

H

United States District Court, W.D. Virginia,
Charlottesville Division.

UNITED STATES of America
v.
Scott M. HAMBRICK.

No. CRIM. A. 98-0042-C.

July 7, 1999.

In criminal prosecution, defendant moved to suppress information obtained from his Internet service provider. The District Court, Michael, Senior District Judge, held that: (1) Electronic Communications Privacy Act did not create reasonable expectation of privacy in Internet customer's personal information, and (2) customer did not have reasonable expectation of privacy in personal information.

Motion denied.

West Headnotes

[1] Criminal Law  **394.5(2)**
[110k394.5\(2\) Most Cited Cases](#)

Defendant in criminal case who is seeking suppression of evidence on Fourth Amendment grounds may invoke violation of his own rights but not rights of third parties. [U.S.C.A. Const.Amend. 4.](#)

[2] Searches and Seizures  **26**
[349k26 Most Cited Cases](#)

Electronic Communications Privacy Act does not create reasonable expectation of privacy for Fourth Amendment purposes in Internet customer's name, address, social security number, credit card number, and proof of Internet connection obtained by Internet providers; Congress did not provide for suppression of improperly obtained data or records, and Act's concern for privacy extends only to government invasions of privacy. [18 U.S.C.A. § 2510-2711.](#)

[3] Searches and Seizures  **26**
[349k26 Most Cited Cases](#)

For Internet customer to have reasonable expectation of privacy in his personal information under risk-analysis approach to Fourth Amendment: (1) data

must not be knowingly exposed to others, and (2) Internet service provider's ability to access data must not constitute disclosure. [U.S.C.A. Const.Amend. 4.](#)

[4] Searches and Seizures  **26**
[349k26 Most Cited Cases](#)

Internet customer had no reasonable expectation of privacy in personal information supplied to Internet service provider; customer knowingly revealed information to provider and selected his own screen name, provider's employees had access to records, and agreement between customer and provider did not limit right of provider to reveal information to nongovernment entities. [U.S.C.A. Const.Amend. 4.](#)

***505** [Bruce R. Williamson, Jr.](#), Williamson & Toscano, Charlottesville, VA, Deborah Chasen Wyatt, Wyatt & Carter, Charlottesville, VA, for Defendant.

Anne Marie Farrar, U.S. Department of Justice, Criminal Division, Washington, DC, for U.S.

MEMORANDUM OPINION

[MICHAEL](#), Senior District Judge.

I.

Before the court is the defendant's January 27, 1999 "Motion to Suppress." Defendant Scott M. Hambrick seeks the suppression of all evidence obtained from his Internet Service Provider ("ISP"), MindSpring, and seeks the suppression of all evidence seized from his home pursuant to a warrant issued by this court. For the reasons discussed below, the court denies the defendant's motion.

II.

FACTS

On March 14, 1998, J.L. McLaughlin, a police officer with the Keene, New Hampshire Police Department, connected to the Internet and entered a chat room called "Gay dads 4 sex." [\[FN1\]](#) McLaughlin's screen name was "Rory14." In this chat room, Detective McLaughlin encountered someone using the screen name "Blowuinva." Based on a series of online conversations between "Rory14" (Det.McLaughlin) and "Blowuinva," McLaughlin concluded that "Blowuinva" sought to entice a fourteen-year-old boy to leave New Hampshire and live with "Blowuinva." Because of the anonymity of the Internet, Detective McLaughlin did not know the true identity of the person with whom he was communicating nor did he know where "Blowuinva"

lived. "Blowuinva" had only identified himself as "Brad."

FN1. Our society has sensationalized all things involving sex. See, e.g., MICHEL FOUCAULT, HISTORY OF SEXUALITY (Alan Sheridan trans., Vintage Books 2d ed.1995) (1978). Mr. Hambrick is a citizen charged with committing a crime. The sexual nature of the crime must not be an issue in resolving the legal issues. The court recites only those facts necessary to place the law in a meaningful context.

