

2000 WL 1062039

United States Court of Appeals, Fourth Circuit.

UNITED STATES of America, Plaintiff-Appellee,
v.
Scott Marshall HAMBRICK, Defendant-Appellant.

Decided Aug. 3, 2000.

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

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. 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 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

The defendant moved to suppress the evidence arguing that the subpoenas were invalid. The government . . . conceded that the subpoenas were invalid, but denied that they were obtained in bad faith. The motion to suppress was . . . denied This appeal follows. [...]

III.

A.

In *Katz v. United States*, . . . the Supreme Court 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." 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.'" 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." 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). The Supreme Court further stated in *Smith* that when an individual voluntarily conveys information to a third party, the individual "assume[s] the risk" of subsequent disclosure.

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).

. . . . The Supreme Court in [*United States v. Miller*—the bank records case] 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 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. Instead, the Supreme Court concluded that they were merely business records of the bank.

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 name; billing address; home, work, and fax phone numbers; and other billing information. When Hambrick entered into a service agree-

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.

ment 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.

[...]

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