[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS

FOR THE ELEVENTH CIRCUIT



---

Nos. 01-15788, 01-16100 and 01-16269

---

D. C. Docket No. 00-0017-CR-N

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

BRADLEY JOSEPH STEIGER,

Defendant-Appellant.

---

Appeals from the United States District Court for the
Middle District of Alabama

---

**(January 14, 2003)**

Before DUBINA, MARCUS and GOODWIN[*], Circuit Judges.

---

[*]Honorable Alfred T. Goodwin, United States Circuit Judge for the Ninth Circuit, sitting by designation.

GOODWIN, Circuit Judge:

Bradley Steiger appeals his convictions for sexual exploitation of children (18 U.S.C. § 2251(a)), possession of a computer containing child pornography (18 U.S.C. § 2252A(a)(5)(B)), and receipt of child pornography through interstate and foreign commerce (18 U.S.C. § 2252(a)(2)(A)). He challenges the district court's conclusion that neither the Fourth Amendment nor Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) ("ECPA"), codified at 18 U.S.C. §§ 2510-2522 ("The Wiretap Act"), warranted suppression of the evidence used to convict him. We affirm.

**I.**

The Montgomery, Alabama Police Department ("MPD") initiated an investigation of Steiger when an unidentified person ("anonymous source" or "source") sent the following e-mail on July 16, 2000:

> I found a child molester on the net. I'm not sure if he is abusing his own child or a child he kidnaped. He is from Montgomery, Alabama. As you see he is torturing the kid. She is 5-6 y.o. His face is seen clearly on some of the pictures. I know his name, internet account, home address and I can see when he is online. What should I do? Can I send all the pics and info I have to these emails?
>
> Regards
>
> P.S. He is a doctor or a paramedic.

The anonymous source attached to this e-mail an electronic image file containing a picture of a white male sexually abusing a young white female who appeared to be approximately four to six years of age.

On July 17, 2000, Captain Kevin Murphy of the MPD replied, asking the anonymous source to call him at his office. The source responded that he was from Turkey and could not afford an overseas phone call, but could send everything by e-mail. Captain Murphy then sent an e-mail stating: "Please feel free to send the information that you have." The source next sent an e-mail with eight attached images showing an adult white male nude from the waist down fondling and pressing the young girl against his body in various positions and exposing her genitalia. One picture depicted clamps connected to a chain attached to the child's labia. The girl was nude in several photographs and partially dressed in others. The anonymous e-mail again identified the molester as "Brad Steiger," and provided Steiger's Internet service account information with AT&T WorldNet, possible home address, telephone number used to connect to the Internet, and a fax number.

The anonymous source also informed Captain Murphy that he had Steiger's "i.p. number with local (Turkish) time." An IP number, also known as an Internet Protocol ("IP") address, "is the unique address assigned to a particular computer connected to the Internet. All computers connected to the Internet have an IP

address." Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1145 (2002). "IP addresses are either static—associated with one computer—or dynamically assigned. The latter is usually the case for patrons of dial-up Internet Service Providers (ISP). . . . Static addresses are undoubtedly easier to trace, but ISPs generally log the assignments of their dynamic addresses." Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berkeley Tech. L. J. 1085, 1104 n.101 (2002).

Captain Murphy viewed the eight images, and, on July 19, asked the source to send Steiger's IP address. The source sent three IP addresses used by Steiger on July 14 and 15; thus, it appears that Steiger's Internet Service Provider assigned dynamic IP addresses for each login. Apparently without being asked to do so, the source sent an e-mail to the MPD on July 19 providing Steiger's checking account records. On July 21, the source sent another e-mail that identified specific folders where pornographic pictures were stored on Steiger's computer.