To determine Blowuinva's identity and location, McLaughlin obtained a New Hampshire state subpoena that he served on Blowuinva's Internet Service Provider, MindSpring, located in Atlanta, Georgia. The New Hampshire state subpoena 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 Internet Protocol Number 207.69.169.92." MindSpring complied with the subpoena. On March 20, 1998, MindSpring supplied McLaughlin with defendant's name, address, credit card number, e-mail address, home and work telephone numbers, fax number, and the fact that the Defendant's account was connected to the Internet at the Internet Protocol (IP) address. FN2

FN2. That the defendant's account was connected to the Internet at the Internet Protocol address means that during the online conversation between McLaughlin and "Blowuinva," the defendant's computer was connected to the Internet through MindSpring.

*506 A justice of the peace, Richard R. Richards, signed the New Hampshire state subpoena. Mr. Richards is not only a New Hampshire justice of the peace, but he is also a detective in the Keene Police Department, Investigation Division. Mr. Richards did not issue the subpoena pursuant to a matter pending before himself, any other judicial officer, or a grand jury. At the hearing on the defendant's motion, the government conceded the invalidity of the warrant. The question before this court, therefore, is whether the court must suppress the information obtained from MindSpring, and all that

flowed from it, because the government failed to obtain a proper subpoena.

III.

DISCUSSION

A.

[1] It has been long established that a defendant in a criminal case who is seeking the suppression of evidence on Fourth Amendment grounds may invoke the violation of his own rights but not the rights of third parties. Courts traditionally refer to this concept as "standing." In Rakas v. Illinois, the Supreme Court suggested that separate treatment of standing was no longer necessary. 439 U.S. 128, 139-40, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). The appropriate question, the Court noted, is whether the "disputed search infringed an interest of the defendant which the Fourth Amendment was designed to protect." Id. at 140, 99 S.Ct. 421.

In Katz v. United States, the Supreme Court provided an important starting point in defining the scope of the interest that the Fourth Amendment protects. 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967). The Court held that the capacity to claim the protection of the Fourth Amendment depends on "whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place." Id. Since Katz, the Court has instructed that the Fourth Amendment applies only where: (1) the citizen has manifested a subjective expectation of privacy, and (2) the expectation is one that society accepts as "objectively reasonable." California v. Greenwood, 486 U.S. 35, 39, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988). This is still the appropriate standard of analysis for use in determining whether the Fourth Amendment protects Mr. Hambrick's MindSpring records. The defendant has asserted that the test articulated in Wyoming v. Houghton--whether the intrusion on the individual's privacy outweighs the degree to which it is necessary to promote legitimate government interests--is the Fourth Amendment test that applies to this case. 526 U.S. 295, ---, 119 S.Ct. 1297, 1300, 143 L.Ed.2d 408 (1999). Such a test, however, does not trump Katz or the implementation of a reasonableness analysis. In order to determine whether an individual's privacy has been intruded, the Katz test must first be applied to assess whether that individual had a reasonable expectation of privacy. Applying the first part of the Katz analysis, Mr. Hambrick asserts that he had a subjective expectation of privacy in the information that MindSpring gave to the government. However, resolution of this matter hinges on whether Mr.

Hambrick's expectation is one that society accepts as "objectively reasonable."

The objective reasonableness prong of the privacy test is ultimately a value judgment and a determination of how much privacy we should have as a society. In making this constitutional determination, this court must employ a sort of risk analysis, asking whether the individual affected should have expected the material at issue to remain private. See *Rakas*, 439 U.S. at 148-49, 99 S.Ct. 421. The defendant asserts that the Electronic Communications Privacy Act ("ECPA") "legislatively resolves" *507 this question. 18 U.S.C. § § 2510-2711 (1994).

