FOR PUBLICATION

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

ROBERT C. KONOP,

Plaintiff-Appellant,

v.

HAWAIIAN AIRLINES, INC., Defendant-Appellee.

No. 99-55106

D.C. No. CV-96-04898-SJL (JGx)

OPINION

Appeal from the United States District Court for the Central District of California J. Spencer Letts, District Judge, Presiding

Argued and Submitted June 8, 2000--Pasadena, California

Filed January 8, 2001

Before: Robert Boochever, Stephen Reinhardt, and Richard A. Paez, Circuit Judges.

Opinion by Judge Boochever

215	
216	
217	
218	
219	

COUNSEL

Robert C. Konop, Pro se, Playa del Rey, California, plaintiffappellant.

Marianne Shipp, Gibson, Dunn & Crutcher, Irvine, California, for the defendant-appellee.

OPINION

BOOCHEVER, Circuit Judge:

Robert Konop ("Konop") appeals: (1) the district court's grant of summary judgment against Konop on his claim that Hawaiian Airlines, Inc. ("Hawaiian") violated the Wiretap Act, 18 U.S.C. §§ 2510-2520, and the Stored Communications Act, 18 U.S.C. §§ 2701-2710, by viewing Konop's secure website under false pretenses; (2) the district court's grant of summary judgment against Konop on his claims that Hawaiian violated the Railway Labor Act, 45 U.S.C.§ 152, by gaining unauthorized access to and disclosing the contents of Konop's website; and (3) the district court's judgment, following a bench trial, entered against Konop on his claim that Hawaiian suspended him in retaliation for his website activities in violation of the Railway Labor Act.

We conclude that, with respect to Konop's claims under the Wiretap Act and the Stored Communications Act, and his statutory claims under the Railway Labor Act which were dismissed on summary judgment, Konop has raised a triable

220

issue of fact. We reverse and remand with respect to those claims. As to Konop's retaliation claim under the Railway Labor Act, which proceeded to trial, we affirm the district court's judgment.

FACTS

Konop, a pilot for Hawaiian, 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 giving management concessions to the existing collective bargaining agreement, Konop encouraged others via his website to consider alternative union representation.

Konop controlled access to his website by requiring visitors to log in with a user name and password. Konop provided user names to certain Hawaiian employees, but not to managers or union representatives. To obtain a password and view the site, an eligible employee had to register and consent to an agreement not to disclose the site's contents.

About December 14, 1995, Hawaiian vice president James Davis ("Davis") contacted Hawaiian pilot Gene Wong ("Wong") and asked permission to use Wong's name to access Konop's site. Davis claimed he was concerned about untruthful allegations that he believed Konop was making on the site. Wong had never logged into the site to create an account, and had never agreed to Konop's terms of use and nondisclosure conditions. When Davis accessed the site using Wong's name, he presumably clicked a button indicating that he was Wong and agreed to Konop's 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 ("Nobles") had contacted

221

him regarding the contents of Konop's website. Morella related that Nobles was upset by accusations that Nobles was suspected of fraud and by other disparaging statements published by Konop. From this conversation with Morella, Konop believed Nobles had obtained the contents of his website and had threatened to sue Konop for defamation based on statements contained on the website.

After speaking with Morella, Konop took down his website for the remainder of the day. He placed it back online the next morning, however, without having learned 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 site using Wong's name.

In the meantime, Davis continued to view the site using Wong's name. Later, Davis also logged in with the name of another pilot, James Gardner ("Gardner"), who had similarly consented to Davis' use of his name. Through April 1, 1996, Konop claims that his records indicate over twenty log-ins by Davis (as Wong) and at least fourteen more by Gardner or Davis (as Gardner).

Konop filed suit alleging numerous state law tort claims along with labor and wiretap claims arising out of Davis' viewing and use of his website. Konop also brought claims arising out of a medical suspension that he alleges was imposed in retaliation for his opposition to proposed labor concessions. The district court granted summary judgment to Hawaiian on all but this last claim of retaliatory suspension, and entered judgment against Konop on that claim after a short bench trial.

