UNPUBLISHED

UNITED STATES COURT OF APPEALS

FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v. No. 99-4793

SCOTT MARSHALL HAMBRICK,
Defendant-Appellant.

Appeal from the United States District Court
for the Western District of Virginia, at Charlottesville.
James H. Michael, Jr., Senior District Judge.
(CR-98-42-C)

Argued: May 4, 2000

Decided: August 3, 2000

Before MURNAGHAN and TRAXLER, Circuit Judges, and
Jerome B. FRIEDMAN, United States District Judge for the
Eastern District of Virginia, sitting by designation.

Affirmed by unpublished per curiam opinion.

COUNSEL

ARGUED: Deborah C. Wyatt, WYATT & CARTER, Charlottesville, Virginia, for Appellant. Anne Marie Farrar, Trial Attorney, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C., for Appellee. **ON BRIEF:** Bruce R. Williamson, WILLIAMSON & TOSCANO, Charlottesville, Virginia, for Appellant. Anthony P. Giorno, OFFICE OF THE UNITED STATES ATTORNEY, Roanoke, Virginia, for Appellee.

Unpublished opinions are not binding precedent in this circuit. See Local Rule 36(c).

OPINION

PER CURIAM:

Scott Marshall Hambrick entered a conditional plea of guilty to one count of transmission of child pornography, in violation of Title 18 U.S.C. § 2252(a)(1), and one count of possession of child pornography, in violation of Title 18 U.S.C. § 2242A(a)(5)(B). Hambrick reserved his right to appeal the district court's denial of his motion to suppress. The district court denied Hambrick's motion to suppress on July 7, 1999, and Hambrick appeals only the denial of this motion.**1** Finding no error in the court's ruling, we affirm.

I.

Hambrick was arrested in his Albemarle County home following a search warrant executed by the Albemarle County Police and federal officials on July 10, 1998. At the time of the offenses and his arrest, Hambrick was a Captain in the Albemarle County Police Department. He was indicted for possession of child pornography, transmission of child pornography, and using an interstate facility to engage a child in sexual activity. These charges stemmed from on-line chats Hambrick had with another adult, Detective J.L. McLaughlin, a police officer with the Keene, New Hampshire Police Department, who is a member of a regional task force against Internet crimes aimed at children. McLaughlin was on-line on a chat room called"#gaydads4sons" when he encountered Hambrick, who engaged McLaughlin in discussions regarding Hambrick's interest in young boys and an exchange

---

1 At sentencing, Hambrick sought a downward departure based on his personal circumstances, which was denied. Originally, defendant argued on appeal that the failure to downwardly depart was reversible error. However, in his reply brief, Hambrick waived the argument on the downward departure and indicated that he only intended to proceed on the motion to suppress.

of pornography, obviously without knowing McLaughlin's connection with the police department. At the time of the chats, McLaughlin assumed the identity of a fourteen-year-old boy and was writing under the screen name, "Rory14," and the defendant was writing under the screen name "BlowUinVA."

During the course of the on-line communications,"BlowUinVA" stated that he was looking for a boy who was bored with his home life and who would run away to live with "BlowUinVA" and engage in a sexual relationship. When "Rory14" informed "BlowUinVA" that he had a twelve-year-old brother, "BlowUinVA" requested that "Rory14" also bring his brother for the purpose of engaging in a sexual relationship with him. "BlowUinVA" stated that he would send money for the boys to take a bus to Richmond, Virginia. Ultimately, "BlowUinVA" sent $270 to a Post Office Box provided by "Rory14" along with explicit instructions regarding the meeting arrangements.

Following several chats with Hambrick, but prior to submission of any child pornography, McLaughlin faxed to Hambrick's Internet Service Provider ("ISP"), MindSpring, a subpoena obtained on March 19, 1998. The subpoena was signed by Richard R. Richards. Mr. Richards is a justice of the peace as well as a detective in the Keene Police Department. It is undisputed that the procedure utilized for the issuance of this subpoena was faulty, and the government has conceded the invalidity of the warrant. The subpoena sought only user non-content information, and not any content information such as e-mail content or file content.

