

302 F.3d 868

United States Court of Appeals,
Ninth Circuit.

Robert C. KONOP, Plaintiff-Appellant,
v.
HAWAIIAN AIRLINES, INC., Defendant-
Appellee.

Filed Aug. 23, 2002.

Before BOOCHEVER, REINHARDT, and
PAEZ, Circuit Judges.

Opinion by Judge BOOCHEVER; Partial
Concurrence and Partial Dissent by Judge
REINHARDT.

BOOCHEVER, Circuit Judge.

Robert Konop brought suit against his employer, Hawaiian Airlines, Inc. (“Hawaiian”), alleging that Hawaiian viewed Konop’s secure website without authorization, disclosed the contents of that website, and took other related actions in violation of the federal Wiretap Act, [and] the Stored Communications Act. . . . The district court granted summary judgment against Konop on all claims Konop appeals

. . . . We now affirm the judgment of the district court with respect to Konop’s Wiretap Act claims We reverse the district court’s judgment with respect to Konop’s claim[] under the Stored Communications Act

FACTS

Konop, a pilot for Hawaiian, created and maintained a website where he posted bulletins critical of his employer, its officers, and the incumbent union, Air Line Pilots Association (“ALPA”). Many of those criticisms related to Konop’s opposition to labor concessions which Hawaiian sought from ALPA. Because ALPA supported the concessions, Konop, via his

website, encouraged Hawaiian employees to consider alternative union representation.

Konop controlled access to his website by requiring visitors to log in with a user name and password. He created a list of people, mostly pilots and other employees of Hawaiian, who were eligible to access the website. Pilots Gene Wong and James Gardner were included on this list. Konop programmed the website to allow access when a person entered the name of an eligible person, created a password, and clicked the “SUBMIT” button on the screen, indicating acceptance of the terms and conditions of use. These terms and conditions prohibited any member of Hawaiian’s management from viewing the website and prohibited users from disclosing the website’s contents to anyone else.

In December 1995, Hawaiian vice president James Davis asked Wong for permission to use Wong’s name to access Konop’s website. Wong agreed. Davis claimed he was concerned about untruthful allegations that he believed Konop was making on the website. Wong had not previously logged into the website to create an account. When Davis accessed the website using Wong’s name, he presumably typed in Wong’s name, created a password, and clicked the “SUBMIT” button indicating acceptance of the terms and conditions.

Later that day, Konop received a call from the union chairman of ALPA, Reno Morella. Morella told Konop that Hawaiian president Bruce Nobles had contacted him regarding the contents of Konop’s website. Morella related that Nobles was upset by Konop’s accusations that Nobles was suspected of fraud and by other disparaging statements published on the website. From this conversation with Morella, Konop believed Nobles had obtained the contents of his website and was threatening to sue Konop for defamation based on statements contained on the website.

After speaking with Morella, Konop took his website offline for the remainder of the day. He placed it back online the next morning, however, without knowing how Nobles had obtained the information discussed in the phone call. Konop claims to have learned only later from the

examination of system logs that Davis had accessed the website using Wong's name.

In the meantime, Davis continued to view the website using Wong's name. Later, Davis also logged in with the name of another pilot, Gardner, who had similarly consented to Davis' use of his name. Through April 1996, Konop claims that his records indicate that Davis logged in over twenty times as Wong, and that Gardner or Davis logged in at least fourteen more times as Gardner.

[...]

DISCUSSION

The district court's grant of summary judgment is reviewed *de novo*. Viewing the evidence in the light most favorable to Konop, we must determine whether there are any genuine issues of material fact and whether the district court correctly applied the relevant substantive law.

I. Electronic Communications Privacy Act Claims

We first turn to the difficult task of determining whether Hawaiian violated either the Wiretap Act, 18 U.S.C. §§ 2510-2522 (2000) or the Stored Communications Act, 18 U.S.C. §§ 2701-2711 (2000),² when Davis accessed Konop's secure website. In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), which was intended to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to "address[] the interception of ... electronic communications." Title II of the ECPA created the Stored Communications Act (SCA), which was designed to "address[] access to stored wire and electronic communications and transactional records."

² The Wiretap Act and SCA have since been amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act).

As we have previously observed, the intersection of these two statutes "is a complex, often convoluted, area of the law." In the present case, the 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 like Konop's secure website. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain a confusing and uncertain area of the law.