On appeal, Konop argues that the district court erred in granting summary judgment for Hawaiian on his claims that Davis' unauthorized viewing of the website violated the Wiretap Act, 18 U.S.C. §§ 2510-2520, and the Stored Communications Act, 18 U.S.C. §§ 2701-2710. Konop also argues that

222

Hawaiian was not entitled to summary judgment on his claim that the acquisition and subsequent use of the site's contents by Davis and Nobles was unlawful under the Railway Labor Act, 45 U.S.C. § 152. Finally, Konop challenges the judgment entered against him on his retaliatory suspension claim, also brought under the RLA, on the ground that the district court improperly quashed subpoenas for witnesses that Konop sought to have testify on his behalf.

ANALYSIS

I. Wiretap Act and Stored Communications Act Claims.

Konop argues that Hawaiian vice president Davis, by accessing Konop's secure website under false pretenses, intercepted an electronic communication in violation of the Wiretap Act, as amended by the Electronic Communications Privacy Act, and accessed an electronic communications facility in violation of the Stored Communications Act.

Protection against eavesdropping on modern electronic communications was added to the Wiretap Act and enacted in the Stored Communications Act by the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 ("ECPA"). Title I of the ECPA amended the Wiretap Act to prohibit unauthorized "interception" of "electronic communications." 18 U.S.C. § 2511. Title II of the ECPA created the Stored Communications Act, which prohibits unauthorized "access" to "a facility through which an electronic communication service is provided." <u>Id.</u> at § 2701.

Civil damages are substantially greater under the Wiretap Act than under the Stored Communications Act. <u>Compare</u> 18 U.S.C. § 2520 <u>with</u> 18 U.S.C. § 2707. As such, it is a significant question whether using false pretenses to view a website constitutes unlawful interception in violation of the Wiretap Act, or unlawful access in violation of the Stored

223

Communications Act, or both. It is also one of first impression.

The Fifth Circuit has characterized the Wiretap Act as "famous (if not infamous) for its lack of clarity." <u>Steve Jackson</u> <u>Games, Inc. v. United States Secret Serv.</u>, 36 F.3d 457, 462 (5th Cir. 1994). We have noted that the Fifth Circuit "might have put the matter too mildly. Indeed, the intersection of the Wiretap Act and the Stored Communications Act is a complex, often convoluted, area of the law." <u>United States v.</u> <u>Smith</u>, 155 F.3d 1051, 1055 (9th Cir. 1998), <u>cert. denied</u>, 525 U.S. 1071 (1999) (citations omitted).

A. Enactment and Interpretation of Wiretap Act.

Our way through this statutory thicket begins with the Wiretap Act as it was written and interpreted prior to its amendment by the ECPA. As originally enacted, the Wiretap Act sanctioned "any person who . . . willfully intercepts, endeavors to intercept, or procures any other person to intercept, any wire or oral communication. . . . " 18 U.S.C.A. § 2511(a) (1970). The Wiretap Act defined "wire communication" as "any communication 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." Id. at § 2510(1). An "oral communication" meant "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." Id. at § 2510(2). "Intercept" was defined as "the aural acquisition of the contents of any wire or oral communication through the use of any

electronic, mechanical, or other device." Id. at § 2510(4).

The term "intercept" received a narrow construction in the influential case of <u>United States v. Turk</u>, 526 F.2d 654 (5th Cir. 1976). At issue in <u>Turk</u> was whether police intercepted a communication when they played back a tape of a telephone call that had been previously recorded by a third party. The

224

Fifth Circuit held no unlawful interception occurred. The court explained that the logic and policy of the Wiretap Act "require participation by the one charged with an`interception' in the contemporaneous acquisition of the communication." <u>Id.</u> at 658.1

A requirement that transmission and acquisition be contemporaneous would be fatal to Konop's claim that Hawaiian violated the Wiretap Act by gaining unauthorized access to his website. There is ordinarily a period of latency between the initial transmission of information for storage on a web server, and the acquisition of that information by its recipients. If interception requires that acquisition and transmission occur contemporaneously, then unauthorized downloading of information stored on a web server cannot be interception.

