United States Court of Appeals,

Fifth Circuit.

No. 93-8661.

STEVE JACKSON GAMES, INCORPORATED, et al., Plaintiffs-Appellants,

v.

UNITED STATES SECRET SERVICE, et al., Defendants,

United States Secret Service and United States of America, Defendants-Appellees.

Oct. 31, 1994.

Appeal from the United States District Court for the Western District of Texas.

Before HIGGINBOTHAM, JONES and BARKSDALE, Circuit Judges.

RHESA HAWKINS BARKSDALE, Circuit Judge:

The narrow issue before us is whether the seizure of a computer, used to operate an electronic bulletin board system, and containing private electronic mail which had been sent to (stored on) the bulletin board, but not read (retrieved) by the intended recipients, constitutes an unlawful intercept under the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, as amended by Title I of the Electronic Communications Privacy Act of 1986, Pub.L. No. 99-508, Title I, 100 Stat. 1848 (1986). We hold that it is not, and therefore AFFIRM.

I.

The district court's findings of fact are not in dispute. *See Steve Jackson Games, Inc. v. United States Secret Service,* 816 F.Supp. 432 (W.D.Tex.1993). Appellant Steve Jackson Games, Incorporated (SJG), publishes books, magazines, role-playing games, and related products. Starting in the mid-1980s, SJG operated an electronic bulletin board system, called "Illuminati" (BBS), from one of its computers. SJG used the BBS to post public information about its business, games, publications, and the role-playing hobby; to facilitate play-testing of games being developed; and to communicate with its customers and free-lance writers by electronic mail (E-mail).

Central to the issue before us, the BBS also offered customers the ability to send and receive private E-mail. Private E-mail was stored on the BBS computer's hard disk drive temporarily, until

the addressees "called" the BBS (using their computers and modems) and read their mail. After reading their E-mail, the recipients could choose to either store it on the BBS computer's hard drive or delete it. In February 1990, there were 365 BBS users. Among other uses, appellants Steve Jackson, Elizabeth McCoy, William Milliken, and Steffan O'Sullivan used the BBS for communication by private E-mail.

In October 1988, Henry Kluepfel, Director of Network Security Technology (an affiliate Bell Company), began investigating the unauthorized duplication and distribution of a computerized text file, containing information about Bell's emergency call system. In July 1989, Kluepfel informed Secret Service Agent Foley and an Assistant United States Attorney in Chicago about the unauthorized distribution. In early February 1990, Kluepfel learned that the document was available on the "Phoenix Project" computer bulletin board, which was operated by Loyd Blankenship in Austin, Texas; that Blankenship was an SJG employee; and that, as a co-systems operator of the BBS, Blankenship had the ability to review and, perhaps, delete any data on the BBS.

On February 28, 1990, Agent Foley applied for a warrant to search SJG's premises and Blankenship's residence for evidence of violations of 18 U.S.C. §§ 1030 (proscribes interstate transportation of computer access information) and 2314 (proscribes interstate transportation of stolen property). A search warrant for SJG was issued that same day, authorizing the seizure of, *inter alia,*

> [c]omputer hardware ... and computer software ... and ... documents relating to the use of the computer system ..., and financial documents and licensing documentation relative to the computer programs and equipment at ... [SJG] ... which constitute evidence ... of federal crimes.... This warrant is for the seizure of the above described computer and computer data and for the authorization to read information stored and contained on the above described computer and computer data.

The next day, March 1, the warrant was executed by the Secret Service, including Agents Foley and Golden. Among the items seized was the computer which operated the BBS. At the time of the seizure, 162 items of unread, private E-mail were stored on the BBS, including items addressed to the individual appellants. Despite the Secret Service's denial, the district court found that Secret Service personnel or delegates read and deleted the private E-mail stored on the BBS.