A. The Internet and Secure Websites

The Internet is an international network of interconnected computers that allows millions of people to communicate and exchange information. The World Wide Web, the best known category of communication over the Internet, consists of a vast number of electronic documents stored in different computers all over the world. . . .

While most websites are public, many, such as Konop's, are restricted. For instance, some websites are password-protected, require a social security number, or require the user to purchase access by entering a credit card number. The legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards. The nature of the Internet, however, is such that if a user enters the appropriate information (password, social security number, etc.), it is nearly impossible to verify the true identity of that user.

We are confronted with such a situation here. Although Konop took certain steps to restrict the access of Davis and other managers to the website,³ Davis was nevertheless able to access the

³ Specifically, Konop configured the website to allow access when a person typed in the correct web address,

received the home page of his website, entered the name of an eligible person, created a password, and clicked the “SUBMIT” button indicating acceptance of the terms and conditions of use. In addition, Konop displayed the following language on the home page of his website:

This is the gateway for NEWS UPDATES and EDITORIAL COMMENTS directed only toward Hawaiian Air’s pilots and other employees, not including HAL management. By entering, you acknowledge and agree to the terms and conditions of use as specified below. You must read this entire page before entry. Others should simply find something else to do with their time.

If you are already a registered user, you may fill in your name along with the other information required below, then enter the system. If you want to visit the system, and you belong to the authorized group, you must supply the proper information before you will be allowed to enter. Make note of the password you enter for your first visit, otherwise future visits may be delayed. Visits by others will be strictly prohibited.

Beneath this language, Konop provided boxes for a person’s name, occupation, email address and password. Below the boxes were two buttons: one said “SUBMIT,” the other said “CLEAR.” The advisement continued:

All name and contact information will be kept strictly confidential. Any effort to defeat, compromise or violate the security of this website will be prosecuted to the fullest extent of the law.

WARNING!

The information contained herein is CONFIDENTIAL, and it is not intended for public dissemination! By requesting entry in the system, you must agree not to furnish any of the information contained herein to any other person or for any other use. Republication or redistribution of this information to any other person is strictly prohibited. Anyone found to disseminate this information to anyone other than those

website by entering the correct information, which was freely provided to Davis by individuals who were eligible to view the website.

B. Wiretap Act

Konop argues that Davis’ conduct constitutes an interception of an electronic communication in violation of the Wiretap Act. The Wiretap Act makes it an offense to “intentionally intercept [] ... any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a). We must therefore determine whether Konop’s website is an “electronic communication” and, if so, whether Davis “intercepted” that communication.

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.” *Id.* § 2510(12). As discussed above, website owners such as Konop transmit electronic documents to servers, where the documents are stored. If a user wishes to view the website, the user requests that the server transmit a copy of the document to the user’s computer. When the server sends the document to the user’s computer for viewing, a transfer of information from the website owner to the user has occurred. Although the website owner’s document does not go directly or immediately to the user, once a user accesses a website, information is transferred from the website owner to the user via one of the specified mediums. We therefore conclude that Konop’s website fits the definition of “electronic communication.”

The Wiretap Act, however, prohibits only “interceptions” of electronic communications. “Intercept” 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.” *Id.* § 2510(4). Standing alone, this

specifically named and allowed here will be banned from this website and held liable to prosecution for violation of the terms and conditions of use and for violation of this contract.

definition would seem to suggest that an individual “intercepts” an electronic communication merely by “acquiring” its contents, regardless of when or under what circumstances the acquisition occurs. Courts, however, have clarified that Congress intended a narrower definition of “intercept” with regard to electronic communications.

In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir.1994), the Fifth Circuit held that the government’s acquisition of email messages stored on an electronic bulletin board system, but not yet retrieved by the intended recipients, was not an “interception” under the Wiretap Act. . . .

We agree with the *Steve Jackson* . . . court[] that the narrow definition of “intercept” applies to electronic communications. Notably, Congress has since amended the Wiretap Act to eliminate storage from the definition of wire communication, *see* USA PATRIOT Act § 209, such that the textual distinction relied upon by the *Steve Jackson* . . . court[] no longer exists. This change, however, supports the analysis of those cases. 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. . . . 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. . . .

