518 F.3d 1196

UNITED STATES of America, Plaintiff-Appellee,
v.
Steven C. PERRINE, Defendant-Appellant.

No. 06-3336.

United States Court of Appeals, Tenth Circuit.

March 11, 2008.

[518 F.3d 1199]

Kristen B. Patty, Wichita, Kansas (Philip R. White, Ariagno, Kerns, Mank & White, LLC, Wichita, Kansas, with her on the brief) for Defendant-Appellant.

Brent I. Anderson, Assistant United States Attorney, Wichita, Kansas (Eric F. Melgren, United States Attorney, Wichita, Kansas, with him on the brief) for Plaintiff-Appellee.

Before TACHA, ANDERSON, and GORSUCH, Circuit Judges.

ANDERSON, Circuit Judge.

Defendant and appellant Steven C. Perrine appeals the denial of his motion to suppress evidence following his conviction by a jury on three counts relating to the distribution, receipt and/or possession of child pornography, one count of possession of a firearm by a convicted felon, and two counts of criminal forfeiture. He also appeals the denial of his motion to dismiss the case against him, on the ground that governmental authorities engaged in outrageous conduct. We affirm.

BACKGROUND

On September 2, 2005, James Vanlandingham reported to local police that, while in a Yahoo! chat room and while using the screen name "dana_hotlips05," he began chatting with a person with the screen name "stevedragonslayer." "stevedragonslayer" invited Vanlandingham/"dana_hotlips05" to watch a web cam video depicting two nude six-to-nine-year-old girls. While waiting for the police to arrive, Vanlandingham stayed on the line with "stevedragonslayer" and continued to chat. Vanlandingham asked if "stevedragonslayer" had any more videos, to which "stevedragonslayer" replied he did not know what might offend "dana_hotlips05." After Vanlandingham informed "stevedragonslayer" that he liked "the young hard stuff," "stevedragonslayer" played several videos depicting young girls in various explicit sexual acts.

"stevedragonslayer" stopped sending video clips to "dana_hotlips05" prior to the arrival of police officers at Vanlandingham's house, but Vanlandingham was able to preserve a copy of the chat room conversation. One of the Pennsylvania law enforcement authorities interviewed Vanlandingham and viewed the saved chat room conversation.

Based upon Vanlandingham's account of these events, Pennsylvania law enforcement personnel obtained a disclosure order dated October 14, 2005, pursuant to 18 U.S.C. § 2703(d) and 18 Pa.C.S.A. § 5743(d), [1] directing Yahoo! to provide the subscriber information for the screen name "stevedragonslayer." Yahoo!'s records indicated that "stevedragonslayer" logged on to the Yahoo! website from the IP address 68.103.177.146 on October 9, 2005, October 22, 2005, October 29, 2005, October 30, 2005, November 1, 2005, and November 6, 2005. [2]

Further investigation revealed that this IP address was maintained by Cox Communications, Inc. Pennsylvania authorities obtained another disclosure order requiring Cox to provide the

subscriber information for that IP address. Cox reported that the Yahoo! logins from this particular IP address at the times reported by Yahoo!

[518 F.3d 1200]

were associated with an account belonging to Steve Perrine, 11944 Rolling Hills Court, Wichita, Kansas.

Pennsylvania authorities then contacted Kansas authorities, who discovered that Steve Perrine had a prior state conviction for sexual exploitation of a child, for which he was still on probation. Wichita police obtained a search warrant for Perrine's house, which was executed on December 22, 2005. In addition to seizing Perrine's computer, the police also found firearms and drug paraphernalia. They accordingly amended the search warrant to authorize seizure of those items as well. A forensic examination of Perrine's computer revealed thousands of images of child pornography.

On February 7, 2006, Perrine was charged in a superceding indictment with one count of distributing child pornography, in violation of 18 U.S.C. § 2252(a)(2); one count of receiving child pornography, in violation of 18 U.S.C. § 2252(a)(2); one count of possessing child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B); one count of being a felon in possession of a firearm, in violation of 18 U.S.C. §§ 922(g)(1) and 924(a)(2); and two counts of forfeiture. Among other motions, Perrine filed a motion to suppress and a motion to dismiss based upon outrageous government conduct.