Captain Murphy collected the information the source provided and referred it to Special Agent Margaret Faulkner of the FBI, who viewed the images and verified the details the anonymous source provided in his first two e-mails. She issued a subpoena to Security at AT&T Worldnet Service, who advised Agent Faulkner that the Internet account the anonymous source referred to was registered to a Brad

Steiger at the home address the source provided. Agent Faulkner then performed an Alabama Driver's License check and obtained a "photo ID" copy of the license issued to a "Bradley Joseph Steiger." She concluded that the photo "appeared identical to the white male subject depicted in the photographs with the young girl." She also checked with the Alabama Medical Board and determined that a "Brad Steiger" had a license to dispense medicine as a practitioner in Alabama and had worked as an emergency room physician in Montgomery. Agent Faulkner went to the hospital where the Medical Board indicated Steiger had been working and showed one of the pictures of Steiger with the young girl. A security officer identified the man as Brad Steiger, a doctor who had been seen around the hospital on occasion. Agent Faulkner then learned that Steiger had become employed by a hospital in Selma, Alabama. She also discovered that Steiger then resided at an address different from the one the source supplied.

Agent Faulkner next prepared an affidavit in support of a search warrant in which she stated that "an anonymous source . . . had located a child molester on the Internet." The affidavit described the pictures the anonymous source sent on July 17 without mentioning that the source had obtained the evidence by "hacking" into Steiger's computer. Agent Faulkner also described in the affidavit the steps she took to corroborate the information the anonymous source provided. After

obtaining a warrant, law enforcement officers searched Steiger's home and seized his computer and related equipment, as well as leg restraints, clamps connected to a chain, and what appeared to be a blindfold.

A federal grand jury returned an indictment against Steiger on November 9, 2000, charging violation of various federal statutes involving sexual exploitation of minors. Count I alleged violation of 18 U.S.C. § 2251(a) (inducing a minor to engage in sexually explicit conduct to produce visual depictions such as exhibition of the genitals and pubic area of a minor); Count II alleged a second violation of § 2251(a); Count III alleged violation of 18 U.S.C. § 2252(a)(5)(B) (knowing possession of a computer containing three or more images of child pornography); Count IV alleged violation of 18 U.S.C. § 2252(a)(2)(A) (knowing receipt of child pornography); Count V alleged violation of 18 U.S.C. § 2423(a) (knowing transportation of minor in interstate commerce with intent that the person engage in sexual activity); and Count VI alleged a second violation of § 2423(a).

An FBI agent stationed in Turkey attempted to interview the source at the end of November 2000 to determine how he had acquired the information regarding Steiger that he sent to the MPD. But the source was adamant about not revealing his identity, but explained in an e-mail on November 30, 2000 how he obtained that information:

> I will not tell you my name or meet you. . . . If I tell you my name and make an official interview with you, that guy and his lawyer will know all about me so I will have an overseas enemy.
>
> I'm not a computer freak. I'm a 33 years [sic] old professional. I have a family. I don't want to risk my peace because of a hobby. I'll answer some of your possible questions.
>
> Do [sic] I know him before?
>
> No. I catched [sic] at least 2000 child pornography collectors with my trap. 3 of them including this guy was [sic] producing their own. The other two realized whats [sic] going on and cut the connection.
>
> How did I know his home address, his fax number, etc?
>
> I couldn't find him on white pages so I searched all the ms word documents in his pc and found this document . . . .
>
> How did I get access to his pc?
>
> I used the well known trojan horse named subseven. . . . I made it undetectable so av softwares [sic] couldnt [sic] see it and bind it with a fake program. After this I posed it to the news group "alt.binaries.pictures.erotica.pre-teen" where one can find 1000s of sick people.
>
> If you have any more questions, just mail me. I tell you again "I WILL NEVER TELL YOU MY NAME AND NEVER MEET YOU."

After Steiger downloaded the fake picture the source posted to the news group, the Trojan Horse program permitted the source to enter into Steiger's computer via the Internet and find the images and identifying information he sent to the MPD.

Steiger filed several motions to suppress, claiming, *inter alia*, that: (1) the evidence asserted in support of the search warrant was obtained in violation of the

Fourth Amendment; (2) Agent Faulkner failed sufficiently to corroborate the information the source supplied; (3) Agent Faulkner intentionally omitted material evidence from her affidavit by failing to inform the magistrate that the source had obtained the information by hacking into Steiger's computer; and (4) the information the source obtained was inadmissible under the Wiretap Act. A magistrate judge recommended denial of Steiger's first motion to suppress. The district court adopted the magistrate's findings and denied the motion.