B. Enactment and Interpretation of ECPA.

The law by which such acts of downloading are judged has changed significantly, however, since <u>Turk</u> read its contemporaneity requirement into the Wiretap Act. The variety of acts constituting interception was expanded by Title I of the ECPA from "aural acquisition" of protected communications to "aural <u>or other</u> acquisition" of protected communications. 18 U.S.C. § 2510(4) (1986) (emphasis added). The ECPA also reclassified and redefined the types of communications pro-

1 The court reasoned:

The words `acquisition . . . through the use of any . . . device' suggest that the central concern is with the activity engaged in at the time of the oral communication which causes such communication to be overheard by uninvited listeners. If a person secrets a recorder in a room and thereby records a conversation between two others, an `acquisition' occurs at the time the recording is made. . . . [If] a new and different `aural acquisition' occurs each time a recording of an oral communication is replayed[, it] would

mean that innumerable `interceptions,' and thus violations of the Act, could follow from a single recording.

Turk, 526 F.2d at 658.

225

tected from interception. The definition of "wire communication" was narrowed from "any communication " made over the wires to "any <u>aural</u> transfer" made over the wires, <u>id.</u> at § 2510(1) (emphasis added), but the definition was also expanded to include "any electronic storage of such communication." <u>Id.</u> In addition, the ECPA added a catch-all category of "electronic communication" defined, with certain exceptions, 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. . . ." <u>Id.</u> at § 2510(12).

In <u>United States v. Smith</u>, 155 F.3d 1051 (9th Cir. 1998), <u>cert. denied</u>, 525 U.S. 1071 (1999), we considered the effect of these amendments on the meaning of "intercept " under the Wiretap Act. We also considered the relation of interception to the new offense of unauthorized access to stored communications facilities under the Stored Communications Act. At issue in <u>Smith</u> was whether the Wiretap Act required suppression of a tape of phone messages retrieved without authorization from the defendant's voice mailbox.

The government argued in <u>Smith</u> that the ECPA was not intended to repudiate <u>Turk</u>'s requirement that acquisition must be contemporaneous with transmission to constitute interception under the Wiretap Act. Instead, maintained the government, Congress intended ECPA Titles I and II to establish a distinction between the strong protection of communications in transmission afforded by the Wiretap Act (which provides for suppression of unauthorized intercepted wire communications, <u>see</u> 18 U.S.C. § 2518(10)(a)), and the weaker protection of communications in storage afforded by the Stored Communications Act (which does not provide for suppression, <u>see</u> 18 U.S.C. § 2708). <u>See Smith</u>, 155 F.3d at 1056-57.

Rejecting these arguments, we found <u>Turk's narrow defini-</u> tion of "intercept" difficult to square with the amended Wiretap Act's definition of "wire communication." If "the term `intercept' necessarily implies contemporaneous acquisition, then the portion of \$ 2510(1) that specifically defines `wire communication' as including stored information is rendered essentially meaningless because messages in electronic storage cannot, by definition, be acquired contemporaneously." <u>Id.</u> at 1058.

The terms "intercept" under the Wiretap Act and "access" under the Stored Communications Act, we concluded, are not "temporally different, with the former, but not the latter, requiring contemporaneity; rather the terms are conceptually, or qualitatively, different." <u>Id.</u>

The word "intercept" entails actually acquiring the contents of a communication, whereas the word "access" merely involves being in position to acquire the contents of a communication. In other words, "access" is, for all intents and purposes, a lesser included offense (or tort, as the case may be) of "interception."

<u>Id.</u> (alterations omitted). Under this scheme, the Wiretap Act and the Stored Communications Act do not discriminate between wire communications based on whether they are in transit or storage, but instead attach different consequences to invasions of privacy based on degrees of intrusion.

If <u>Smith</u>'s definition of "intercept" applies to electronic communications, then a person's unauthorized acquisition of the contents of a secure website would constitute an interception in violation of the Wiretap Act. The only circuit court to have decided the issue, however, has held that "intercept" does not mean the same thing when applied to electronic communications as when applied to wire communications. The Fifth Circuit, in <u>Steve Jackson Games v. United States Secret</u> <u>Service</u>, 36 F.3d 457 (5th Cir. 1994), concluded that, with respect to electronic communications, Congress intended the ECPA to carry forward the <u>Turk</u> definition of"intercept" as

227

contemporaneous acquisition. The court noted that the ECPA defines "electronic communication" as a "transfer" of signals, and that "unlike the definition of `wire communication,' the definition of `electronic communication' does not include electronic storage of such communications." Id. at 461.