Appellants filed suit in May 1991 against, among others, the Secret Service and the United

States, claiming, *inter alia*, violations of the Privacy Protection Act, 42 U.S.C. § 2000aa, *et seq.*[1]; the Federal Wiretap Act, as amended by Title I of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2521 (proscribes, *inter alia*, the intentional interception of electronic communications); and Title II of the ECPA, 18 U.S.C. §§ 2701-2711 (proscribes, *inter alia*, intentional access, without authorization, to stored electronic communications).[2]

The district court held that the Secret Service violated the Privacy Protection Act, and awarded actual damages of $51,040 to SJG; and that it violated Title II of the ECPA by seizing stored electronic communications without complying with the statutory provisions, and awarded the statutory damages of $1,000 to each of the individual appellants. And, it awarded appellants $195,000 in attorneys' fees and approximately $57,000 in costs. But, it held that the Secret Service did not "intercept" the E-mail in violation of Title I of the ECPA, 18 U.S.C. § 2511(1)(a), because its acquisition of the contents of the electronic communications was not contemporaneous with the transmission of those communications.

II.

As stated, the sole issue is a very narrow one: whether the seizure of a computer on which is stored private E-mail that has been sent to an electronic bulletin board, but not yet read (retrieved)

---

[1]Section 2000aa(a) provides that it is

> unlawful for a government officer or employee, in connection with the investigation ... of a criminal offense, to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication....

Among the items seized was a draft of *GURPS Cyberpunk*, a book intended by SJG for immediate publication. It was one of a series of fantasy role-playing game books SJG published. "GURPS" is an acronym for SJG's "Generic Universal Roleplaying System". "Cyberpunk" refers to a science fiction literary genre which became popular in the 1980s, which is characterized by the fictional interaction of humans with technology and the fictional struggle for power between individuals, corporations, and government.

[2]Kluepfel, the Assistant United States Attorney, and Agents Foley and Golden were also sued. In addition to the statutory claims, appellants also claimed violations of the First and Fourth Amendments to the United States Constitution. And, in September 1992, they added state law claims for conversion and invasion of privacy. Prior to trial, the claims against the individuals were dismissed, and appellants withdrew their constitutional and state law claims.

by the recipients, constitutes an "intercept" proscribed by 18 U.S.C. § 2511(1)(a).[3]

Section 2511 was enacted in 1968 as part of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, often referred to as the Federal Wiretap Act. Prior to the 1986 amendment by Title I of the ECPA, it covered only wire and oral communications. Title I of the ECPA extended that coverage to electronic communications.[4] In relevant part, § 2511(1)(a) proscribes "intentionally intercept[ing] ... any wire, oral, or electronic communication", unless the intercept is authorized by court order or by other exceptions not relevant here. Section 2520 authorizes, *inter alia*, persons whose electronic communications are intercepted in violation of § 2511 to bring a civil action against the interceptor for actual damages, or for statutory damages of $10,000 per violation or $100 per day of the violation, whichever is greater. 18 U.S.C. § 2520.[5]

The Act defines "intercept" 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."

---

[3]Appellants raised two other issues regarding damages, but later advised that they have been settled. And, prior to briefing, the Secret Service dismissed its cross-appeal.

[4]An "electronic communication" is defined 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, but does not include—
>
> (A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;
>
> (B) any wire or oral communication;
>
> (C) any communication made through a tone-only paging device; or
>
> (D) any communication from a tracking device (as defined in section 3117 of this title)....

18 U.S.C. § 2510(12).

[5]Title I of the ECPA increased the statutory damages for unlawful interception from $1,000 to $10,000. *See Bess v. Bess*, 929 F.2d 1332, 1334 (8th Cir.1991). On the other hand, as noted, Title II authorizes an award of "the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case ... less than the sum of $1000". 18 U.S.C. § 2707(c). As discussed, the individual appellants each received Title II statutory damages of $1,000.

18 U.S.C. § 2510(4). The district court, relying on our court's interpretation of intercept in *United States v. Turk,* 526 F.2d 654 (5th Cir.), *cert. denied,* 429 U.S. 823, 97 S.Ct. 74, 50 L.Ed.2d 84 (1976), held that the Secret Service did not intercept the communications, because its acquisition of the contents of those communications was not contemporaneous with their transmission. In *Turk,* the government seized from a suspect's vehicle an audio tape of a prior conversation between the suspect and Turk. (Restated, when the conversation took place, it was not recorded contemporaneously by the government.) Our court held that replaying the previously recorded conversation was not an "intercept", because an intercept "require[s] participation by the one charged with an "interception' in the contemporaneous acquisition of the communication through the use of the device". *Id.* at 658.