Steiger then filed a motion for reconsideration, as well as a motion for leave to argue in person. Steiger's motion seeking to argue pro se was limited at this time to oral argument before the district court on his motion to suppress. He indicated his intent in this motion to have "counsel present to assist him in other proceedings." The parties then submitted additional briefs on various aspects of their arguments. In one submission, Steiger responded to the government's Fourth Amendment position stating: "The defense is not relying upon the 'agent of government' defense although it was an argument mentioned in the early stages of the case (before having full disclosure)."

The district court again denied the motion to suppress, holding that Steiger had abandoned his agent-of-the-government theory. The court alternatively reasoned that even if that argument had not been abandoned, the anonymous source

had acted as a private individual. There was no proof that the source acted as a government agent, and, therefore, his acts did not implicate the Fourth Amendment. Without deciding whether the Wiretap Act applied, the district court also held that the Act did not include suppression as a remedy because the provisions addressing suppression did not refer to electronic communications.

The district court subsequently denied as untimely myriad successive motions to suppress and motions for reconsideration in which Steiger asserted, *inter alia*, that he had not abandoned his agent-of-the-government argument and that the anonymous source was "actually a 'confidential governmental agent' who by his actions has conducted an unlawful 'search' of [Steiger's] computer at the direction of an 'unknown agency' and has conducted an elaborate ruse to obscure his identity and to protect the agency for whom he is or was working. . . ." The district court also denied these motions on their merits because Steiger had produced no facts to meet his burden of proving the source acted as a government agent, finding that "all [Steiger had was] mere speculation and conjecture."

After the prosecution had presented its case, the defense moved for a directed verdict of acquittal on each of the charges. The district court granted the motion in part by dismissing Count V (interstate transportation of a minor). After the case went to the jury, Steiger filed a motion to waive counsel and proceed pro se,

contending that his attorney had provided ineffective assistance of counsel. After questioning Steiger and strongly recommending that he allow Christine Freeman from the Federal Defender's Office to represent him, the district court granted Steiger's motion to proceed pro se and appointed Freeman as standby counsel.

The jury then found Steiger guilty on Counts I-IV and VI. Steiger, with the assistance of Freeman, moved for acquittal or a new trial, and later for reconsideration of the verdict for Counts II and IV. The district court granted the motions in part by acquitting Steiger on Counts II and VI (second violations of statutes charged in Counts I and V). It then entered a judgment and conviction on Counts I, III, and IV, and sentenced Steiger to 210 months in prison and 3 years of supervised release.

## II.

### A. The Fourth Amendment

Steiger claims that the search warrant was obtained in violation of his Fourth Amendment right against unreasonable searches and seizures because it was based in part on information from an anonymous source who hacked into his computer. Steiger first argues that the district court erred in finding he had abandoned his agent-of-the-government theory. We need not reach the correctness of that finding because the record is clear that the source acted at all material times as a private

individual. The district court correctly held that suppression was not warranted on this ground.

A search by a private person does not implicate the Fourth Amendment unless he acts as an instrument or agent of the government. *United States v. Ford*, 765 F.2d 1088, 1090 (11th Cir. 1985). For a private person to be considered an agent of the government, we look to two critical factors: (1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the private actor's purpose was to assist law enforcement efforts rather than to further his own ends. *See United States v. Simpson*, 904 F.2d 607, 610 (11th Cir. 1990) (citing *United States v. Miller*, 688 F.2d 652, 657 (9th Cir. 1982)); *see also Ford*, 765 F.2d at 1090 (holding that the district court properly denied motion to suppress where there was no evidence that the government "had any pre-knowledge of the search [or] that the agents openly encouraged or cooperated in the search").

The district court's finding of probable cause for the search warrant was based on the information provided in the anonymous source's first and second e-mails, together with Agent Faulkner's affidavit describing how she personally corroborated that information. The information conveyed in those two e-mails was limited to that which the source had acquired *before* making *any* contact with the MPD. Thus, even assuming *arguendo* that the MPD tacitly encouraged further

nonconsensual searches, the information relied on in support of the warrant—graphic images showing Steiger sexually abusing a young child and identifying information regarding Steiger which Agent Faulkner thoroughly corroborated—more than sufficed to establish probable cause.