The district court held a motions hearing, at which Perrine testified that he was "stevedragonslayer." Perrine further testified that he had enabled peer-to-peer file sharing on his computer, thereby giving anyone with internet access and certain software the ability to gain entrance to certain files on his computer. After subsequent briefing, the district court denied Perrine's motions.

The case proceeded to a jury trial. A Wichita Police Department Computer Forensics detective, Detective Stone, testified that he found in excess of 16,000 images of child pornography on Perrine's computer. Detective Stone also found Kazaa, a peer-to-peer file sharing program, installed on Perrine's computer. Stone further testified that Kazaa is a program which allows individual users like Perrine to identify folders that are available to share with others, search other computers with Kazaa for specific topics, and download files from other computers, while allowing other computers to download files from Perrine's computer. [3]

Additionally, Annie Cheung, the senior compliance paralegal at Yahoo!, testified that Yahoo! tracks dates, times, and IP addresses for log-in attempts on a Yahoo! account and maintains that information for approximately thirty days. She further

[518 F.3d 1201]

testified that Yahoo! records showed that the IP addresses 68.103.177.226 and 68.103.177.146 belonged to "stevedragonslayer."

Perla Rodriguez, the Cox Communications Customer Escalations Coordinator, testified that residential account IP addresses can change because they are leased for twenty-four hours at a time. Cox Communications residential account IP addresses release and renew every twenty-four hours; when an IP address releases, if the same IP address is available, it reattaches within a few seconds. Rodriguez further testified that only one IP address is assigned to a user at a time and that it is the customer's address on the internet when he or she is online. She stated that the IP address 68.103.177.146 was used by Perrine. Perrine was convicted on all counts.

Perrine thereafter filed a motion for a new trial, a motion for a judgment of acquittal, and a motion for arrest of judgment. After denying the motions, the district court sentenced Perrine to 235 months' imprisonment, to be followed by supervised release for life. Perrine appeals, arguing

(1) the district court erred in failing to suppress evidence obtained against him in violation of the Fourth Amendment and/or 18 U.S.C. § 2703(d) and 18 Pa.C.S.A. § 5743(d); and (2) the district court erred in failing to dismiss the case against Perrine due to outrageous government conduct.

DISCUSSION

Perrine appeals the denial of his motion to suppress. "When reviewing a district court's denial of a motion to suppress, we review the district court's factual findings for clear error and consider the evidence in the light most favorable to the Government." *United States v. Zamudio-Carrillo,* 499 F.3d 1206 , 1209 (10th Cir. 2007). Further, "[d]eterminations relating to the sufficiency of a search warrant and the applicability of the good-faith exception are conclusions of law, . . . which this court reviews *de novo."* *United States v. Danhauer,* 229 F.3d 1002 , 1005 (10th Cir.2000). Finally, while we review the district court's ruling on the sufficiency of a search warrant de novo, we do not review de novo the determination of probable cause by the issuing judge or magistrate. Rather, a state judge's "decision to issue a warrant is entitled to great deference," and we "need only ask whether, under the totality of the circumstances presented in the affidavit, the [state] judge had a `substantial basis' for determining that probable cause existed." *United States v. Artez,* 389 F.3d 1106 , 1111 (10th Cir.2004) (further quotations and citations omitted).

We first consider Perrine's argument that evidence was seized in violation of the ECPA and its state law equivalent, as well as the Fourth Amendment.