Based on the subpoena, McLaughlin received the following information from MindSpring: Hambrick's name, billing address, on-line address ("IP address"), credit card information, and other identifying information. The government obtained this information to determine the identity of "BlowUinVA," and this information was not utilized to access Hambrick's e-mails or other file content. McLaughlin then referred the matter to the FBI, who assumed the identity of "Rory14" in the on-line communications with Hambrick. The FBI later sought information from MindSpring by using a "grand jury subpoena."

Based on the information received from the subpoenas, the FBI obtained a search warrant for Hambrick's residence, and executed the

warrant on July 10, 1998. The search yielded computers and computer disks containing child pornography, including those transmitted to McLaughlin during the investigation. As a result, the defendant was indicted on July 16, 1998 for two counts of using an interstate facility to engage a child in sexual activity, and two counts of transmission of child pornography. Later, the grand jury returned a superceding indictment against the defendant for three counts of transmission of child pornography, one count of possession of child pornography, two counts of using an interstate facility to engage a child in sexual activity, and one count for forfeiture.

The defendant moved to suppress the evidence arguing that the subpoenas were invalid. The government, including the New Hampshire Attorney General, conceded that the subpoenas were invalid, but denied that they were obtained in bad faith. The motion to suppress was taken under advisement by the district court. The defendant subsequently entered into a plea agreement contingent on the district court's decision on the motion to suppress. The district court denied the motion, and the defendant pled guilty to one count of possession of child pornography and one count of transmission of child pornography, and retained the right to appeal the denial of the motion to suppress. This appeal follows.

II.

In reviewing the denial of a motion to suppress, we review the factual findings of the district court for clear error and its legal conclusions de novo. See United States v. Johnson, 114 F.3d 435, 439 (4th Cir. 1997).

III.

A.

In Katz v. United States, 389 U.S. 347 (1967), the Supreme Court analyzed the scope of the protection afforded by the Fourth Amendment, stating that a search occurs only when there has been a "physical intrusion" in a "constitutionally protected area," noting further that the Fourth Amendment "protects people, not places." Id. at 351-53.

Since Katz, the Supreme Court has consistently held that the application of the Fourth Amendment depends on whether the person invoking this protection can claim a "justifiable," "reasonable," or "legitimate expectation of privacy." See , e.g., Rakas v. Illinois, 439 U.S. 128, 143 (1978); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Terry v. Ohio, 392 U.S. 1, 9 (1968). To establish an expectation of privacy under the Fourth Amendment, Hambrick must establish 1) that he held "an actual (subjective) expectation of privacy," and 2) that this expectation of privacy is "one that society is prepared to recognize as `reasonable.'" See Katz, 389 U.S. at 361 (Harlan, J., concurring). The district court correctly applied the traditional Fourth Amendment analysis as stated in Katz to Hambrick's billing information released to the government, and the district court properly denied Hambrick's motion to suppress. **2** At issue on appeal is whether Hambrick had a legitimate privacy expectation in information that he provided to MindSpring which was subsequently released to the government as a result of an invalid subpoena.

"What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." Id. at 351. Accordingly, the Supreme Court has held that a "person has no legitimate expectation of privacy in information . . . voluntarily turn[ed] over to third parties." Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (holding that under Katz, the defendant likely did not entertain an actual expectation of privacy in the phone numbers he dialed that were revealed through a pen registry, and if he did, that expectation was not one society would consider legitimate). The Supreme Court further stated in Smith that when an individual voluntarily conveys information to

---

2 We similarly agree with the district court's conclusion with regard to the inapplicability of the Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§ 2510-2711, to the facts of this case. The ECPA does not represent a legislative determination of a reasonable expectation of privacy in non-content information released by ISPs. The ECPA does not even provide for the relief requested in this case, namely in the form of suppression. See 18 U.S.C.§ 2707 (providing to aggrieved individual a right to certain civil remedies); 18 U.S.C. § 2708 (reciting exclusivity of remedies); see also Tucker v. Waddell, 83 F.3d 688, 693 (4th Cir. 1996) (holding that the ECPA does not authorize a civil suit against a governmental entity for violations of§ 3703(c)).

a third party, the individual "assume[s] the risk" of subsequent disclosure. See id. at 744.