We also reject Steiger's argument for suppression based on Agent Faulkner's failure to advise the judge who issued the warrant *how* the source obtained the information he sent to the MPD. Steiger asserts that no judge would have found probable cause knowing that the source had hacked into his computer. But he supplies no authority for this assertion. To justify suppression of evidence seized under a warrant, the alleged deliberate or reckless failure to include material information in the affidavit must conceal information that would defeat probable cause. *See United States v. Cross*, 928 F.2d 1030, 1040 (11th Cir. 1991); *see also United States v. Jenkins*, 901 F.2d 1075, 1080 (11th Cir. 1990) (Minor or immaterial omissions from the affidavit will not invalidate a warrant where the omitted information, if furnished, would not have precluded a finding of probable cause.). And we must give "great deference" to a lower court's determination that the totality of the circumstances supported a finding of probable cause. *United States v. Brundidge*, 170 F.3d 1350, 1352 (11th Cir. 1999).

Agent Faulkner put the magistrate judge on notice regarding the manner in which she had received the information asserted in support of the warrant—*i.e.*, that it came from an anonymous source who claimed to have found a child molester on the Internet. Because information obtained by a private person is not subject to the Fourth Amendment's exclusionary rule, a statement that the anonymous source had hacked into Steiger's computer to obtain that information would not have affected the magistrate's finding of probable cause.

**B. The Wiretap Act**

Unlike the Fourth Amendment, the Wiretap Act applies to private conduct as well as to governmental agents. The Act denounces certain "interceptions." Steiger's argument that the district court should have granted his motion to suppress pursuant to the Wiretap Act presents two questions of first impression in this Circuit: (1) whether the anonymous source "intercepted" any "electronic communications" in violation of the Wiretap Act; and (2) if so, whether any of the Act's provisions require suppression. The district court declined to address the threshold issue and instead ruled that even if the source had intercepted electronic communications in violation of the Wiretap Act, the Act's provisions provide for suppression only with respect to unlawful interceptions of oral or wire communications. Steiger concedes that the Wiretap Act expressly provides for

suppression only with respect to unlawfully intercepted *oral* and *wire* communications. *See* 18 U.S.C. §§ 2515, 2518(10)(a). But he asserts that suppression of unlawfully seized *electronic* communications is available by negative implication under 18 U.S.C. § 2517(3), which authorizes disclosure of electronic evidence at trial if it was acquired in accordance with the Wiretap Act. He also claims that the Wiretap Act authorizes suppression of evidence seized in violation of the Fourth Amendment.

We hold that the anonymous source did not intercept electronic communications in violation of the Wiretap Act. We also hold that while the Wiretap Act clearly provides criminal and civil sanctions for the unlawful interception of electronic communications, *see* 18 U.S.C. §§ 2511(1), (4), (5), 2520, the Act provides no basis for moving to suppress such communications.

(1) The anonymous source did not intercept electronic communications in violation of the Wiretap Act when he hacked into Steiger's computer.

In 1986, Title I of the ECPA amended the federal Wiretap Act, which previously had addressed only interception of wire and oral communications, to also address interception of electronic communications. *See* Pub.L. No. 99-508, 100 Stat. 1848; S.Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557; 18 U.S.C. §§ 2510(12); 2511(1)(a); *Konop v. Hawaiian Airlines, Inc*, 302 F.3d 868, 874 (9th Cir. 2002). At the same time, Title II of the ECPA created

the Stored Communications Act ("SCA") to cover access to stored communications and records. *See* Pub.L. No. 99-508, 100 Stat. 1848; S.Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557; 18 U.S.C. § 2701(a); *Konop*, 302 F.3d at 874. We begin our analysis by agreeing with the Ninth Circuit that

> the intersection of these two statutes is a complex, often convoluted, area of the law. [T]he difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication . . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. [U]ntil Congress brings the laws in line with modern technology, protection of the Internet . . . will remain a confusing and uncertain area of the law.

*Konop*, 302 F.3d at 874 (internal quotation marks and citations omitted) (collecting law review articles criticizing judicial interpretations of the ECPA).

The Wiretap Act generally prohibits the intentional "interception" of "wire, oral, or electronic communications." *See* 18 U.S.C. § 2511(1). Thus, we must decide whether any information the source provided in his first two e-mails to the MPD falls within the definition of "electronic communications," and, if so, whether the source "intercepted" that information within the meaning of the Act.