I. ECPA/State Law and Fourth Amendment

Perrine argues that compliance with 18 U.S.C. § 2703(d) and 18 Pa.C.S.A. § 5743(d) is "akin to a *Terry* stop within the scope of the Fourth Amendment and suppression is available to remedy violations." Appellant's Br. at 7. Section 2703 is the core provision of the ECPA, and it authorizes the government to require disclosure of stored communications and transaction records by third-party service providers. Under 18 U.S.C. § 2703(c)(2), "[a] provider of electronic communication service or remote computing service shall disclose to a governmental entity the . . . name; . . . address; . . . telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address . . . of a subscriber to or customer of such service. . . ." 18 U.S.C. § 2703(c)(2). Section 2703(d) specifies that "[a] court order for disclosure

[518 F.3d 1202]

under subsection . . . (c) . . . shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought[ ] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). [4]

Perrine argues that suppression, an appropriate remedy for an impermissible *Terry* stop, [5] is an available remedy for a violation of the ECPA. However, section 2708 of the ECPA specifically states that "[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. Section 2707, in turn, describes remedies for violations of the Act as including civil actions for violators other than the United States and administrative discipline against federal employees in certain circumstances. 18 U.S.C. § 2707. Thus, violations of the ECPA do not warrant exclusion of evidence. *See United States v. Steiger,* 318 F.3d 1039 , 1049 (11th Cir. 2003); *United States v. Smith,* 155 F.3d 1051 , 1056 (9th Cir.1998); *Bansal v. Russ,* 513 F.Supp.2d 264 , 282-83 (E.D.Pa.2007); *United States v. Sherr,* 400 F.Supp.2d 843 , 848 (D.Md.2005); *United States v. Kennedy,* 81 F.Supp.2d 1103 , 1110 (D.Kan.2000). [6]

Perrine next argues that, in any event, the government violated the ECPA and the Pennsylvania law by failing to present "specific and articulable" facts in support of its applications for court orders requiring Yahoo! and Cox to reveal Perrine's IP address and name,

and that the government therefore used illegally obtained information in support of its search warrants. We disagree. As Perrine notes, the "specific and articulable facts" standard derives from the Supreme Court's decision in *Terry.* Thus, we are familiar with the standard imposed.

Perrine argues the government's affidavit in support of its application for an order failed to provide specific and articulable facts because it did not attach a copy of the "chat" between "stevedragonslayer" and Vanlandingham; it did not contain anything specifically indicating that Vanlandingham was a truthful and reliable person; and it failed to show that "stevedragonslayer" was logged on to Yahoo! on the date of the crime, September 2, 2005, at 2 p.m. The affidavit attached to the October 14, 2005, application for a disclosure order for Yahoo! stated as follows:

Officer Humbert received information from Leetsdale Police Officer Wayne Drish indicating that a resident of his jurisdiction had received what appeared to be child pornography via his computer while in a Yahoo! Inc messaging chat room.

Officer Humbert interviewed the resident, James Vanlandingham, and learned that he was logged into Yahoo Messaging Chat on September 2, 2005 at approximately 2:00 PM EDT. He received a message from an individual logged in Yahoo Messaging Chat as "stevedragonslayer." This individual invited James Vanlandingham to view his web cam. When James Vanlandingham viewed the cam he was presented with images of a young female he describes as between 6 and 9 years of age performing

[518 F.3d 1203]

oral sex on an adult male, images of a young female he describes as between 6 and 9 years of age having oral sex performed on her by an adult female and images of two young females he describes as between 6 and 9 years of age walking around in a bathroom unclothed. James Vanlandingham immediately reported the incident to law enforcement. I did view that chat log of this session between James Vanlandingham and "stevedragonslayer."

Appellant's App. at 72, attach. D. The affidavit attached to the December 8, 2005, application for a disclosure order for Cox recited the same information as above, and added at the bottom:

On 11/22/05 I received a response from Yahoo! Inc. which provided the IP login address of 68.103.177.146 for the screenname "stevedragonslayer" on 10/09/05, 10/22/05, 10/29/05, 10/30/05, 11/01/05, and 11/06/05.

Appellant's App. at 83: attach. E.

The statutory standard requires that "the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The affidavits above satisfy that standard. There is no reason to doubt Vanlandingham's account of what happened; indeed, he immediately contacted the police, which suggests he was simply a concerned citizen. Further, the officer stated that he had personally read the chat log between Vanlandingham and "stevedragonslayer." The details provided are specific and certainly would lead to a reasonable suspicion that "stevedragonslayer" was involved in child pornography.

