

36 F.3d 457

United States Court of Appeals,  
Fifth Circuit.

**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.

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. 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 freelance 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 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) [commonly referred to as the Stored Communications Act, "SCA"].

The district court held that the Secret Service 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) by the recipients, constitutes an "intercept" proscribed by 18 U.S.C. § 2511(1)(a).

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. 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.

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." 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. 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 [i.e., the SCA], 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). “Electronic storage” is defined as

- (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”.

[...]

Our conclusion is reinforced further by consideration of the fact that Title II of the ECPA [i.e., SCA] 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*, 33 F.3d 1434, 1444 (5th Cir.1994).

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. . . .

[...]

### III.

For the foregoing reasons, the judgment is  
AFFIRMED.