In United States v. Miller, 425 U.S. 435 (1976), the Supreme Court cited Hoffa v. United States, 385 U.S. 293 (1966), for the proposition that "`no interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into `the security a man relies upon when he places himself or his property within a constitutionally protected area.'" Miller, 425 U.S. at 440 (citing Hoffa, 385 U.S. at 301-02). The Supreme Court in Miller emphasized that an individual has no Fourth Amendment privacy interest in information released to a third party and later conveyed by that third party to a governmental entity, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."**3** Id. at 443. The Supreme Court concluded that the bank records subpoenaed in Miller were not "private papers" and that the defendant could assert neither ownership nor possession over these papers. See id. at 441-42. Instead, the Supreme Court concluded that they were merely business records of the bank. See id. at 442.

The subpoena at issue in this case requested that MindSpring produce "any records pertaining to the billing and/or user records documenting the subject using your services on March 14th, 1998 at 1210HRS (EST) using the Internet Protocol Number 207.69.169.92." This information was requested in order to determine the identity of the individual using the screen name "BlowUinVA," as this screen name is tied to the user's identity in all of MindSpring's business records. The information the government received from MindSpring consisted of Hambrick's subscriber information, which included his

---

3 The district court, however, noted that there is no evidence in this case to suggest that there was a restrictive agreement between Hambrick and MindSpring that would limit the right of MindSpring to release Hambrick's personal information to nongovernmental entities. The district court further observed that it is common practice for ISPs, such as Mindspring, to reveal the type of information at issue in this case to marketing firms and other organizations interested in soliciting business from Internet users.

name; billing address; home, work, and fax phone numbers; and other billing information. When Hambrick entered into a service agreement with MindSpring, he knowingly revealed this information to MindSpring and its employees. The records that the government obtained from MindSpring had been available to MindSpring employees in the normal course of business. Once the government received this information, it was not later utilized to read Hambrick's e-mails or to attain any other content information.

While under certain circumstances, a person may have an expectation of privacy in content information, a person does not have an interest in the account information given to the ISP in order to establish the e-mail account, which is non-content information. See Smith, 442 U.S. at 741 (noting critical distinction between content and non-content information); Katz, 389 U.S. at 352 (holding that the user of a public telephone is entitled to "assume that the words he utters into the mouthpiece will not be broadcast to the world"). Disclosure of this non-content information to a third party destroys the privacy expectation that might have existed previously. In this case, the government never utilized the non-content information retrieved from MindSpring to attain additional content information, such as the substance of Hambrick's e-mails. In this case, as in Miller , there is no legitimate expectation of privacy in information "voluntarily conveyed to [a third party] and exposed to their employees in the ordinary course of business." Miller, 425 U.S. at 442. The information subject to the motion to suppress is merely third-party business records, and therefore, Hambrick's Fourth Amendment claim cannot succeed.**4**

B.

The invalidity of the subpoena in this case does not trigger the application of the Fourth Amendment, as Hambrick had no privacy

---

4 While the Court is aware of the"revolutionary" nature of the Internet as well as the vast extent of communications it has initiated, the information at issue in this case is not distinguishable from the materials in Miller and Smith, as the government merely obtained non-content information that was part of MindSpring's business records. We do not address here any subsequent use of the non-content information to reveal the substance of an Internet user's e-mails or other file content.

interest in the non-content information obtained as a result of the subpoena. In Miller, the Supreme Court held that the "general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time the subpoena issued." Id. at 444. Extending this rationale to circumstances in which the evidence is obtained as a result of an invalid subpoena, the Supreme Court in United States v. Payner, 447 U.S. 727 (1980), held that a federal court should not "suppress otherwise admissible evidence on the ground that it was seized unlawfully from a third party not before the court." Id. at 735. The Payner Court reasoned that "the interest in deterring illegal searches does not justify the exclusion of tainted evidence at the instance of a party who was not the victim of the challenged practices." Id. Based on these Supreme Court standards, Hambrick had no legally protected interest in the information provided by MindSpring to the government pursuant to an invalid subpoena. Therefore, the district court correctly concluded that Hambrick had no reasonable expectation of privacy in the information the government obtained from MindSpring, and we agree with the district court's denial of Hambrick's motion to suppress.

For the foregoing reasons, the judgment of the district court is affirmed.

AFFIRMED