Perrine also alleges that the application for the order was deficient because it failed to show that "stevedragonslayer" was on line with Vanlandingham on September 2, 2005, at 2 PM. The district court dismissed this as "of no moment" because Yahoo!'s logs simply did not go back that far. As indicated above, Yahoo! employee Annie Cheung testified that Yahoo! tracks dates, times, and IP addresses for login attempts on a Yahoo! account and maintains that information for approximately thirty days. Both Cheung's testimony and the actual document turned over by Yahoo! to law enforcement pursuant to the court's order revealed that "stevedragonslayer" had IP addresses of both 68.103.177.226 and 68.103.177.146. Appellant's App. at 129-30. Yahoo!'s

records also revealed that "stevedragonslayer" with IP address 68.103.177.146 had logged on to Yahoo! a number of times in October and November 2005.

We agree with the district court that the absence of a specific record of "stevedragonslayer" with IP address 68.103.177.226 or 68.103.177.146 being logged on at 2 PM on September 2, 2005, does not undermine the adequacy of the affidavit. The reason for that absence is simply that Yahoo! fails to maintain records for more than thirty days. Perrine admitted he was "stevedragonslayer" and gives no explanation for who else could have been logged on to Yahoo! on September 2, 2005, with the name "stevedragonslayer," when every other login for "stevedragonslayer" matches the IP address of Perrine's computer. [7] In sum, we conclude that the affidavits

[518 F.3d 1204]

submitted in the application for an order under the ECPA and the Pennsylvania statute contained "specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought[ ][ ][is] relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d); 18 Pa.C.S.A. § 5743(d).

Perrine also appears to make a broader Fourth Amendment challenge to the government's acquisition of his subscriber information from Yahoo! and Cox. The district court held:

the identifying information at issue here — defendant's name, address, etc. — was information that he voluntarily transmitted to the third-party internet providers, Cox and Yahoo!. Indeed, defendant also admitted at the hearing that he had enabled peer-to-peer file sharing on his computer, thereby giving anyone with internet access the ability to gain entrance to his computer. Under such a scenario, a defendant holds no reasonable expectation of privacy that the Fourth Amendment will protect.

Mem. and Order at 16, Appellant's App. at 149. We agree with the district court.

Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation. *See, e.g., Guest v. Leis,* 255 F.3d 325 , 336 (6th Cir.2001) (holding, in a non-criminal context, that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person-the system operator"); *United States v. Hambrick,* 225 F.3d 656 (4th Cir.2000) (unpublished), affirming *United States v. Hambrick,* 55 F.Supp.2d 504 , 508-09 (W.D.Va.1999) (holding that there was no legitimate expectation of privacy in noncontent customer information provided to an internet service provider by one of its customers); *United States v. D'Andrea,* 497 F.Supp.2d 117 , 120 (D.Mass.2007) ("The *Smith* line of cases has led federal courts to uniformly conclude that internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access."); *Freedman v. America Online, Inc.,* 412 F.Supp.2d 174 , 181 (D.Conn.2005) ("In the cases in which the issue has been considered, courts have universally found that, for purposes of the Fourth Amendment, a subscriber does not maintain a reasonable expectation of privacy with respect to his subscriber information."); *United States v. Sherr,* 400 F.Supp.2d 843 , 848 (D.Md.2005) ("The courts that have already addressed this issue . . . uniformly have found that individuals have no Fourth Amendment privacy interest in subscriber information given to an ISP."); *United States v. Cox,* 190 F.Supp.2d 330 , 332 (N.D.N.Y.2002) (same); *United States v. Kennedy,* 81 F.Supp.2d 1103 , 1110 (D.Kan.2000) ("Defendant's constitutional rights were not violated when [internet provider] divulged his subscriber information to the government. Defendant has not demonstrated an objectively reasonable legitimate expectation of privacy in his subscriber information."). *Cf. United States v. Forrester,* 512 F.3d 500 , 510 (9th Cir.2008) ("e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet

[518 F.3d 1205]

service providers for the specific purpose of directing the routing of information."); *United States v. Lifshitz*, 369 F.3d 173 , 190 (2d Cir.2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers. . . . They may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient.").