Appellants agree with *Turk*'s holding, but contend that it is not applicable, because it "says nothing about government action that both *acquires* the communication prior to its delivery, and *prevents* that delivery." (Emphasis by appellants.) Along that line, appellants note correctly that *Turk*'s interpretation of "intercept" predates the ECPA, and assert, in essence, that the information stored on the BBS could still be "intercepted" under the Act, even though it was not in transit. They maintain that to hold otherwise does violence to Congress' purpose in enacting the ECPA, to include providing protection for E-mail and bulletin boards. For the most part, appellants fail to even discuss the pertinent provisions of the Act, much less address their application. Instead, they point simply to Congress' intent in enacting the ECPA and appeal to logic (i.e., to seize something before it is received is to intercept it).

But, obviously, the language of the Act controls. In that regard, appellees counter that "Title II, not Title I, ... governs the seizure of stored electronic communications such as unread e-mail messages", and note that appellants have recovered damages under Title II. Understanding the Act requires understanding and applying its many technical terms as defined by the Act, as well as engaging in painstaking, methodical analysis. As appellees note, the issue is not whether E-mail can be "intercepted"; it can. Instead, at issue is what constitutes an "intercept".

Prior to the 1986 amendment by the ECPA, the Wiretap Act defined "intercept" as the "aural

acquisition" of the contents of wire or oral communications through the use of a device. 18 U.S.C. § 2510(4) (1968). The ECPA amended this definition to include the "aural *or other* acquisition of the contents of ... wire, *electronic,* or oral communications...." 18 U.S.C. § 2510(4) (1986) (emphasis added for new terms). The significance of the addition of the words "or other" in the 1986 amendment to the definition of "intercept" becomes clear when the definitions of "aural" and "electronic communication" are examined; electronic communications (which include the non-voice portions of wire communications), as defined by the Act, cannot be acquired aurally.

Webster's Third New International Dictionary (1986) defines "aural" as "of or relating to the ear" or "of or relating to the sense of hearing". *Id.* at 144. And, the Act defines "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. § 2510(18). This definition is extremely important for purposes of understanding the definition of a "wire communication", which is defined by the Act as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) ... *and such term includes any electronic storage of such communication.*

18 U.S.C. § 2510(1) (emphasis added). In contrast, as noted, an "electronic communication" is defined 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 ... but does not include ... any wire or oral communication...." 18 U.S.C. § 2510(12) (emphasis added).

Critical to the issue before us is the fact that, unlike the definition of "wire communication", *the definition of "electronic communication" does not include electronic storage of such communications. See* 18 U.S.C. § 2510(12). See note 4, *supra.*[6] "Electronic storage" is defined as

---

[6]Wire and electronic communications are subject to different treatment under the Wiretap Act. The Act's exclusionary rule, 18 U.S.C. § 2515, applies to the interception of wire communications, including such communications in electronic storage, *see* 18 U.S.C. § 2510(1), but not to the interception of electronic communications. *See* 18 U.S.C. § 2518(10)(a); *United States v. Meriwether,* 917 F.2d 955, 960 (6th Cir.1990); S.Rep. No. 99-541, 99th Cong., 2d Sess. 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577. And, the types of crimes that may be investigated by means of surveillance directed at electronic communications, 18 U.S.C. § 2516(3) ("any federal felony"), are not as limited as those that may be investigated by means of

> (A) any *temporary,* intermediate *storage* of a wire or *electronic communication incidental to the electronic transmission thereof;* and
>
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication....

18 U.S.C. § 2510(17) (emphasis added). The E-mail in issue was in "electronic storage". 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" (part of the definition of "wire communication") reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage".[7]

We could stop here, because "[i]ndisputably, the goal of statutory construction is to ascertain legislative intent through the plain language of a statute—without looking to legislative history or other extraneous sources". *Stone v. Caplan (Matter of Stone),* 10 F.3d 285, 289 (5th Cir.1994). But, when interpreting a statute as complex as the Wiretap Act, which is famous (if not infamous) for its lack of clarity, *see, e.g., Forsyth v. Barr,* 19 F.3d 1527, 1542-43 (5th Cir.), *cert. denied,* --- U.S. ----, --- S.Ct. ----, --- L.Ed.2d ---- (1994), we consider it appropriate to note the legislative history for confirmation of our understanding of Congress' intent. *See id.* at 1544.

