In The

UNITED STATES COURT OF APPEALS

For the Eighth Circuit

No. 02-1238

Criminal

UNITED STATES OF AMERICA,

APPELLANT,

v.

DALE ROBERT BACH,

APPELLEE.

Appeal from the United States District Court for the

District of Minnesota

BRIEF OF APPELLANT

THOMAS B. HEFFELFINGER
United States Attorney

BY: Bridgid E. Dowdal
Paul H. Luehr
Attorney ID No. 0253716
Attorney ID No. DC 445720
District of Minnesota
600 United States Courthouse
300 South Fourth Street
Minneapolis, MN 55415
(612) 664-5600

Attorneys for Appellant

SUMMARY AND REQUEST FOR ORAL ARGUMENT

The District Court erred in holding that the Fourth Amendment is violated where a state police officer faxed a search warrant to Yahoo and was not physically present to "supervise and instruct" Yahoo employees as it gathered the electronic information in compliance with the warrant. Relying on a rigid and formalistic reading of Title 18 U.S.C. § 3105, which textually requires that the executing officer be physically present to execute a federal warrant, the District Court found that a parallel requirement exists under the Constitution. But § 3105 applies to the execution of federal, not state, warrants. More fundamentally, neither § 3105, nor the Constitution, requires am officer's presence during the execution of each and every warrant.

Only the Fourth Amendment governs suppression of evidence seized by state and local officials. See United States v. Applequist, 145 F.3d 976, 978-979 (8th Cir. 1998). Here, the sole question is whether defendant's Fourth Amendment's rights were violated by virtue of a state officer not being physically present to serve Yahoo with the search warrant.

The issue in this case involves a relatively unchartered area of technologically advanced mechanisms for creating, distributing and storing information. As the 10th Circuit

recently stated in United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) petition for cert. filed (March 25, 2002).

> The advent of the electronic age and, as we see in this case, the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law. . . . This does not, of course, mean that the Fourth Amendment does not apply to computers and cyberspace. Rather, we must acknowledge the key differences and proceed accordingly.

In the present case, it was legally, factually and constitutionally reasonable for law enforcement officers to fax the search warrant to Yahoo instead of physically serving it upon them. Casting the Fourth Amendment "reasonableness" requirement as an inflexible rule forbidding an Internet service provider ("ISP") from responding to a search warrant outside the physical presence of an officer would undercut every law enforcement investigation that depends on such electronic evidence. In many cases it would be literally impossible for an officer to be physically present inside the provider's facilities during the retrieval of an ISP's electronic records.

This Court should reverse the District Court's holding that it is a violation of defendant's Fourth Amendment rights for Yahoo to comply with a valid search warrant that was served by law enforcement by facsimile.

The United States respectfully requests that the Court grant oral argument on this issue and allot twenty (20) minutes of argument to each side.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

PAGE

CASES:

TABLE OF AUTHORITIES (cont.)

STATEMENT OF THE ISSUES

I. WHETHER SECTION 3105 APPLIES TO STATE OFFICERS IN THIS CASE WHERE THERE IS NO FOURTH AMENDMENT VIOLATION.

United States v. Murphy, 69 F.3d 237 (8th Cir. 1995)

United States v. Applequist, 145 F.3d 976 (8th Cir. 1998)

Ayeni v. Mottola, 35 F.3d 680 (2d Cir. 1994)
cert. denied 514 U.S. 1062 (1995)

II. WHETHER THE FOURTH AMENDMENT REQUIRES AN OFFICER TO BE PRESENT WHILE AN EMAIL PROVIDER RENDERED TECHNICAL ASSISTANCE IN THE EXECUTION OF A VALID SEARCH WARRANT.

Wilson v. Arkansas, 514 U.S. 927 (1995)

United States v. Walser, 275 F.3d 981(10th Cir. 2001), petition for cert. filed (Mar. 25, 2002)

Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and Terminating Trap, Bell Telephone Co. of Pennsylvania, 610 F.2d 1148 (3rd Cir. 1979)["Pennsylvania Bell"]

In re Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities, United States v. Mountain States Telephone & Telegraph Co., 616 F.2d 1122 (9th Cir. 1980)["Mountain Bell"]

Craighead Elec. Co-op Corp. v. City Water and Light Plant of Jonesboro, 278 F.3d 859, 861(8th Cir. 2002)

Washington v. Kern, 914 P.2d 114, 117-18 (Wa. Ct. App. 1996) Rev denied by 925 P.2d 988 (WA. 1996).

18 U.S.C. §2703(a)-(f)(2001)

III. WHETHER BLANKET SUPPRESSION WAS PROPER WHEN DEFENDANT LACKED STANDING TO CHALLENGE THE SEARCH AND SEIZURE OF ANOTHER PERSON'S EMAIL ACCOUNT.

United States v. Rodriguez-Arreola, 270 F.3d 611(8th Cir. 2001)

United States v. Gomez, 16 F.3d 254(8th Cir. 1994)

JURISDICTIONAL STATEMENT

This appeal is taken by the United States from a final order suppressing evidence entered on December 17, 2001, by the Honorable Paul A. Magnuson of the United States District Court for the District of Minnesota. The District Court had jurisdiction pursuant to 18 U.S.C. § 3231.

A timely notice of appeal was filed by the United States on January 15, 2002. This court has jurisdiction pursuant to 18 U.S.C. § 3731.