We endorsed the reasoning of <u>Steve Jackson Games</u> in <u>Smith</u>, and this would ordinarily end our inquiry. Though electronic communications were not at issue in <u>Smith</u>, and our endorsement of <u>Steve Jackson Games</u> in that case was therefore not essential to our holding, we do not lightly reconsider persuasive dicta, even if they do not bind us. But confronting the issue squarely for the first time in this case, we find ourselves unpersuaded that Congress intended one definition of "intercept" to govern "wire communications, " and another to govern "electronic communications."

C. Acquisition Need Not Be Contemporaneous with Transmission.

We first note that the Wiretap Act provides but a single definition of "intercept," and that definition does not expressly contain or suggest the contemporaneity requirement read into it by <u>Turk</u>. See 18 U.S.C.§ 2510(4). Though silence is consistent with the presumption that Congress acts with awareness of prevailing judicial constructions when it reenacts or amends a law, see Native Village of Venetie I.R.A. Council v. State of Alaska, 944 F.2d 548, 554 (9th Cir. 1991), the <u>Turk</u> contemporaneity rule had not gained wide currency when Congress passed the ECPA.2 Nor does any reference to <u>Turk</u> or contemporaneity appear in the statute's legislative history.3

2 We have found only one apparent adoption of <u>Turk</u>'s reading of "intercept"-- and that in passing -- by a circuit court prior to the ECPA's passage on October 21, 1986. <u>See U.S. v. Shields</u>, 675 F.2d 1152, 1156 (11th Cir. 1982).

3 Intent to carry forward the rule in <u>Turk</u> is suggested at first glance by the pronouncement in the Senate Report on the ECPA that the "definition

228

The textual basis for the Fifth Circuit's conclusion in <u>Steve</u> <u>Jackson Games</u>, that stored electronic communications are not protected from interception under the Wiretap Act, is that the statute defines "electronic communication" as a "transfer" of information without expressly including storage of information. In contrast, the corresponding definition of "wire communication" does expressly include storage of information. It is plausible, however, that the express inclusion of stored communications in the definition of "wire communication" was intended not for purposes of contrast, but for clarification. The language was a late subcommittee addition to the draft ECPA to ensure that voice mail and similar stored wire communications would be protected as wire communications. <u>See S. Rep. No. 99-541, 99th Cong., 2d Sess. (1986),</u> <u>reprinted in</u> 1986 U.S.C.C.A.N. 3555, 3566.

This addition was necessary because, as one commentator has noted, wire communication does not necessarily include storage of that communication. Tatsuya Akamine, <u>Proposal</u> for a Fair Statutory Interpretation: E-Mail Stored in a Service <u>Provider Computer Is Subject to an Interception Under the</u> <u>Federal Wiretap Act</u>, 7 J.L. & Pol'y 519, 550-51 (1999). Electronic communication, on the other hand, cannot successfully be completed without being stored. <u>Id.</u> at 561 ("`Electronic storage' is a part of the entire communication process, and thus, the definition of `electronic communication' impliedly covers `electronic storage,' whether or not that definition includes the specific reference to `electronic storage.' "). Therefore, it was not necessary for Congress to explicitly include the concept of storage in its definition of electronic communication.

of `intercept' under current law is retained with respect to wire and oral communications except that the term `or other' is inserted after `aural.' " S. Rep. No. 99-541, 99th Cong., 2d Sess. (1986), <u>reprinted in</u> 1986 U.S.C.C.A.N. 3555, 3567. But the caveat referring to the insertion of text in the statute indicates that "current law" was meant to denote the text of the statute itself, and not necessarily any particular judicial interpretation of "intercept."

229

We are wary of attributing subtle purpose and indirection to the language of a statute that appears to have been crafted with little of either. In other instances, where Congress has provided lesser protection for electronic communications, it has done so straightforwardly, and for discernable reasons. Electronic communication service providers must divulge communications in certain circumstances as an incident to their services, for example, and the Wiretap Act expressly permits them to do so. See 18 U.S.C. § 2511(3)(b); 1986 U.S.C.C.A.N. at 3580. No expectation of privacy attaches to electronic communications made available through facilities readily available to the public, and interception of such communications is also expressly permitted under the Wiretap Act. See 18 U.S.C. § 2511(2)(g)(i). A suggestion by the Justice Department resulted in a provision emphasizing the unavailability of suppression, where not constitutionally

required, as a remedy for unlawful interception of electronic communications. <u>See</u> 18 U.S.C. § 2518(10)(c); 1986 U.S.C.C.A.N. at 3577.