As the district court noted, the ECPA's legislative history makes it crystal clear that Congress did not intend to change the definition of "intercept" as it existed at the time of the amendment. *See* 816 F.Supp. at 442 (citing S.Rep. No. 99-541, 99th Cong., 2d Sess. 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567). The Senate Report explains:

> Section 101(a)(3) of the [ECPA] amends the definition of the term "intercept" in current section 2510(4) of title 18 to cover electronic communications. The definition of "intercept" under current law is retained with respect to wire and oral communications except that the

---

surveillance directed at wire or oral communications. *See* 18 U.S.C. § 2516(1) (specifically listed felonies).

[7]Stored wire communications are subject to different treatment than stored electronic communications. Generally, a search warrant, rather than a court order, is required to obtain access to the contents of a stored electronic communication. *See* 18 U.S.C. § 2703(a). But, compliance with the more stringent requirements of § 2518, including obtaining a court order, is necessary to obtain access to a stored wire communication, because § 2703 expressly applies only to stored *electronic* communications, not to stored *wire* communications. *See* James G. Carr, *The Law of Electronic Surveillance,* § 4.10, at 4-126—4-127 (1994) (citing H.R.Rep. No. 99-647, 99th Cong., 2d Sess. 67-68 (1986)).

> term "or other" is inserted after "aural." This amendment clarifies that it is illegal to intercept the nonvoice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication.

1986 U.S.C.C.A.N. at 3567.

Our conclusion is reinforced further by consideration of the fact that Title II of the ECPA clearly applies to the conduct of the Secret Service in this case. Needless to say, when construing a statute, we do not confine our interpretation to the one portion at issue but, instead, consider the statute as a whole. *See, e.g., United States v. McCord,* --- F.3d ----, ----, 1994 WL 523211, at *6 (5th Cir.1994) (citing N. Singer, 2A *Sutherland Statutory Construction,* § 46.05, at 103 (5th ed. 1992)).

Title II generally proscribes unauthorized access to stored wire or electronic communications. Section 2701(a) provides:

> Except as provided in subsection (c) of this section whoever—
>
> > (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> >
> > (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication *while it is in electronic storage in such system* shall be punished....

18 U.S.C. § 2701(a) (emphasis added).

As stated, the district court found that the Secret Service violated § 2701 when it

> intentionally accesse[d] without authorization a facility [the computer] through which an electronic communication service [the BBS] is provided ... and thereby obtain[ed] [and] prevent[ed] authorized access [by appellants] to a[n] ... electronic communication while it is in electronic storage in such system.

18 U.S.C. § 2701(a). The Secret Service does not challenge this ruling. We find no indication in either the Act or its legislative history that Congress intended for conduct that is clearly prohibited by Title II to furnish the basis for a civil remedy under Title I as well. Indeed, there are persuasive indications that it had no such intention.

First, the substantive and procedural requirements for authorization to intercept electronic communications are quite different from those for accessing stored electronic communications. For example, a governmental entity may gain access to the contents of electronic communications that

have been in electronic storage for less than 180 days by obtaining a warrant. *See* 18 U.S.C. § 2703(a). But there are more stringent, complicated requirements for the interception of electronic communications; a court order is required. *See* 18 U.S.C. § 2518.

Second, other requirements applicable to the interception of electronic communications, such as those governing minimization, duration, and the types of crimes that may be investigated, are not imposed when the communications at issue are not in the process of being transmitted at the moment of seizure, but instead are in electronic storage. For example, a court order authorizing interception of electronic communications is required to include a directive that the order shall be executed "in such a way as to minimize the interception of communications not otherwise subject to interception". 18 U.S.C. § 2518(5). Title II of the ECPA does not contain this requirement for warrants authorizing access to stored electronic communications. The purpose of the minimization requirement is to implement "the constitutional obligation of avoiding, to the greatest possible extent, seizure of conversations which have no relationship to the crimes being investigated or the purpose for which electronic surveillance has been authorized". James G. Carr, *The Law of Electronic Surveillance,* § 5.7(a) at 5-28 (1994).