STATEMENT OF THE FACTS

A. The Search Warrant

On October 10, 2000, Sgt. Brook Schaub ("Schaub") of the St. Paul Police Department, was working as part of the Minnesota Internet Crimes Against Children Task Force ("MICAC") when he was contacted by a woman ("DL"). See Appendix ("App.") at 2. DL gave Schaub a text document that she had retrieved from and printed off her family computer. Id. at 2-3. The document contained a partial log of a dialogue that took place between her son ("AM"), who is a minor, and a party using the name, "dlbch15." Id. at 3. In the dialogue between these parties, "dlbch15" asked AM where he should hide an object near AM's home. Id. "dlbch15" also asked AM, "don't you want to see me again?" Id. The dialogue also stated that if "dlbch15" was going to drive to St. Paul to hide the object near AM's house, then "[dlbch15] would rather see [AM] again." Id. The suggestion that AM had met with "dlbch15" on earlier occasions prompted DL to seek the assistance of MICAC. Id.

When questioned by law enforcement about the dialogue, AM stated that it occurred in a "chat room" on an Internet website, *www.yahoo.com*. Id. AM said that "dlbch15" was going to hide Playboy magazines for AM in the bushes near a business on Ford Parkway. Id. AM stated that he had met "dlbch15" in person on

September 10, 2000 on Ford Parkway, but denied any sexual contact between them. Id. When interviewed at the Children's Hospital, AM did not disclose any sexual contact with "dlbch15", and failed to make a photo identification of the defendant, Dale Robert Bach ("Bach"). Id.

In Schaub's affidavit in support of the Ramsey County search warrant he stated that he is a licensed peace officer with 23 years of experience and has specialized training in the investigation of Internet crimes. Id. He knew through his training and experience that the Internet is a common tool for individuals to get sexual gratification either by viewing sexually explicit images involving minors or by interacting with minors. Id. Schaub knew that such individuals use "chat rooms" to contact potential victims, gain their trust, and possibly set up face-to-face meetings. Id. Accordingly, such meetings frequently result in a sexual assault of the minor. Id.

Schaub also stated that computers are frequently used to store child pornography as well as "chat interaction" with children. Id. He expressed familiarity with Yahoo, and similar Internet companies. Id. Schaub knew that Yahoo acts as a host for Internet "chat rooms." Id. He stated that a connection between computers through the Internet can be traced through an Internet Protocol address, which acts in a way analogous to the way a Caller-ID feature works on a telephone system. Id.

Schaub stated that based on his experience and training it is not unusual for victims to deny the occurrence of sexual abuse, particularly when the victim is male. Id. Victims may also be inclined to deny abuse as a result of their relationship with the perpetrator. Id.

Schaub stated that children most likely to become victims in this way have few friends and outside interests, spend an inordinate amount of time on the Internet, have limited social skills in comparison to their peer group, and use the computer as their only outlet to socialization. Id. Schaub asked DL whether that profile would apply to her child, AM. Id. DL responded that it did. Id. She added that AM has bipolar dysfunction, attention deficit, below average grades, and few friends. Id. With the consent of DL, their family computer was inspected and the hard drive was seized for forensic examination. Id. No incriminating evidence was found on the hard drive. Id.

Schaub also explained that, to access services at *www.yahoo.com*, an individual has to provide information to the company, but Schaub knew that individuals often provide false information. Id. From this information, a user profile is created. User profiles are public information that can be accessed by anyone. In checking the profile for

"dlbch15@yahoo.com", Schaub found that it was created by a male individual named Dale, age 26, from Minneapolis, MN; Schaub further discovered that the nickname "dlbch15" was linked to an email address of *dlbch15@prodigy.com*. Schaub sent an administrative subpoena to Prodigy, seeking the subscriber information for *"dlbch15@prodigy.com"*. The subscriber information for that email address identified the defendant, Dale Bach, at 3512 Nicollet Avenue South, Minneapolis, Minnesota, (612) 825-9832. Further investigation revealed that defendant Bach, born December 27, 1958, was a registered sex offender based on a 1996 conviction for criminal sexual conduct in the third degree in Duluth, Minnesota. In that case, Bach plead guilty to having oral and anal sex with a 14-year old boy. See App. at 1-4.

On October 11, 2000, Schaub sent a preservation letter to Yahoo, requesting that Yahoo, "according to their procedures, refrain from removing from their server, or deleting any incoming or outgoing email messages associated with" the email accounts of *dlbch15@yahoo.com* and *bubbagum_7@yahoo.com*. See App. at 7. The *bubbagum_7@yahoo.com* is the Yahoo account for AM, one of the minor victims in this case. Id.

On January 3, 2001, Schaub obtained a state search warrant from the Honorable J. Thomas Mott of the Ramsey County District

Court. The purpose of the Ramsey County warrant was to retrieve from Yahoo emails between the and possible victims of criminal sexual conduct, including but not limited to AM. Id. at _1-3. The Ramsey County warrant also sought the Internet Protocol addresses connected to the 's account. App. at 1-4. Both the warrant itself and Schaub's Affidavit indicated that the warrant would be faxed to Yahoo in compliance with California Statute §1524.2. Schaub faxed the signed warrant to Yahoo. Id. at 1-4.

On January 8, 2001, Schaub received a package from Yahoo which was delivered by DHL Worldwide Express. App. at 6. The package contained one zip disc with all the emails preserved by Yahoo in victim AM's account *bubbagum_7@yahoo.com*, and all the emails preserved in defendant's *dlbch15@yahoo.com*, account, which amounted to five emails retrieved from defendant's "In" box and one email from defendant's "trash", all of which were printed out by Yahoo and sent in hard copy form.[1] Id. According to Yahoo, all information in the two email accounts was downloaded either onto the zip disc or printed out, and sent to Schaub. App. at 22, ¶¶ 13, 14. According to Yahoo, the technicians responsible for compliance with the warrant do not

[1] Only three of the emails found in defendant's account had attachments. Yahoo printed out all six emails and attachments from the account of *dlbch15@yahoo.com* and sent everything to Schaub. Only one of the six emails contained child pornography and was charged in counts 5 and 6 of the Indictment.

selectively choose or review the contents of the named accounts. Id.