Furthermore, as Perrine conceded, he had peer-to-peer software on his computer, which permitted anyone else on the internet to access at least certain folders in his computer. To the extent such access could expose his subscriber information to outsiders, that additionally vitiates any expectation of privacy he might have in his computer and its contents. Thus, Perrine has no Fourth Amendment privacy expectation in the subscriber information he gave to Yahoo! and Cox.

II. Search of His House

Perrine also challenges the search of his house. In particular, he argues "[t]he affidavits in support of the search warrants do not establish probable cause as the facts revealed therein were not particularized as to [Perrine], contained stale information of alleged criminal activity relating to [Perrine], and materially omitted facts vitiating probable cause." Appellant's Br. at 22.

"[P]robable cause exists where attending circumstances `would lead a prudent person to believe there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Cantu*, 405 F.3d 1173 , 1176 (10th Cir.2005) (quoting *United States v. Basham*, 268 F.3d 1199 , 1203 (10th Cir.2001)). In assessing whether there is probable cause for a warrant, "we assess the sufficiency of a supporting affidavit based on the totality of the circumstances." *Id.* Further, a magistrate's or judge's determination that a warrant is supported by probable cause is entitled to "great deference." *Id.* On review, our task is to "ensur[e] `that the magistrate had a substantial basis for concluding probable cause existed.'" *United States v. Tisdale*, 248 F.3d 964 , 970 (10th Cir.2001) (quoting *Illinois v. Gates*, **462 U. S. Reports 213** , 238-39, 103 S.Ct. 2317 , 76 L.Ed.2d 527 (1983)).

The affidavits in support of the search warrants in this case provided sufficient information for the judge to conclude that probable cause existed. They recited essentially the same facts as in the applications for the disclosure orders, quoted above, with the addition of a description of the information obtained from Yahoo! and Cox, which identified Perrine as "stevedragonslayer." They also recited the fact that Wichita police officer Shawn Bostick, after further investigation of Perrine/"stevedragonslayer," discovered that he had been previously convicted in Kansas state court of exploitation of a child, was still on probation for that offense, and that the prior case involved Perrine sending images of child pornography and showing videos containing child pornography via Yahoo! Messenger using a web cam.

Perrine argues they were not "particularized to" him, Appellant's Br. at 22, because they did not state that Yahoo!'s records showed that "stevedragonslayer" was in fact logged on to Yahoo! on September 2, 2005. For the same reasons we found that this omission did not undermine the sufficiency of the applications for the disclosure orders, we find it does not undermine the sufficiency of the affidavits in support of the search warrants.

Perrine next argues that the affidavits contained stale information. Perrine asserts that 111 days had passed between the chat between "stevedragonslayer" and Vanlandingham and the submission of the affidavits. Whether information is stale depends on "the nature of

[518 F.3d 1206]

the criminal activity, the length of the activity, and the nature of the property to be seized." *United States v. Riccardi*, 405 F.3d 852 , 860 (10th Cir.2005) (further quotation omitted). We have explained:

The observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.

Id. at 861 (quoting *United States v. Lamb,* 945 F.Supp. 441 , 460 (N.D.N.Y.1996)); *see also* *United States v. Hay,* 231 F.3d 630 , 636 (9th Cir.2000); *United States v. Harvey,* 2 F.3d 1318 , 1322-23 (3d Cir.1993); *United States v. Koelling,* 992 F.2d 817 , 823 (8th Cir.1993); *United States v. Rabe,* 848 F.2d 994 , 997 (9th Cir.1988). The district court correctly found that the information in the affidavits was not stale.

Finally, Perrine argues the affidavits omitted information that would have vitiated probable cause. Essentially, he reiterates the argument that the affidavits did not state that none of the log ons by the IP address connected to "stevedragonslayer" occurred on September 2, nor did they attach the Yahoo! Login Tracker, which revealed that fact. He argues that the judge, had he known those facts, would not have found probable cause. For the reasons already stated, we reject this argument. The affidavits gave the issuing judge a "substantial basis for . . . conclud[ing] that a search would uncover evidence of wrongdoing." *Illinois v. Gates,* **462 U. S. Reports 213** , 236, 103 S.Ct. 2317 , 76 L.Ed.2d 527 (1983) (internal quotation marks omitted).