The Electronic Communications Privacy Act

Congress enacted the Electronic Communications Privacy Act of 1986 to protect against the unauthorized interception of various forms of electronic communications and to update and elaborate on federal privacy protections and standards in light of changing computer and telecommunications technologies. S REP. NO. 99-541, at 1 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555. Title I of the Act addresses the interception of wire, oral and electronic communications. Title II addresses access to stored wire and electronic communications and transactional records. Title III addresses pen registers and trap and trace devices. The information obtained through the use of the government's invalid subpoena consisted of the defendant's name, address, social security number, credit card number, and certification that the defendant was connected to the Internet on March 14, 1998. Thus, this information falls within the provisions of Title II of the ECPA.

The government may require that an ISP provide stored communications and transactional records only if (1) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or (2) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of the information in question. See 18 U.S.C. § 2703(a)(c)(1)(B). When an ISP discloses stored communications or transactional records to a government entity without the requisite authority, the aggrieved customer's sole remedy is damages. See 18 U.S.C. § § 2707- 2708 (1994 & Supp.1996).

[2] Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain,

the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of "reasonably objective" for Fourth Amendment purposes. Despite its concern for privacy, Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act. Additionally, the ECPA's concern for privacy extends only to government invasions of privacy. ISPs are free to turn stored data and transactional records over to nongovernmental entities. See 18 U.S.C. § 2703(c)(1)(A) (1994) ("[A] provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service ... to any person other than a governmental entity."). For Fourth Amendment purposes, this court does not find that the ECPA has legislatively determined that an individual has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection. The fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information. This, however, does not end the court's inquiry. This court must determine, within the constitutional framework that the Supreme Court has established, whether Mr. Hambrick's subjective expectation of privacy is one that society is willing to recognize.

Privacy Interests and Internet Service Providers

[3] To have any interest in privacy, there must be some exclusion of others. To have a reasonable expectation of privacy under the Supreme Court's risk-analysis approach to the Fourth Amendment, two conditions must be met: (1) the data must not be knowingly exposed to others, and (2) the Internet service provider's ability to access the data must not constitute a disclosure. In *Katz*, the Supreme Court *508 expressly held that "what a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection." 389 U.S. at 351, 88 S.Ct. 507. Further, the Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); see, e.g., *United States v. Miller*, 425 U.S. 435, 442-43, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976); *Couch v. United States*, 409 U.S. 322, 335-36, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973).

The Supreme Court's risk-analysis approach makes the work of the courts difficult when analyzing

previously adjudicated situations in the world of cyberspace. This court's research, assisted by the parties' thorough briefs, has failed to find any factually and legally analogous case law. The defendant cites [United States v. Maxwell, 45 M.J. 406 \(1996\)](#), as the only published federal decision that deals with the question of the expectation of privacy in information obtained from an ISP. Although some of the facts of [Maxwell](#) appear to be similar to the facts in the present case, [Maxwell](#) has little or no precedential value because the United States Court of Appeals for the Armed Forces decided the case. That court reviews the convictions of a court-martial and is entirely separate from the United States Courts of Appeals. Also, despite the fact that the Electronic Communications Privacy Act is evidence that some degree of privacy should be accorded the information at issue in this matter, the ECPA ultimately falls short of serving as a source of extra-constitutional protection for the information and cannot undo the Supreme Court's restrictive risk-analysis approach.

[4] The court finds the defendant's implicit argument that certain information in cyberspace should be private requires careful consideration. Legal scholars and Congress have noted the ubiquity of cyberspace in the lives of all Americans. *See generally, e.g., S. REP. NO. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555; Michael Adler, Note, Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search, 195 YALE L.J. 1093 (1996); Randolph S. Sergeant, Note, A Fourth Amendment Model for Computer Networks and Data Privacy, 81 VA. L. REV. 1181 (1995).* The members of our society increasingly live important parts of their lives through the Internet. Cyberspace is a nonphysical "place" and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis. So long as the risk-analysis approach of *Katz* remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology. In so doing, the court must deny Mr. Hambrick's motion to suppress.