Among the six emails recovered from defendant's account was an email dated August 1, 2000 from a minor victim using the screen name of "assbait" ("Victim B"). App. at 31. In that email, the defendant attempted to arrange an in-person meeting with Victim B. Id. Additionally, the information sent to Schaub by Yahoo revealed that "dlbch15" used other identities including "seeknboyz" and "yphx.6128259832." App. at 32. Schaub noted that the phone number, 612-825-9832, belongs to the defendant. Id. The registration material associated with the Yahoo account showed Minneapolis as the city of residence and listed December 27, 1958 as "dlbch15"'s date of birth. Id.

One email in defendant's account was apparently sent to *dlbch15@yahoo.com* and had an attached photograph of a naked boy. See App. at 32. Schaub was familiar with this particular picture, having seen it before while investigating other child pornography cases. Id. The other email messages between "dlbch15" and other individuals discussed "dlbch15" meeting with other individuals and exchanging pictures with them. Id. In some of the email messages, "dlbch15" directs the recipient to visit a particular site to view a picture of "dlbch15". Id. At that site, the individual pictured matches the defendant's driver's license picture. Id. at 31.

In the meantime, Minneapolis Police Sgt. Ann Quinn-Robinson determined from postal authorities that the defendant, Dale Bach, was receiving mail at 3512 Nicollet Avenue South, Minneapolis, MN. See App. at 26-33. On January 26, 2001, Sgt. Quinn-Robinson, obtained a search warrant from Hennepin County Judge Patricia Belois to search the defendant's home. Id. The Hennepin County warrant authorized seizure of computer hard drives, storage devices and other evidence that tended "to show the possession or distribution of child pornography or the enticement of children on line." Id. On January 29, 2001, the Hennepin County warrant was executed at 's residence and among the items seized was defendant's computer, discs and a digital camera. Id. Officers also seized "post-it" notes with names and phone numbers. Id. A forensic search of the defendant's hard drive revealed among other evidence of child pornography, a stored copy of the email from Victim B to defendant, the same email that was part of the materials Yahoo gathered and sent to Schaub in compliance with the Ramsey County Search Warrant.

B. Judge Magnuson's Order

The Government objected to the magistrate's Report and Recommendation ("R&R") which suppressed all evidence obtained from the Ramsey County search warrant. See App. at 8-18. The Honorable Paul A. Magnuson adopted the R&R and, concluded the evidence obtained from the Ramsey County warrant should be

suppressed. Id. The District Court first stated that the execution of the warrant was unreasonable under the Fourth Amendment because Schaub "was not present and acting in the warrant's execution when the Yahoo employees searched and seized information from Bach's Yahoo Account." Id. at 12. According to the District Court, "Schaub's absence rendered this search and seizure unreasonable." Id. The District Court found that § 3105 requires, at least with respect to federal searches, that the executing officer be present and acting in the warrant's execution when a third party is assisting the search, and went on to rule that compliance with § 3105 is part of the reasonableness requirement of the Fourth Amendment. Id. at 13 ("[T]he requirement that an officer be present and acting in a warrant's execution when a third party is assisting the officer helps to effectuate the fundamental Fourth Amendment protection against general searches and seizures."). In support of its holding, the Court stated, in part:

> The circumstances of this case * * * do not justify Schaub's choice to fax the warrant to Yahoo and allow Yahoo employees to conduct the search and seizure without any supervision or instruction. Police officers have taken an oath to uphold federal and state constitutions and are trained to conduct a search lawfully and in accordance with the provisions of the warrant. Civilians, on the other hand, are not subject to any sort of discipline for failure to adhere to the law. In fact, an internet service provider is immune from suit so long as it is providing assistance in accordance with the terms of the warrant. 18 U.S.C. § 2703(e). Without an officer present, this conditional grant of immunity may become

> an irrefutable protection for internet service providers to conduct searches that traverse the clearly defined limits of a warrant. In the particular context of this case, there were no safeguards ensuring that the Yahoo employees conducting the search and seizure of information in Bach's e-mail account were cautiously abiding by the terms of the Ramsey County warrant. Accordingly, the execution of the Ramsey County warrant does not pass constitutional muster.

Id. at 14. The District Court, citing United States v. Moore, 956 F.2d 843, 847-848 (8th Cir. 1992) recognized that although there was no federal involvement in the investigation, Minnesota has a statutory presence requirement similar to § 3105. Id. at 14-16. In that regard, the District Court found that evidence seized by state officers in conformity with the Fourth Amendment should not be suppressed in a subsequent federal prosecution. See United States v. Bieri, 21 F.3d 811, 816 (8th Cir. 1994), cert. denied 513 U.S. 878 (1994). However, the District Court held that suppression was appropriate here because the state officers' conduct violated both federal statutory law and state law. Id. at 15-16.

ARGUMENT

I. SECTION 3105 DOES NOT APPLY TO STATE OFFICERS IN THIS CASE WHERE THERE IS NO FOURTH AMENDMENT VIOLATION.

A. Standard of Review

When there is a question about suppression involving the applicability of a federal statute, the District Court's findings of fact are reviewed for clear error and its application of law is reviewed de novo. See United States v. Maxwell, 25 F.3d 1389, 1395 (8th Cir. 1994), cert. denied. 513 U.S. 1031 (1994); United States v. Schenk, 983 F.2d 876, 879 (8th Cir. 1993) (citing standard of review regarding the application of Fourth Amendment and 18 U.S.C. § 3109).

