was issued. On July 24, 2007, the Columbus Police executed a search warrant at an apartment linked to Registe where they found a gun and the cell phone assigned to the phone number at issue in this case. Later, on September 19, 2007, Columbus Police

acquired a court order for the production of documentary evidence from Cricket Communications, specifically the cell phone records of Kareem Penn from July 10, 2007 to July 25, 2007. Thereafter, Registe filed a motion to suppress the phone records on January 7, 2011, which the trial court denied.

On appellate review of a ruling on a motion to suppress, "the trial court's findings on disputed facts will be upheld unless clearly erroneous, and its application of the law to undisputed facts is subject to de novo review. [Cit.]" Barrett v. State, 289 Ga. 197, 200 (1) (709 SE2d 816) (2011).

As an initial matter, telephone billing records are business records owned by the telephone company, not the defendant. As a result, defendants generally lack standing to challenge the release of such records under the Fourth Amendment because they do not have a reasonable expectation of privacy in records belonging to someone else. Kesler v. State, 249 Ga. 462, 469 (5) (291 SE2d 497) (1982). Accordingly, Registe is not entitled to challenge the release of phone records in this case on Fourth Amendment grounds.

Registe does argue that the release of the cell phone records in this case failed to comply with relevant state and federal statutory provisions. OCGA § 16-11-66.1 states that:

> (a) A law enforcement officer, a prosecuting attorney, or the Attorney General may require the disclosure of stored wire or electronic communications, as well as transactional records pertaining thereto, to the extent and under the procedures and conditions provided for by the laws of the United States. (b) A provider of electronic communication service or remote computing service shall provide the contents of, and transactional records pertaining to, wire and electronic communications in its possession or reasonably accessible thereto when a requesting law enforcement officer, a prosecuting attorney, or the Attorney General complies with the provisions for access thereto set forth by the laws of the United States.

In turn, the "laws of the United States" referenced in the statute include the provisions of 18 U.S.C. § 2701 *et seq*, which address mandatory or voluntary disclosure of electronic communications records to the government. 18 U.S.C. § 2702 (c) (4) allows the voluntary release of non-content records, including subscriber information, "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." Registe maintains that, in this case, there were no emergency conditions supporting a release of the telephone records.

It must first be pointed out that the remedy sought by Registe, namely suppression of evidence, is not an available remedy under either OCGA § 16-

11-66.1[1] or 18 U.S.C. § 2702 (c) (4).[2] However, OCGA § 16-11-67 provides: "No evidence obtained in a manner which violates any of the provisions of this part [regarding wiretapping, eavesdropping, surveillance, and related offenses] shall be admissible in any court of this state except to prove violations of this part." Registe contends that, under this provision, the telephone records should have been considered inadmissible.

We disagree because the *voluntary* disclosure of telephone records in this case satisfied the applicable statutes.[3] Under the facts set forth in the trial court's order, we conclude that Cricket believed in good faith that disclosure of Registe's cell phone records was appropriate. Here, Cricket received information directly from police that its records could help identify an at-large suspect of a double homicide committed within a day of the request and that the suspect presented a present and immediate danger. This supported Cricket's

---

[1] OCGA § 16-11-66.1 (e) provides: "Violation of this Code section shall be punishable as contempt."

[2] 18 U.S.C. § 2707 allows a subscriber to file a civil action against any party who improperly releases covered records or information.

[3] For this reason, it is questionable whether OCGA § 16-11-66.1 or OCGA § 16-11-67 are applicable at all to this case, as the former statute appears to apply only to *mandatory* disclosures.

good faith belief that there was an ongoing emergency, and that belief supported Cricket's voluntary disclosure of its records.[4]

Therefore, the voluntary release of Registe's cell phone records by Cricket to the police complied with the state and federal statutory provisions cited above and precluded suppression of the evidence.[5] Registe's motion to suppress was properly denied.[6]

Judgment affirmed. All the Justices concur, except Hunstein, C.J., and Blackwell, J., who concur specially.

---

[4] We emphasize that the release of information in this case was *voluntary* and thereby governed by 18 U.S.C. § 2702 (c) (4). Cricket was not compelled to release its records, but it did so in good faith. Had police *mandated* the release of records and Cricket did not want to voluntarily release them, 18 U.S.C. § 2703 would have required police to provide Cricket with a warrant, court order, or evidence of the subscriber's consent.

[5] For this reason, we need not address Registe's remaining contentions.