Even were we to conclude that probable cause was not established, we would affirm the denial of Perrine's motion to suppress under the good faith exception of *United States v. Leon,* **468 U. S. Reports 897** , 920-24, 104 S.Ct. 3405 , 82 L.Ed.2d 677 (1984) . In *Leon,* "the Supreme Court adopted a good-faith exception to the application of the exclusionary rule and specifically applied that exception where `an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope,' even though the search warrant was later deemed to be invalid." *United States v. Herrera,* 444 F.3d 1238 , 1249 (10th Cir. 2006) (quoting *Leon,* **468 U. S. Reports 920** , 104 S.Ct. 3405). "In this circuit, we have concluded that `*Leon's* good faith exception applies only narrowly, and ordinarily only when an officer relies, in an objectively reasonable manner, on a mistake made by someone other than the officer.'" *United States v. Cos,* 498 F.3d 1115 , 1132 (10th Cir.2007) (quoting *Herrera,* 444 F.3d at 1249).

In this case, law enforcement personnel searched Perrine's house in reliance on warrants issued by a state judge. "When reviewing the reasonableness of an officer's reliance upon a search warrant, this court must examine the underlying documents to determine whether they are `devoid of factual support.'" *Danhauer,* 229 F.3d at 1006 (quoting *United States v. McKneely,* 6 F.3d 1447 , 1454 (10th Cir. 1993)). The *Leon* Court recognized four situations in which an officer would not have reasonable grounds for believing that a search warrant had been properly issued. In any of those situations, the good-faith

[518 F.3d 1207]

exception to the exclusionary rule does not apply. Thus, if the issuing judge was misled by an affidavit containing false information or information that the affiant would have known was false but for his "reckless disregard of the truth," the evidence should be suppressed. *Leon,* **468 U. S. Reports 923** , 104 S.Ct. 3405 . Or suppression is required when the affidavit supporting the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* (further quotation omitted). Additionally, the exception does not apply "when a warrant is so facially deficient that the executing officer could not reasonably believe it was valid." *Danhauer,* 229 F.3d at 1007 (citing *Leon,* **468 U. S. Reports 923** , 104 S.Ct. 3405). None of those situations is present in this case.

III. Governmental Outrageous Conduct

Perrine moved to dismiss this case on the ground that the government had engaged in outrageous conduct. The district court denied the motion. We review that denial de novo. *United States v. Pedraza*, 27 F.3d 1515 , 1521 (10th Cir.1994).

Perrine's claim of outrageous governmental conduct is based upon the following: as indicated above, when Perrine committed the instant offense, he was on probation for a prior offense involving child pornography on his computer. His computer had been confiscated in connection with that prior offense. Before the police returned his computer to him, they thought the computer had been "cleaned" so that all pornography was removed. Wichita Police Detective Shawn Bostick testified that he had turned the computer over to the forensics unit to have it cleaned. Prior to releasing the computer to Perrine's attorney in the prior case, Bostick did not check to see that the forensics unit had in fact cleaned the computer. Perrine claims that the computer was returned to him with the child pornography from the prior case still on it, which he claims is tantamount to sticking a needle with heroin into the arm of an addict.

When explaining what happened to Perrine's computer, Bostick testified that, during the investigation of the prior case, Perrine had mentioned that he kept a hidden back-up copy of each of his files. Bostick further opined that, if the hidden back-up copy was missed during the search of the computer, the files could have been moved back to the computer after the computer was returned to Perrine, and it would appear that the files had been on the computer the entire time. Bostick thus testified, "As I stated, is it possible I returned child pornography to [Perrine] mistakenly? It is possible. Is it possible the stuff wasn't there? It's possible." Appellee's Supp.App. at 49. The district court found "returning these images to defendant was probably negligent, even incompetent; however, defendant has failed to make any showing that any governmental official acted intentionally in leaving the images on his computer." Mem. and Order at 10, Appellant's App. at 143.