B. Section 3105 Does Not Apply to Sgt. Schaub's Execution of the Valid Ramsey County State Warrant.

Only the Federal Constitution governs this case, not § 3105 standing on its own. While the District Court focused on the "presence" requirement of § 3105, it has no independent legal significance here because federal statutes only apply to state or local searches when federal agents play a "significant part" in the execution of the state warrant. United States v. Murphy, 69 F.3d 237, 242 (8th Cir. 1995) cert. denied 516 U.S. 1153 (1996). Even the District Court concluded that federal agents played no role in Sgt. Schaub's investigation of this case. Furthermore, while the "presence" requirement of Minn. Stat. §

626.13 closely tracks that of § 3105, the Minnesota statute is not controlling here. Citing United States v. Moore, 956 F.2d 843, 846 (8th Cir. 1992), the District Court held that "state officials must comply with *both* state law and Fourth Amendment search and seizure requirements" to avoid suppression, App. at 9. (emphasis added). This is an erroneous legal conclusion. This Court made clear in Moore that "evidence seized by state officers in conformity with the Fourth Amendment will not be suppressed in a federal prosecution because *state* law was violated." Moore, 956 F.2d at 847 (emphasis in original); accord United States v. Bieri, 21 F.3d 811, 816 (8th Cir. 1994); United States v. Baker, 16 F.3d 854, 856 (8th Cir. 1994) ("[a] police violation of state law does not establish a Fourth Amendment violation.") Therefore, § 3105 is not applicable here because the state officers executed a State Search Warrant. Moreover, the "presence" requirement of § 3105 will not lead to suppression unless there is a constitutional violation. In United States v. Applequist, 145 F.3d 976 (8th Cir. 1998) this Court rejected the argument that a District Court should suppress evidence based on the failure of a state officer to comply with 18 U.S.C. § 3105 and a similar Arkansas state statute.[2] This Court held, "Only the Fourth Amendment governs

[2] The Arkansas statute read: "A search warrant may be executed by any officer. The officer charged with its execution

the suppression of evidence seized by state and local officials." Id. at 978; cf. United States v. Goodson, 165 F.3d 610, 614 (8th Cir. 1999) cert. denied 527 U.S. 1030 (1999)(state warrant executed without federal involvement is not governed or controlled by Federal Rule of Criminal Procedure Rule 41(c)).[3] Thus, the Eighth Circuit has recognized that violations of § 3105 do not amount to per se violations of the Constitution.

Here the District Court rejected Applequist and relied solely on a District Court decision in Ayeni v. C.B.S., Inc., 848 F. Supp. 362 (E.D.N.Y. 1994) for the proposition that § 3105 codifies the Fourth Amendment. App. at 13. Interestingly, Ayeni actually undercuts the lower court's analysis. On appeal, the Second Circuit held that § 3105 "is *not* determinative of the scope of the Fourth Amendment" but rather "provides some basis for giving content to the Amendment's generalized standard of *reasonableness.*" (emphasis added). Ayeni v. Mottola, 35 F.3d 680, 687 (2nd Cir. 1994).[4]

---

may be accompanied by such other officers or persons as may be reasonably necessary for the successful execution of the warrant with all practicable safety." Ark. R. Crim. P. 13.3(a).

[3] In Applequist, this Court also reached a similar conclusion regarding the applicability of 18 U.S.C. § 3109, which requires federal officers to knock and announce their presence prior to executing a search warrant. Applequist, 145 F.3d at 978-79.

[4] The holding of Ayeni v. Mottola, 35 F.3d 680, 687 (2nd Cir. 1994) was abrogated on other grounds by Wilson v. Layne. 526 U.S. 603 (1999). Specifically, the Supreme Court abrogated

II. THE FOURTH AMENDMENT DOES NOT REQUIRE AN OFFICER TO BE PRESENT WHILE AN EMAIL PROVIDER RENDERS TECHNICAL ASSISTANCE IN THE EXECUTION OF A VALID SEARCH WARRANT.

A. Standard of Review

The only matters in controversy here are legal issues. The District Court's conclusions of law are reviewed de novo. United States v. Guevara-Martinez, 262 F.3d 751 (8th Cir. 2001); United States v. Hawkins, 215 F.3d 858, 860 (8th Cir. 2000) cert. denied, 531 U.S. 972 (2000); United States v. Pitts, 173 F.3d 677, 680 (8th Cir. 1999).

B. Yahoo's Technical Assistance was Constitutionally Reasonable and Did Not Require an Officer to Be Present.

The "touchstone of the Fourth Amendment is reasonableness." Ohio v. Robinette, 519 U.S. 33, 39 (1996) quoting Florida v. Jimeno, 500 U.S. 248, 250 (1991); United States v. Alcantar, 271 F.3d 731, 738 (8th Cir. 2001) cert. denied 122 S.Ct. 1380 (2002). The Supreme Court has emphasized that standards of reasonableness are "not susceptible of Procrustean application." Ker v. California, 374 U.S. 23, 37 (1963). Instead, reasonableness is measured in objective terms by examining the totality of the circumstances, without recourse to formulas or bright-line rules. Robinette, 519 U.S. at 39. Each case must be decided contextually, "in recognition of the 'endless

---

the portion of Ayeni that recognized the right to collect money damages against police. Id. at 618.

variations in the facts and circumstances' implicating the Fourth Amendment." Id., quoting Florida v. Royer, 460 U.S. 491, 506 (1983).