When Scott Hambrick surfed the Internet using the screen name "Blowuinva," he was not a completely anonymous actor. It is true that an average member of the public could not easily determine the true identity of "Blowuinva." Nevertheless, when Mr. Hambrick entered into an agreement to obtain Internet access from MindSpring, he knowingly revealed his name, address, credit card number, and telephone number to MindSpring and its employees. Mr. Hambrick also selected the screen name

"Blowuinva." When the defendant selected his screen name it became tied to his true identity in all MindSpring records. MindSpring employees had ready access to these records in the normal course of MindSpring's business, for example, in the keeping of its records for billing purposes, and nothing prevented MindSpring from revealing this information to nongovernmental actors. [\[FN3\]](#) *509 Also, there is nothing in the record to suggest that there was a restrictive agreement between the defendant and MindSpring that would limit the right of MindSpring to reveal the defendant's personal information to nongovernmental entities. Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.

[FN3.](#) It is apparently common for ISPs to provide certain information that Mr. Hambrick alleges to be private to marketing firms and other organizations interested in soliciting business from Internet users.

Although not dispositive to the outcome of this motion, it is important to note that the court's decision does not leave members of cybersociety without privacy protection. Under the ECPA, Internet Service Providers are civilly liable when they reveal subscriber information or the contents of stored communications to the government without first requiring a warrant, court order, or subpoena. *See 18 U.S.C. §§ 2703, 2707, 2708 (1994 & Supp.1996).* Here, nothing suggests that MindSpring had any knowledge that the facially valid subpoena submitted to it was in fact an invalid subpoena. Had MindSpring revealed the information at issue in this case to the government without first requiring a subpoena, apparently valid on its face, Mr. Hambrick could have sued MindSpring. This is a powerful deterrent protecting privacy in the online world and should not be taken lightly.

The defendant's motion to suppress also embraces evidence found in his home pursuant to a residence search warrant. The defendant contends that because the residence search warrant was supported by an affidavit reciting evidence allegedly protected as to the defendant by his right to privacy, the court likewise must suppress the materials seized from his home. As this court has found that the MindSpring materials are not so protected, the predicate for this motion to suppress the materials seized from the defendant's home fails, and therefore the court does

not suppress such materials.

B.

Finally, the court briefly addresses the government's argument that, even if the defendant has a reasonable expectation of privacy in the records, the MindSpring records are the product of inevitable discovery and should be admitted despite the defective subpoena. Following the New Hampshire authorities' initial investigation of Mr. Hambrick, New Hampshire turned the case over to the Federal Bureau of Investigation. In the course of its investigation, the FBI obtained a grand jury subpoena for the same records that had been the subject of the invalid New Hampshire subpoena. The government principally relies on *Nix v. Williams* to support its argument that even though the New Hampshire authorities obtained Mr. Hambrick's records as the result of an invalid subpoena, the same records inevitably would have been discovered during the course of a subsequent federal investigation. [467 U.S. 431, 447, 104 S.Ct. 2501, 81 L.Ed.2d 377 \(1984\)](#).

The court need not reach this issue because it denies the defendant's motion on other grounds, but notes that the Fourth Circuit has made it clear that an inevitable discovery argument based on conjecture about what may have been discovered if the initial search had been legal must fail. See *United States v. Thomas*, [955 F.2d 207, 210-11 \(4th Cir.1992\)](#). The FBI would not have become involved in the investigation of Mr. Hambrick but for the fact that he does not reside in New Hampshire. Mr. Hambrick's records revealed this fact only after the issuance of the invalid New Hampshire subpoena. For the government's argument to succeed, the court would have to assume that without the information about Mr. Hambrick's place of residence, the FBI would have become involved in the investigation and then would have issued a subpoena for the same records that the New Hampshire authorities already had obtained. Such assumptions *510 involve too much conjecture to be termed "inevitable."

IV.

For the foregoing reasons, the defendant's motion to suppress all evidence obtained from his ISP, MindSpring, and all evidence seized from his home pursuant to a subsequent warrant must be denied. An appropriate Order shall, this day, issue.

The court wishes to express its appreciation to the parties for the assistance that their thorough briefs provided.

55 F.Supp.2d 504

END OF DOCUMENT