"Electronic communications" are defined in the Wiretap Act as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or

photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). At least one Circuit has held that information stored on a server and conveyed from a private website to users clearly falls within the definition of "electronic communications." *Konop*, 302 F.3d at 876. Here, the source penetrated Steiger's computer by using a "Trojan Horse" virus that enabled him to discover and download files stored on Steiger's hard drive. That information was transferred from Steiger's computer to the source over one of the specified media and thus falls within the Wiretap Act's definition of "electronic communications."

"Interception" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). The Circuits which have interpreted this definition as applied to electronic communications have held that it encompasses only acquisitions contemporaneous with transmission. *See Konop*, 302 F.3d at 878-89 (withdrawing previous panel opinion at 236 F.3d 1035 (9th Cir. 2001) holding to the contrary); *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457 (5th Cir. 1994); *see also United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998).

The Fifth Circuit observed in *Steve Jackson Games* that, before Congress enacted the ECPA, federal courts had read "intercept" to mean the acquisition of a

communication contemporaneous with transmission. 36 F.3d at 460 (citing *United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976)). The *Steve Jackson Games* court further explained that in passing the ECPA, Congress intended to retain the previous definition of "intercept" while amending the Wiretap Act to cover interceptions of electronic communications. 36 F.3d at 462. But the Fifth Circuit reasoned that the word "intercept" could not describe identical conduct with respect to both wire and electronic communications, because they were defined differently. *Steve Jackson Games*, 36 F.3d at 461-62. Specifically, the ECPA redefined the term "wire communication" to include electronic storage of the communication, but omitted reference to storage from its definition of "electronic communication." *See* 18 U.S.C. § 2510(1) (2000) (defining "wire communication"); 18 U.S.C. § 2510(12) (2000) (defining "electronic communication").

This textual difference illustrates Congress' intent that one could "intercept" a wire communication in storage, but could not "intercept" a similarly situated electronic communication:

> Congress' use of the word "transfer" in the definition of "electronic communication," and its omission in that definition of the phrase "any electronic storage of such communication" . . . reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage."

*Steve Jackson Games,* 36 F.3d at 461-62; *see also Konop*, 302 F.3d at 877. The Ninth Circuit in *Konop* explained that it already had relied on "the same textual distinction as the Fifth Circuit" to conclude in *Smith* "that wire communications in storage could be 'intercepted' under the Wiretap Act":

> Congress' inclusion of storage in the definition of "wire communication" militated in favor of a broad definition of the term "intercept" with respect to wire communications, one that included acquisition of a communication subsequent to transmission. [With respect to wire communications only, the prior definition of "intercept"—acquisition contemporaneous with transmission—had been overruled by the ECPA. On the other hand [*Smith*] suggested a narrower definition of "intercept" was still appropriate with regard to electronic communications. . . .

302 F.3d at 877-78 (citing *Smith*, 155 F.3d at 1057).

The *Konop* court also noted that Congress' recent amendment to the Wiretap Act eliminating "storage" from the definition of "wire communication" provides further support to the analysis relied on in *Steve Jackson Games* and *Smith*:

> By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of "intercept"—acquisition contemporaneous with transmission—with respect to wire communications. The purpose of the recent amendment was to reduce protection of voice mail messages to the lower level of protection provided other electronically stored communications. When Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term "intercept" with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make that definition applicable to voice mail messages as well. Congress,

> therefore, accepted and implicitly approved the judicial definition of "intercept" as acquisition contemporaneous with transmission.

302 F.3d at 878 (internal citations omitted). Indeed, as *Konop* pointed out, this definition is "consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.'" *Id*. (quoting *Webster's Ninth New Collegiate Dictionary* 630 (1985)).

The Fifth and Ninth Circuits' reasoning is persuasive and we hold that a contemporaneous interception—*i.e.*, an acquisition during "flight"—is required to implicate the Wiretap Act with respect to electronic communications.