The District Court recognized that "the required level of [police] supervision varies depending on the circumstances." See App. at 14, quoting Commonwealth v. Sbordone, 678 N.E.2d 1184, 1189 (Mass. 1997). In this case, the ministerial nature of Yahoo's role meant that Sgt. Schaub's presence and personal supervision would have added nothing. See App. at 22, ¶ 13. When Yahoo receives a search warrant for email account information (usually by fax), it forwards the warrant to its Compliance Group. Id. That group then coordinates with its Technical Group to find and retrieve the requested information. Id. at 22, ¶¶ 11-12. Once the appropriate account is located, Yahoo downloads and forwards to law enforcement all the account information that falls within the time period specified by the warrant. Id. at ¶ 13.

Law enforcement officers such as Schaub, do not have the technical training to participate in or supervise this process. Indeed, if a law enforcement officer were "present" and engaged in retrieving the data, he would not be providing constitutional safeguards, but instead, he "would have to be supervised by Yahoo! personnel to ensure that only the requested information [was] being obtained." Id at ¶ 9. The District Court was concerned that, in the absence of a law enforcement officer, providers like Yahoo "*may* . . . conduct searches that traverse the clearly defined limits of a warrant." See App. at 14.

Nevertheless, the District Court did not cite to any facts showing that Yahoo actually did infringe upon the rights of the defendant. Id. To the contrary, Special Agent Lese submitted an affidavit based on her conversation with Yahoo's general counsel to explain that Yahoo does not exercise discretion when it gathers email account information for law enforcement pursuant to a warrant:

> When accessing a user's information, pursuant to a search warrant, the Yahoo processor does not selectively go through the user's information, but rather gathers all information in an account that is within the time frame specified in the warrant. The processor does not specifically look at the content of the user's account.

App. at 22, ¶ 13.

By taking these actions, Yahoo merely enables law enforcement to conduct a search for electronic evidence off-site where it will not be as onerous or intrusive. See United States v. Horn, 187 F.3d 781, 788 (8th Cir. 1999) cert. denied 529 U.S. 1029 (2000) (upholding the removal of a suspected child pornographer's entire video collection "for examination elsewhere" because officers "could not practically view more than 300 videos at the search site").

Moreover, Yahoo's activities conform to judicial standards governing the proper role of private third parties involved in executing a warrant. Law enforcement generally has broad discretion to determine how best to proceed with a search, Dalia v. United States, 441 U.S. 238, 257 (1979), and third parties

may be called upon if they are needed to "assist the police in their task."[5] Wilson v. Layne, 526 U.S. 603, 611 (1999); Buonocore v. Harris, 65 F.3d 347 (4th Cir. 1995); United States v. Schwimmer, 692 F.Supp. 119 (E.D.N.Y. 1988) (private computer expert may assist officers in a computer search). In this regard, the Court in United States v. Sparks, 265 F.3d 825, 831 (9th Cir. 2001) applied a three-part test that is instructive:

> First, the civilian's role must be to aid the efforts of the police. In other words, civilians cannot be present simply to further their own goals. Second, the officer must be in need of assistance. Police cannot invite civilians to perform searches on a whim; there must be some reason why a law enforcement officer cannot himself conduct the search and some reason to believe that postponing the search until an officer is available might raise a safety risk. Third, the civilians must be limited to doing what the police had authority to do.

Sparks, 265 F.3d, at 831-832 (citations omitted).

Applying this test, the identification and collection of email information by Yahoo's staff was reasonable. First, Yahoo's technical staff searched the company's database solely to assist a police investigation. Second, only Yahoo technical staff could perform the database search to retrieve the data sought under the warrant and to prevent the violation of the privacy rights of innocent third parties. See App. at 21-24, ¶¶ 9, 17.a. Finally, Yahoo only gathered data related to the

[5] The District Court acknowledged that the warrant "was not rendered unreasonable by the mere assistance of Yahoo employees." See App. at 9.

account holder and the time frame specified in the warrant. Id. at 22, ¶ 13. Thus, Yahoo's actions were constitutionally reasonable because they were properly limited to aid Sgt. Schaub's investigation.[6]

C. It Would Be Unreasonable to Require a Police Officer to Be Present While an Email Provider Renders Technical Assistance in the Execution of a Valid Search Warrant.

---

[6] In fact, a separate basis for reversing the District Court's decision exists because the search and seizure did not take place at Yahoo at all. Rather, the search occurred later, on January 8, 2001 in St. Paul, Minnesota when Sgt. Schaub received the data from Yahoo and examined it for evidence of criminal activity. United States v. Jacobsen, 466 U.S. 109, 113, 120 (1984)).

Additionally, by signing up as a Yahoo customer, the defendant agreed to the following Terms of Service ("TOS"), App. at 21, Aff. ¶ 15:

> You acknowledge and agree that Yahoo may preserve Content and may also disclose Content if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary to: (a) comply with legal process; (b) enforce the TOS; (c) respond to claims that any Content violates the rights of third-parties; or (d) protect the rights, property, or personal safety of Yahoo, its users and the public.

Thus, the defendant had no reasonable expectation that Yahoo would refrain from collecting or forwarding his email account data in order to comply with a search warrant, or to protect Yahoo's private contract rights and the interest of its customers. See United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) cert. denied 122 S.Ct. 292 (2001) (finding no reasonable expectation of privacy in employee's computer where employer had policy stating it would "audit, inspect, and/or monitor" employees' Internet use).

As a result, because the "Search and Seizure" did not occur until Sgt. Schaub took control of the data, the execution of the warrant complied with § 3105, and no statutory or constitutional violations occurred.