"[T]he relevant inquiry when assessing claims of outrageous government conduct is whether, considering the totality of the circumstances . . . the government's conduct is so shocking, outrageous and intolerable that it offends the universal sense of justice." *United States v. Garcia*, 411 F.3d 1173 , 1181 (10th Cir.2005) (further quotation omitted). "`To succeed on an outrageous conduct defense, the defendant must show either (1) excessive government involvement in the creation of the crime, or (2) significant governmental coercion to induce the crime.'" *Id.* (quoting *Pedraza*, 27 F.3d at 1521). An outrageous conduct defense is of "narrow scope." *Id.*

[518 F.3d 1208]

(quoting *United States v. Lacey*, 86 F.3d 956 , 964 (10th Cir.1996)).

We agree with the district court that, assuming the government did return Perrine's computer to him with child pornography still on it, that was the product of negligence or incompetence, at most. It hardly meets the high standard of outrageous conduct.

CONCLUSION

For the foregoing reasons, the district court's order is AFFIRMED.

Notes:

1. As discussed more fully below, 18 U.S.C. § 2703(d) is part of the Electronic Communications Privacy Act ("ECPA"), which regulates the disclosure of electronic communications and subscriber information. 18 Pa. C.S.A. § 5743(d) is the Pennsylvania state law similar to the ECPA.

2. "The IP, or Internet Protocol, address is unique to a specific computer. Only one computer would be assigned a particular IP address." *United States v. Kennedy*, 81 F.Supp.2d 1103 , 1105 n. 3 (D.Kan.2000).

3. Another court has recently described Kazaa as follows:

Kazaa is a computer program that connects a computer to other computers on which the Kazaa program is also running. Kazaa's purpose is to allow users to download each other's shared files. The Kazaa program allows the user to designate which folders — and therefore which files — on his computer are shared with other Kazaa users. Each shared file has several descriptive fields that are viewable by other Kazaa users. These fields generally describe the file's contents and can be edited by a file's possessor. Kazaa makes each user's shared files discoverable to other users by allowing any user to perform a keyword search of the descriptive fields of all shared files. Files with descriptive fields containing the search term are listed for the searcher, who can then see all the descriptive fields for each file on the list. Based on these descriptions, the searcher decides which of the available files to download onto his computer. The searcher is likewise free to refrain from downloading a file in which, based on its descriptive fields, the searcher is uninterested.

United States v. Sewell, 513 F.3d 820 , 821 (8th Cir.2008). *See also* *United States v. Shaffer,* 472 F.3d 1219 , 1220-22 (10th Cir.2007) (describing more fully how Kazaa operates).

4. 18 Pa.C.S.A. § 5743 provides for comparable disclosure and has virtually identical requirements for the court order.

5. Under *Terry v. Ohio,* **392 U. S. Reports 1** , 88 S.Ct. 1868 , 20 L.Ed.2d 889 (1968) , investigatory stops are permitted if "supported by a reasonable suspicion of criminal activity." *United States v. Treto-Haro,* 287 F.3d 1000 , 1004 (10th Cir.2002).

6. The Pennsylvania statute at issue similarly provides exclusively civil remedies for violations of the act. *See* 18 Pa.C.S.A. §§ 5747, 5748.

7. While no one argues the point, and it is not critical to our decision, it is widely known that any single service provider, like Yahoo!, does not permit more than one subscriber to have the same screen name. Thus, there would have been only one "stevedragonslayer" as a Yahoo! subscriber during the period of time relevant to this case. Since Perrine admitted he was "stevedragonslayer" and both Vanlandingham and Officer Humbert observed the chat session with "stevedragonslayer," there can be little doubt that the individual chatting with Vanlandingham on September 2, 2005, and showing pornographic videos was, in fact, Perrine. Furthermore, despite his wholly speculative arguments to the contrary, Perrine presents no evidence that anyone else "hijacked" his computer and went on line using the name "stevedragonslayer."