Obviously, when intercepting electronic communications, law enforcement officers cannot know in advance which, if any, of the intercepted communications will be relevant to the crime under investigation, and often will have to obtain access to the contents of the communications in order to make such a determination. Interception thus poses a significant risk that officers will obtain access to communications which have no relevance to the investigation they are conducting. That risk is present to a lesser degree, and can be controlled more easily, in the context of stored electronic communications, because, as the Secret Service advised the district court, technology exists by which relevant communications can be located without the necessity of reviewing the entire contents of all of the stored communications. For example, the Secret Service claimed (although the district court found otherwise) that it reviewed the private E-mail on the BBS by use of key word searches.

Next, as noted, court orders authorizing an intercept of electronic communications are subject to strict requirements as to duration. An intercept may not be authorized "for any period longer than

is necessary to achieve the objective of the authorization, nor in any event longer than thirty days". 18 U.S.C. § 2518(5). There is no such requirement for access to stored communications.

Finally, as also noted, the limitations as to the types of crimes that may be investigated through an intercept, *see* 18 U.S.C. § 2516, have no counterpart in Title II of the ECPA. *See, e.g.,* 18 U.S.C. § 2703(d) (co urt may order a provider of electronic communication service or remote computing service to disclose to a governmental entity the contents of a stored electronic communication on a showing that the information sought is "relevant to a legitimate law enforcement inquiry").

In light of the substantial differences between the statutory procedures and requirements for obtaining authorization to intercept electronic communications, on the one hand, and to gain access to the contents of stored electronic communications, on the other, it is most unlikely that Congress intended to require law enforcement officers to satisfy the more stringent requirements for an intercept in order to gain access to the contents of stored electronic communications.[8]

At oral argument, appellants contended (for the first time) that Title II's reference in § 2701(c) to § 2518 (which sets forth the procedures for the authorized interception of wire, oral, or electronic communications) reflects that Congress intended considerable overlap between Titles I and II of the ECPA.[9] As stated, § 2701(a) prohibits unauthorized access to stored wire or electronic communications. Subsection (c) of § 2701 sets forth the exceptions to liability under subsection (a), which include conduct authorized:

---

[8]The ECPA legislative history's explanation of the prohibitions regarding disclosure also persuades us of the soundness of *Turk*'s interpretation of "intercept" and our understanding of the distinctions Congress intended to draw between communications being transmitted and communications in electronic storage. In describing Title II's prohibitions against disclosure of the contents of stored communications, the Senate Report points out that § 2702(a) (part of Title II) "generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication *while in electronic storage* by that service to any person other than the addressee or intended recipient." S.Rep. No. 99-541, 97th Cong. 2nd Sess. 37, 1986 U.S.C.C.A.N. 3555, 3591 (emphasis added). It then goes on to state that § 2511(3) of the Wiretap Act, as amended by Title I of the ECPA, "prohibits such a provider from divulging the contents of a communication *while it is in transmission*". *Id.* (emphasis added).

[9]It goes without saying that we generally will not consider issues raised for the first time at oral argument. For this rare exception, the parties, as ordered, filed supplemental briefs on this point.

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or *2518* of this title.

18 U.S.C. § 2701(c) (emphasis added).[10]

Appellants overemphasize the significance of this reference to § 2518. As discussed in notes 6-7, *supra*, it is clear that Congress intended to treat wire communications differently from electronic communications. Access to stored electronic communications may be obtained pursuant to a search warrant, 18 U.S.C. § 2703; but, access to stored wire communications requires a court order pursuant to § 2518. Because § 2701 covers both stored wire and electronic communications, it was necessary in subsection (c) to refer to the different provisions authorizing access to each.

III.

For the foregoing reasons, the judgment is

AFFIRMED.

---

[10]Section 2703 sets forth the requirements for governmental access to the contents of *electronic* (but not wire) communications. For electronic communications that have been in electronic storage for 180 days or less, the government can gain access to the contents pursuant to a federal or state warrant. 18 U.S.C. § 2703(a). For communications that are maintained by a remote computing service and that have been in storage for more than 180 days, the government can gain access by obtaining a warrant, by administrative or grand jury subpoena, or by obtaining a court order pursuant to § 2703(d). 18 U.S.C. § 2703(b).

Section 2704 also deals only with *electronic* communications; it provides, *inter alia*, that a governmental entity may include in its subpoena or court order a requirement that the service provider create and maintain a duplicate of the contents of the electronic communications sought. 18 U.S.C. § 2704.