The Supreme Court has stated, "The Fourth Amendment's flexible requirement of reasonableness should not be read to mandate a rigid rule of announcement that ignores countervailing law enforcement interests." Wilson v. Arkansas, 514 U.S. 927, 934 (1995). Law enforcement must move quickly to collect and preserve electronic evidence in Internet cases. The difficulty of this task is compounded by the fact that such evidence can be voluminous, intermingled with irrelevant data, and "vulnerable to tampering or destruction." United States v. Walser, 275 F.3d 981, 985 (10th Cir. 2001), citing United States v. Henson,848 F.2d 1374, 1383-84 (6th Cir. 1988); United States v. Tamura, 694 F.2d 591, 597 (9th Cir. 1982); and United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000). Requiring an officer to be present at all phases of email searches would make investigations impossible and impractical, slow and expensive, and overly intrusive. Such a requirement would hamper not only investigations into child exploitation, as alleged in this case, but also investigations into other types of crime that commonly involve the use of computers, including Internet fraud, hacking, software piracy, cyberstalking, threats against the President, and international terrorism.

In many cases it would be literally ***impossible*** for a law enforcement officer to be physically present within a service provider's facility for all aspects of a search, especially if

he/she is seeking different types of account information. The contents of an email message may be accessible only by a few high-level administrators at headquarters, while Internet Protocol numbers and other types of connection information may be available only through systems managers at several remote locations, and subscriber or billing information may only be stored at the customer service center. Where, then, are officers supposed to go in order to be "present" for purposes of § 3105?

Trying to coordinate the identification and collection of each piece of email data, so that it occurs in the officer's "presence" would require an enormous amount of time and money.[7] Even assuming that an email provider could access all of its account information from one location at one time, a rigid application of § 3105 would impose significant costs for training, travel and time on law enforcement, especially state or local police. An officer like Sgt. Schaub would have to find a State law enforcement officer in California to serve and "be present" for the execution of the warrant, or Schaub would have to travel to Silicon Valley whenever he needed evidence related to a Yahoo email address.

[7] Agent Lese points out that electronic search warrants are time-consuming even without rigid "presence" requirements. In a recent search warrant, a large institution took two months to comply with the warrant completely. App. at 23, ¶ 17.a.

Besides increasing the time and expense for law enforcement, the District Court's ruling would impose unreasonable burdens on private third parties – service providers like Yahoo and their customers or subscribers. Yahoo would have to endure five to ten disruptions by law enforcement every week. App. at 21-22, ¶ 8; see United States v. Schandl, 947 F.2d 462, 465 (11th Cir. 1991) cert. denied 504 U.S. 975 (1992) (noting that an on-site search for electronic evidence "might [be] far more disruptive" than an off-site examination). An ever-present officer would also trigger new "privacy issues and legal concerns" for the company. App. at 21-22, ¶ 9. The Electronic Communications Privacy Act ("ECPA") is supposed to protect consumers' privacy by prohibiting providers from disclosing account information to the government in the absence of legal process. 18 U.S.C. §§ 2703(a)-(d). Yet Yahoo could face liability under the same act any time a "shoulder surfing" officer saw an account not specified in his warrant.

Thus, a strict application of the "presence" requirement in § 3105 would undermine the very privacy rights that the District Court hoped to preserve. Not only would a rigid "presence" requirement be impractical and burdensome, it would be invasive and constitutionally unreasonable under the facts in this case.

C. Yahoo and Sgt. Schaub's Actions were Reasonable in Light of Section 3105's Limited Application to Searches for Electronic Evidence.

The Court should consider the special circumstances posed by the nature of the evidence collected in this case. As the 10th Circuit recently stated in Walser, 275 F.3d at 986:

> The advent of the electronic age and, as we see in this case, the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law. . . . This does not, of course, mean that the Fourth Amendment does not apply to computers and cyberspace. Rather, we must acknowledge the key differences and proceed accordingly.

In the present case, the administrative nature of Yahoo's activity means that a rigid application of Section 3105 is not appropriate. Both the Third and Ninth Circuits considered Section 3105 in the context of early telephonic "trap and trace" orders, issued under Fed. R. Crim. Prod. 41, which required telephone companies to install a device to capture incoming numbers to a target's telephone. In both cases, the Circuit courts explicitly rejected the notion that an officer must be present while a private third party carries out the technical aspects of a search. In In re Application of the United States for an Order Authorizing the Installation of a Pen Register or Touch-Tone Decoder and Terminating Trap, Bell Telephone Co. of Pennsylvania, 610 F.2d 1148, 1154 (3rd Cir. 1979)[hereinafter "Pennsylvania Bell"], the District Court had issued a trap and

trace order under Rule 41, but the telephone company asserted that the order violated Section 3105 and Rule 41(c)(1) requiring that a warrant be directed at a law enforcement officer. The Third Circuit rejected this argument and held that these provisions merely set forth a rule "denying ordinary citizens and corporations the authority to execute search warrants" on their own. Id. Because law enforcement officers were ultimately responsible for the execution of trap and trace orders, the court found there were no problems "associated with private exercise of search and seizure powers. . . ." Id.