[6] Although the trial court denied Registe's motion to suppress on other grounds, a trial court's ruling on a motion to suppress will be upheld if it is right for any reason. Fincher v. State, 276 Ga. 480, 481 (2) (578 SE2d 102) (2003).

S12A1190. REGISTE v. THE STATE

HUNSTEIN, Chief Justice, concurring specially.

Because I agree that applicable state law does not provide for suppression as a remedy for a service provider's improper voluntary disclosure of cellular phone records, I concur in the majority's conclusion that Registe's motion to suppress was properly denied. I write, however, to register my disagreement with the majority's reliance on the federal Stored Communications Act in reaching this conclusion. In addition, I write to highlight the sizable loophole created by our current legislative scheme in this area, which potentially enables law enforcement to circumvent the strict procedural requirements for accessing protected records by simply "requesting" such records with a tone of sufficient urgency so as to generate a belief on the part of the custodian that an emergency exists.

1. As suggested but not clearly settled in the majority opinion, I believe that OCGA § 16-11-66.1 regulates only those situations in which law enforcement is authorized to require the disclosure of stored wire or electronic information from a service provider. Subsection (a) on its face describes the

prerequisites for law enforcement to "require" such disclosures; subsection (b) mandates that service providers "shall" make disclosures when law enforcement complies with subsection (a). Intended to establish ground rules for the issuance and use of warrants, subpoenas, and other means by which law enforcement can compel the disclosure of information, the statute does not address situations involving voluntary disclosures by service providers. Compare 18 U.S.C. § 2702 (c) (enumerating circumstances under which voluntary disclosures by service providers are proper). Because voluntary disclosures fall entirely outside the scope of OCGA § 16-11-66.1 and are not otherwise regulated under the code sections to which the suppression remedy in OCGA § 16-11-67 applies, there is no statutory basis under state law for ordering the suppression of evidence obtained through such voluntary disclosures.

Unlike our state law, which is directed primarily at the circumstances under which law enforcement is authorized to access protected information, the federal Stored Communications Act is directed more broadly at the circumstances under which the service provider is authorized to disclose such information to third parties generally. See 18 U.S.C. §§ 2702, 2703. The voluntary disclosure of protected information by service providers thus fits

comfortably within the realm of the federal law. As the majority opinion notes, 18 U.S.C. § 2702 (c) (4) permits the voluntary disclosure of protected records "to a government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay." Though the majority may be correct in concluding that Cricket's disclosure in this case satisfied the requirements of this "emergency" exception under federal law, we need not decide that issue because the federal law does not provide for suppression of evidence as a remedy for violations. Thus, for purposes of assessing Registe's motion to suppress, whether Cricket complied with the Stored Communications Act in making its voluntary disclosure is irrelevant. In short, because the suppression remedy is applicable only for violations of state law, and because state law does not regulate voluntary disclosures by service providers, there is no statutory basis for suppression of the evidence in this case.

2. As this case demonstrates, the absence of regulation of voluntary disclosures under current state law affords law enforcement officers virtual free rein to "encourage" service providers, by making reference to an urgent law enforcement need, to disclose information that the officers could otherwise

access without customer consent only by obtaining a warrant, court order, or subpoena. The strict procedural safeguards designed to protect stored electronic information from routine law enforcement scrutiny can be easily circumvented so long as the officers making the "request" do so in a manner that is not overtly coercive. Law enforcement officers have little incentive to undertake the more onerous task of obtaining a warrant or court order, at least at the outset, when they can simply send an urgent-sounding fax like that used in this case and hope that the service provider is sufficiently impressed by the gravity of the situation to disclose the information without further inquiry. If the service provider does comply, law enforcement has obtained what it wants without any judicial oversight; there is no potential for suppression of the evidence under state law; and, because the disclosure is considered "voluntary," any potential liability under the federal Stored Communications Act would presumably fall on the shoulders of the service provider. See 18 U.S.C. § 2702 (a) (3) (general prohibition on disclosure of subscriber information by service provider); § 2707 (authorizing civil actions for damages and other relief against those who violate statute). Law enforcement has nothing to lose by first attempting to effectuate a voluntary disclosure and can always resort to a warrant or court order if its

initial attempt fails.

There is no indication that the police in this case had any untoward motives, but I am concerned that our current scheme invites potential abuse. Because it is the service providers who largely control the extent to which abusive practices succeed, I encourage these service providers to exercise caution and independent judgment in responding to law enforcement records requests that have not been approved through the judicial process.

I am authorize to state that Justice Blackwell joins in Division 1 of this special concurrence.