The Ninth and Fifth Circuits also concluded that their reading of the Wiretap Act "is consistent with the structure of the ECPA, which created the SCA for the express purpose of addressing 'access to *stored* . . . electronic communications and transactional records.'" *Konop*, 302 F.3d at 878-79 (emphasis in original) (quoting S.Rep. No. 99-541 at 3); *Steve Jackson Games*, 36 F.3d at 463. These two cases reasoned that

> [t]he level of protection provided stored communications under the SCA is considerably less than that provided by communications covered by the Wiretap Act. . . . [If] acquisition of a stored communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA. Congress could not have intended this result.

*Konop*, 302 F.3d at 879; *see also Steve Jackson Games*, 36 F.3d at 463.

Though we agree with the Fifth and Ninth Circuits' interpretation of the Wiretap Act, we do not rely on this particular reasoning in doing so. *See generally Konop*, 302 F.3d at 889 (Reinhardt, J., dissenting in part) (explaining that "[t]he majority's interpretation of the Wiretap Act depends in part on a tortured reading of the Stored Communications Act"). The SCA creates criminal and civil penalties, but no exclusionary remedy, for unauthorized access to a "facility through which an electronic communication service is provided" to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication *while it is in electronic storage in such system*." 18 U.S.C. § 2701 (emphasis added); *see also* 18 U.S.C. §§ 2707, 2708. "Electronic communication service" is defined as "any service which provides users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). The SCA also generally prohibits an entity providing an electronic communication service to the public from disclosing information absent an applicable exception. *See* 18 U.S.C. § 2702. Thus, the SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system (BBS).

The SCA, however, does not appear to apply to the source's hacking into Steiger's computer to download images and identifying information stored on his

hard-drive because there is no evidence to suggest that Steiger's computer maintained any "electronic communication service" as defined in 18 U.S.C. § 2510(15). *Cf. Konop*, 302 F.3d at 879-80 (finding SCA applicable to information stored on a BBS); *Steve Jackson Games*, 36 F.3d at 462-64 (applying SCA to information stored on a secure website accessed by third-party users). We note, however that the SCA may apply to the extent the source accessed and retrieved any information stored with Steiger's Internet service provider. In sum, our reading of the Wiretap Act to cover only real-time interception of electronic communications, together with the apparent non-applicability of the SCA to hacking into personal computers to retrieve information stored therein, reveals a legislative hiatus in the current laws purporting to protect privacy in electronic communications. This hiatus creates no remedy.

We now turn to the issue of whether the anonymous source acquired any electronic communications contemporaneously with their transmission. The Ninth Circuit in *Konop* held that viewing a private website by way of the Internet without authorization did not constitute an interception of electronic communications in violation of the Wiretap Act because such unauthorized viewing merely gained access to stored electronic communications. 302 F.3d at 879. Similarly, the Fifth Circuit in *Steve Jackson Games* rejected an argument that seizure of a computer

used to operate an electronic bulletin board system (BBS) constituted an interception of the stored but unread e-mail contained on that system, reasoning that e-mail stored on the BBS' computer hard drive was no longer in transmission and thus could not be intercepted within the meaning of the Wiretap Act. 36 F.3d at 461.

Indeed, under the narrow reading of the Wiretap Act we adopt from the Fifth and Ninth Circuits, very few seizures of electronic communications from computers will constitute "interceptions."

> [T]here is only a narrow window during which an E-mail interception may occur—the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

Jarrod J. White, *E-Mail @Work.com: Employer Monitoring of Employee E-Mail*, 48 Ala. L. Rev. 1079, 1083 (1997).

In this case, there is nothing to suggest that any of the information provided in the source's e-mails to the MPD was obtained through contemporaneous acquisition of electronic communications while in flight. Rather, the evidence shows that the source used a Trojan Horse virus that enabled him to access and download information stored on Steiger's personal computer. This conduct, while

possibly tortious, does not constitute an interception of electronic communications in violation of the Wiretap Act.

(2) Suppression is not a remedy under the Wiretap Act with respect to unlawfully seized electronic communications.