The Ninth Circuit adopted the same reasoning in In re Application of the United States for an Order Authorizing an In-Progress Trace of Wire Communications Over Telephone Facilities, United States v. Mountain States Telephone & Telegraph Co., 616 F.2d 1122 (9th Cir. 1980)[hereinafter "Mountain Bell"]. Objecting to a "trap and trace" order issued pursuant to Rule 41, the appellant argued that the order was "fatally defective" under § 3105 because it "placed the entire responsibility for the search on Mountain Bell" rather than on federal agents. Id. at 1130. The Ninth Circuit rejected this challenge, noting that appellant had raised "a distinction without a difference." Id. It held:

> [T]he actions ordered were technical ones which only that company could perform. . . . Throughout the operation, the agents remained solely responsible for

> the use to be made of the information obtained. Under such circumstances there was no abuse of either Rule 41 or 18 U.S.C. § 3105. . . .[T]he requirement that warrants be served only by law enforcement officers contemplates the traditional situation in which the pursuit of tangible property takes place through means of a physical search of persons or places. But the use of electronic surveillance, such as pen registers and traces, is to a large extent sui generis: no warrant is "served," no persons or premises are "searched," no confrontation between the government and citizen takes place; rather a computer is programmed to detect electronic impulses which, when decoded, provide a list of telephone numbers. Once it is determined that such an operation is constitutionally permissible. . . . it appears to this court to make little difference whether, as with pen registers, federal agents install the device and then monitor it themselves, or as in the case of traces using ESS facilities, telephone company technicians acting at the behest of federal officials perform these functions.

Id. at 1130 (footnotes and citations omitted).

Similarly in the instant case, there was no physical confrontation between law enforcement agents and a private person. Collecting the information covered by the warrant involved technical computer queries that targeted the accounts and time period specified by the search warrant. App. at 22, ¶ 13. Once the data was recovered, Sgt. Schaub was solely responsible for examining and using the information obtained. Thus, under Pennsylvania Bell and Mountain Bell, no violation of § 3105 occurred, and the execution of the warrant was reasonable.

E. Yahoo and Sgt. Schaub Followed Section 2703 of the ECPA, Which Protects Individual Privacy and Sets Forth

Procedures That Are Reasonable in Searches for Electronic Evidence.

When conducting the search for electronic evidence, Sgt. Schaub followed the procedures of the Electronic Communications Privacy Act ("the ECPA"), as codified under 18 U.S.C. § 2703. This was appropriate for two reasons. First, this statute is more recent and applicable to electronic searches, and under basic rules of statutory construction, § 2703 should govern this Internet case rather than § 3105. Second, in constitutional terms, § 2703 provides a reasonable set of procedures to follow when conducting a search of an individual's email account.

This Circuit has recently held, "It is a familiar principle of statutory construction that a general statute must yield when there is a specific statute involving the same subject matter." Craighead Elec. Co-op Corp. v. City Water and Light Plant of Jonesboro, 278 F.3d 859, 861(8th Cir. 2002). The Supreme Court has similarly stated, "[An earlier statute's] generalities should not lightly be construed to frustrate a specific policy embodied in a later federal statute." United States v. Estate of Romani, 523 U.S. 517, 530, (1998) quoting Massachusetts v. United States, 333 U.S. 611, 635, (1948) (Justice Jackson's dissent). This means that a strict application of the older

general statute, 18 U.S.C. § 3105, should not undermine the intent and purpose of the newer more specific procedures outlined in 18 U.S.C § 2703 of the ECPA.

The basic provisions of § 3105 date back eighty-four years and were passed as part of the Espionage Act of 1917. Section 7 of Title XI of the Act read, "A search warrant may in all cases be served by any of the officers mentioned in its direction, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution." See H.R. Conf. Rep. No. 65-65 at 14 (1917). This section was one of several set forth under the general heading "Search Warrants" and codified under 18 U.S.C. former § 611, *et seq*. (1940 ed.) Many of these provisions were eventually incorporated into Rule 41 of the Federal Rules of Criminal Procedure. See Fed. R. Crim. P. 41, Advisory Committee Notes, "1944 Adoption, Notes to Subdivisions (a)-(g)." Section 7 of the Espionage Act remained a separate statute and was re-codified in 1948 under § 3105 of Title 18. The only revision to the statute occurred at that time, and made clear that a warrant could be served by any "officer authorized by law to serve such warrant." See 18 U.S.C. § 3105; H.R. Report 80-304.

While § 3105 is a decades-old law of general applicability, § 2703 is a newer statute that more specifically addresses

privacy in the burgeoning field of electronic communications. When Senator Leahy introduced the ECPA, he did so because existing law was "hopelessly out of date." S. Rep. 99-541 at 2 (1986), reprinted in 1986 U.S.C.C.A.N. 3555. The Senate Judiciary Committee echoed this sentiment: "[The law] has not kept pace with the development of communications and computer technology. Nor has it kept pace with changes in the structure of the telecommunications industry." Id. at 3. Congress also spoke to the particular need to protect stored electronic data, like the contents of the email that are at issue in this case. The Senate Report stated,

> The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized record keeping systems, Americans have lost the ability to lock away a great deal of personal and business information.

Id. As a result of these concerns, Congress passed the ECPA, including § 2703, with the specific intent "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." Id.

Based on these facts, Congress has spoken more recently and directly to the issues at hand through the ECPA and § 2703. More importantly, Congress has set forth specific

procedures in § 2703 that are constitutionally reasonable.

First, § 2703 protects the privacy of electronic records and requires the government to obtain a search warrant based on probable cause if it wants to obtain the contents of email communications without giving notice to a target. 18 U.S.C. § 2703(a)-(b)(2001).[8] Section 2703 also specifies the legal process the government must use to obtain email messages with notice, or other information such as technical or transactional records (e.g. server logs), and subscriber information. See 18 U.S.C. § 2703(a)-(d) (2001). Section 2703 further provides for the preservation of electronic records and gives immunity to providers who comply with the statute. See 18 U.S.C. § 2703(e)-(f) (2001).