We therefore hold that for a website such as Konop’s to be “intercepted” in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage. This conclusion is consistent with the ordinary meaning of “intercept,” which is “to stop, seize, or interrupt in progress or course before arrival.” *Webster’s Ninth New Collegiate Dictionary* 630 (1985). More importantly, it 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.” S.Rep. No. 99-541 at 3 (emphasis added). The level of protection provided stored communications under the SCA is considerably less than that provided communications covered by the Wiretap Act. Section 2703(a) of the SCA details the procedures law enforcement must follow to access the contents of stored electronic communications, but these procedures are considerably less burdensome and less restrictive than those required to obtain a wiretap order under the Wiretap Act. *See Steve Jackson Games*, 36 F.3d at 463. Thus, if Konop’s position were correct and acquisition of a stored electronic 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. As the Fifth Circuit recognized in *Steve Jackson Games*, “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.” *Id.*

Because we conclude that Davis’ conduct did not constitute an “interception” of an electronic communication in violation of the Wiretap Act, we affirm the district court’s grant of summary judgment against Konop on his Wiretap Act claims.⁷

C. Stored Communications Act

Konop also argues that, by viewing his secure website, Davis accessed a stored electronic communication without authorization in violation of the SCA. The SCA makes it an offense to “intentionally access[] without authorization a facility through which an electronic communication service is provided . . . and thereby

⁷ Konop also claims that Hawaiian violated the Wiretap Act when Davis used and disclosed the contents of Konop’s website. As there was no interception under the Wiretap Act, this claim also fails.

obtain[] ... access to a wire or electronic communication while it is in electronic storage in such system.” 18 U.S.C. § 2701(a)(1). The SCA excepts from liability, however, “conduct authorized ... by a user of that service with respect to a communication of or intended for that user.” 18 U.S.C. § 2701(c)(2). The district court found that the exception in § 2701(c)(2) applied because Wong and Gardner consented to Davis’ use of Konop’s website. It therefore granted summary judgment to Hawaiian on the SCA claim.

The parties agree that the relevant “electronic communications service” is Konop’s website, and that the website was in “electronic storage.” In addition, for the purposes of this opinion, we accept the parties’ assumption that Davis’ conduct constituted “access without authorization” to “a facility through which an electronic communication service is provided.”

We therefore address only the narrow question of whether the district court properly found Hawaiian exempt from liability under § 2701(c)(2). Section 2701(c)(2) allows a person to authorize a third party’s access to an electronic communication if the person is 1) a “user” of the “service” and 2) the communication is “of or intended for that user.” See 18 U.S.C. § 2701(c)(2). A “user” is “any person or entity who—(A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use.” 18 U.S.C. § 2510(13).

The district court concluded that Wong and Gardner had the authority under § 2701(c)(2) to consent to Davis’ use of the website because Konop put Wong and Gardner on the list of eligible users. This conclusion is consistent with other parts of the Wiretap Act and the SCA which allow intended recipients of wire and electronic communications to authorize third parties to access those communications. In addition, there is some indication in the legislative history that Congress believed “addressees” or “intended recipients” of electronic communications would have the authority under the SCA to allow third parties

access to those communications. See H.R.Rep. No. 99-647, at 66-67 (explaining that “an addressee [of an electronic communication] may consent to the disclosure of a communication to any other person” and that “[a] person may be an ‘intended recipient’ of a communication ... even if he is not individually identified by name or otherwise”).

Nevertheless, the plain language of § 2701(c)(2) indicates that only a “user” of the service can authorize a third party’s access to the communication. The statute defines “user” as one who 1) *uses* the service and 2) is duly authorized to do so. Because the statutory language is unambiguous, it must control our construction of the statute, notwithstanding the legislative history. The statute does not define the word “use,” so we apply the ordinary definition, which is “to put into action or service, avail oneself of, employ.” *Webster’s* at 1299.

Based on the common definition of the word “use,” we cannot find any evidence in the record that Wong ever used Konop’s website. There is some evidence, however, that Gardner may have used the website, but it is unclear when that use occurred. At any rate, the district court did not make any findings on whether Wong and Gardner actually used Konop’s website—it simply assumed that Wong and Gardner, by virtue of being eligible to view the website, could authorize Davis’ access. The problem with this approach is that it essentially reads the “user” requirement out of § 2701(c)(2). Taking the facts in the light most favorable to Konop, we must assume that neither Wong nor Gardner was a “user” of the website at the time he authorized Davis to view it. We therefore reverse the district court’s grant of summary judgment to Hawaiian on Konop’s SCA claim.

[...]

CONCLUSION

For the foregoing reasons, we affirm the district court’s judgment with respect to Konop’s Wiretap Act claims We reverse the district court’s judgment on Konop’s Stored Communications Act claim[].