Even if Steiger could demonstrate that the actions of the source constituted an "interception" in violation of the Wiretap Act, the suppression provision in the Act provides no basis for moving to suppress electronic communications. By its terms, 18 U.S.C. § 2515 applies *only* to "wire or oral communication[s]," and not to "electronic communications":

> Whenever any *wire or oral communication* has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

18 U.S.C. § 2515. Despite the fact that the ECPA amended numerous sections of the Wiretap Act to include "electronic communications," the ECPA did not amend § 2515. Further, although, as noted by Steiger, Congress considered amending § 2515 in the USA Patriot Act to "extend[] the statutory exclusion rule in 18 U.S.C. § 2515 to electronic communications," the Act was passed without such an amendment. *Compare* H.R. Rep. No. 236(I), at 8 (2001), *with* USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

"[I]t is generally presumed that Congress acts intentionally and purposely when it includes particular language in one section of a statute but omits it in another," *BFP v. Resolution Trust Corp.*, 511 U.S. 531, 536 (1994) (citing *Chicago v. Envtl. Def. Fund*, 511 U.S. 328, 338 (1994) (internal quotation marks omitted)). That presumption is made even stronger when, as here, Congress has amended a statute to include certain language in some, but not all, provisions of the statute.

Case law supports this conclusion. In *United States v. Meriwether*, the Sixth Circuit held that it could not "under the ECPA grant appellant's requested remedy—suppression [because t]he ECPA does not provide an independent statutory remedy of suppression for interceptions of electronic communications." 917 F.2d 955, 960 (6th Cir. 1990) (citations omitted); *see also, e.g.*, *United States v. Reyes*, 922 F.Supp. 818, 837 (S.D.N.Y. 1996) (holding that exclusion of evidence is not a remedy for the ECPA violation).

To the extent Steiger argues that §§ 2517 and 2518(10)(c) create a suppression remedy for unlawful interceptions of electronic communications under the statute,[1] the legislative history makes clear that a statutory suppression remedy

---

[1]18 U.S.C. § 2517 delineates the limitations on privileged disclosure of any wire, oral, or electronic communications obtained by investigative or law enforcement officers through the procedures explicated in § 2518. "[A]pplication[s] for an order authorizing or approving the interception of a wire, (continued...)

does not exist for unlawful interceptions of "electronic communications." As the

---

[1](...continued)
oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application." 18 U.S.C. § 2518(1). Section 2518 explains in part the contents required for such an application, the character of an order that may be entered by the federal courts authorizing or approving the interception of any wire, oral or electronic communication under the Act, and procedures by which law enforcement or investigative officers may intercept wire, oral or electronic communications in "emergency situation[s]." 18 U.S.C. § 2518. Further, § 2518 authorizes persons aggrieved by a violation of the Act:

> [T]o move to suppress the contents of any wire or oral communication intercepted pursuant to [the Act], or evidence derived therefrom, on the grounds that-- (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval.

18 U.S.C. § 2518(10)(a). However, § 2518 also explains that "[t]he remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications." 18 U.S.C. § 2518(10)(c). In addition to the suppression remedy of § 2515, an aggrieved person can, in a civil action, recover "(1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c) and punitive damages in appropriate cases; and (3) a reasonable attorney's fee and other litigation costs reasonably incurred." 18 U.S.C. § 2520(b). Notably, as with § 2515, none of these provisions provide a mechanism by which an aggrieved person can move for suppression of "electronic communications."

Government notes, the Senate Report accompanying the ECPA discusses the ECPA's addition of 2518(10)(c), stating:

> Subsection 101(e) of the Electronic Communications Privacy Act amends subsection 2518(10) of title 18 to add a paragraph (c) which provides that with respect to the interception of electronic communications, the remedies and sanctions described in this chapter are the only judicial remedies and sanctions available for nonconstitutional violations of this chapter involving such communications. In the event that there is a violation of law of a constitutional magnitude, the court involved in a subsequent trial will apply the existing Constitutional law with respect to the exclusionary rule.
>
> The purpose of this provision is to underscore that, as a result of discussions with the Justice Department, the [ECPA] does not apply the statutory exclusionary rule contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the interception of electronic communications.

S. Rep. No. 99-541, at 23. The omission of "electronic communications" from section 2515 is dispositive. The Wiretap Act does not provide a suppression remedy for electronic communications unlawfully acquired under the Act.

## IV.

Because this case implicates neither the Fourth Amendment nor the Wiretap Act, we AFFIRM the judgment of the district court.