Whereas § 3105 "contemplates the traditional situation in which the pursuit of tangible property takes place through means of a physical search of persons or places," Mountain Bell, 616 F.2d at 1130, by passing § 2703 Congress

[8] This brief cites to § 2703 as enacted in 2001 when the search of defendant's records was conducted. Under the USA Patriot Act, Congress recently renumbered subsections, revised § 2703 to cover voice mail, and expanded the government's subpoena power.

recognized that an electronic search and seizure is entirely different. It seldom involves a face-to-face confrontation and often requires the use of highly trained technicians to collect off-site evidence from a variety of computers.

In light of these differences, the ECPA contemplates that an "electronic communication service provider," like Yahoo, will "disclose" or deliver electronic data to law enforcement, not that a law enforcement officer will enter and physically take control of a company's computer system.[9] In this way, the ECPA treats a search warrant for email records more like a subpoena or a search warrant served on a bank, hospital, law firm, or another third party with

[9] See 18 U.S.C. 2703(a)("A government entity may require disclosure by a provider of electronic communication service of the contents of an electronic communication ... in storage" pursuant to a warrant); 2703(b) ("A governmental entity may require a provider of remote computer service to disclose . . . contents" pursuant to a proper warrant, order or subpoena); 2703(c)(1)(A) ("a provider . .. may disclose a [non-content] record" to a private party); 2703(c)(1)(B) ("a provider . . . shall disclose a [non-content] record. . . to a governmental entity" pursuant to a warrant or court order); 2704(a)(3)(A) (requiring providers to retain backup data until "delivery of the information"); 2704(a)(4)(stating a "service provider shall release such backup copy to the requesting governmental entity" after proper notice of an order or subpoena); 2706 (allowing providers to be reimbursed for costs incurred in "searching for, assembling, reproducing, or otherwise providing such information").

sensitive client information.

For example, in a case analogous to this one, Washington v. Kern, 914 P.2d 114, 117-18 (Wa. Ct. App. 1996), the Court upheld a search for bank records where the police officer handed the warrant to bank employees with instructions to deliver the specified records later. The court explained that the officer's presence was not required while the bank records were being gathered because "[a] police officer will not ordinarily perform a search of a bank's records, indeed may not be qualified to do so". Id.

This example shows that an officer's presence may not be necessary or proper when a warrant is served on a third party that holds numerous sensitive records. This example also underscores the balanced approach taken by the ECPA and § 2703. Section 2703 properly allows the government to obtain certain email messages without notice if it secures a search warrant based on probable cause. At the same time, the statute protects the interests of the email provider and its other customers by allowing disclosure of evidence in lieu of a direct seizure.

In short, the provisions of § 2703 are recent, specific and reasonable to apply in an Internet case like this one.

Because Sgt. Schaub and Yahoo followed § 2703 closely, their actions were reasonable and not in violation of defendant's Fourth Amendment rights.

III. Blanket Suppression of All Evidence Obtained From The Ramsey County Warrant is Improper Because Defendant Lacks Standing to Challenge the Victim's Email Account.

A. Standard of Review

Whether the defendant has standing to challenge certain evidence is a question of law that should be reviewed de novo. United States v. Hayes, 120 F.3d 739, 743 (8th Cir. 1997). Although the government did not object on the basis of standing at the District Court level, the argument has not been waived. See United States v. Rodriguez 270 F.3d 611, 616-17 (8th Cir. 2001). "[I]t is elementary that standing relates to the justiciability of a case and cannot be waived by the parties." Sierra Club v. Robertson, 28 F.3d 753, 757 n. 4 (8th Cir. 1994), quoted in Rodriguez, 270 F.3d at 617.

B. Defendant has No Standing To Challenge the Search and Seizure of Another Person's Email Account.

The District Court not only erred when it ruled that an officer should have been present when Yahoo gathered account information, but it also erred when it imposed blanket suppression as the remedy in this case. See App. at 8-17. Sgt. Schaub requested that Yahoo produce data related to defendant's email account, *dlbch15@yahoo.com,* as well as AM's email account *bubbagum_7@yahoo.com*. Id. at 1-

3. Yet, the defendant has no standing to challenge any evidence seized from the *bubbagum7@yahoo.com* account. To establish standing, the defendant has the burden of demonstrating that he has a reasonable expectation of privacy in the area searched. United States v. Gomez, 16 F.3d 254, 256 (8th Cir. 1994). The "factors relevant to the determination of standing include; "ownership, possession and/or control of the area searched or item seized; historical use of the property or item; [and] ability to regulate access" to the area searched. Id. Since victim AM owned, controlled, and used *bubbagum_7@yahoo.com,* the defendant did not, and cannot establish standing as to that email account, and any evidence seized from it should not be suppressed.

CONCLUSION

Based on the foregoing facts and argument, the District Court's memorandum and order for suppression should be reversed.

CERTIFICATE OF COMPLIANCE

The undersigned attorney for the United States certifies this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32. The brief has 1229 lines of monospaced type. The brief was prepared using WordPerfect 8. The undersigned attorney also certifies that the computer diskette containing the full text of the Brief of Appellee has been scanned for viruses and to the best of our ability and technology, believes it is virus-free.

Dated: May 6, 2002

Respectfully submitted,

THOMAS B. HEFFELFINGER
United States Attorney

BY: BRIDGID E. DOWDAL
PAUL H. LUEHR
Assistant U.S. Attorney's
600 U.S. Courthouse
300 South Fourth Street
Minneapolis, MN 55415
Attorneys for Appellee

ADDENDUM OF APPELLEE