No similarly straightforward provision of the Wiretap Act affords stored electronic communications a lesser degree of protection from interception than stored wire communications. We know of no reason why Congress might have wished to do so. An electronic communication in storage is no more or less private than an electronic communication in transmission. Distinguishing between the two for purposes of protection from interception is "irrational" and "an insupportable result given Congress' emphasis of individual privacy rights during passage of the ECPA." Thomas Greenberg, <u>E-Mail and Voice Mail: Employee Privacy and the Federal</u> Wiretap Statute, 44 Am. U. L. Rev. 219, 248-49 (1994).

A 1996 amendment to the Wiretap Act also suggests Congress understood electronic communications to include stored communications unless specified otherwise. The amendment appended a proviso to the Wiretap Act's definition by specifying: "`electronic communication'... does not include ...

230

electronic funds transfer information stored by a financial institution. . . ." 18 U.S.C. § 2510(12)(D). The exclusion of certain kinds of stored information from the definition of electronic communication implies that Congress understood the term in ordinary circumstances to include stored information. This understanding is stated expressly in the conference report to the amendment: "[The amendment] will allow law enforcement to obtain [stored] bank records through the usual grand jury subpoena, or other court order procedure, <u>without requiring a wiretap order</u> for these purposes." H.R. Conf. Rep. No. 104-518, 104th Cong., 2d Sess. (1996), <u>reprinted in</u> 1996 U.S.C.C.A.N. 944, 956-57 (emphasis added). It is perfectly clear that the framers of the Wiretap Act's current definition of "electronic communication" understood that term to include communications in transit and storage alike.

We believe that Congress intended the ECPA to eliminate distinctions between protection of private communications based on arbitrary features of the technology used for transmission. Reflecting on technological developments of the 1980s with which the old Wiretap Act had failed to keep pace, the Senate Report on the ECPA lamented: Today, we have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing. A phone call may be carried by wire, by microwave or fiber optics. It can be transmitted in the form of digitized voice, data or video. Since the divestiture of AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services. It does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major

231 U.S. corporations today, would not be covered by the statute.

1986 U.S.C.C.A.N. at 3556-57. It makes no more sense that a private message expressed in a digitized voice recording stored in a voice mailbox should be protected from interception, but the same words expressed in an e-mail stored in an electronic post office pending delivery should not.

We conclude that it would be equally senseless to hold that Konop's messages to his fellow pilots would have been protected from interception had he recorded them and delivered them through a secure voice bulletin board accessible by telephone, but not when he set them down in electronic text and delivered them through a secure web server accessible by a personal computer. We hold that the Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit.

D. Exceptions.

Our holding does not mean that an unlawful interception occurs every time someone views a web page. Among the Wiretap Act's many exceptions, one provides: "It shall not be unlawful . . . for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). This exception does not exempt Davis' conduct, however, because Konop's website was configured to require user names and passwords that were available only to certain nonmanagement Hawaiian employees.

Another exception provides that it is not a violation of the Wiretap Act to intercept an electronic communication where "one of the parties to the communication has given prior consent to such interception...." Id. at 2511(2)(d). Hawaiian claims that Wong was an authorized user of

232

Konop's website whose consent entitled Davis to view its contents. Konop does not dispute that Wong, as a Hawaiian pilot, was able to set up an account by identifying himself, creating a password, and agreeing to the website's terms of use, which restricted disclosure of its contents to any other person. But Hawaiian concedes that Wong never actually took these steps before Davis used his name to view Konop's website.

It does not follow from the fact that Wong was eligible to gain access to the website that he was a "party " to its contents. Neither the statute nor the case law hazards a definition of "parties to the communication," but Webster's relevantly defines "party" as "a person or group <u>participating</u> in an action or affair." <u>Merriam Webster's Collegiate Dictionary</u> 1332 (Deluxe ed. 1998) (emphasis added). Never having accepted Konop's offer to furnish access to the website in exchange for a promise of confidentiality, Wong never actually participated in any communication with Konop.

"[P]arties to the communication" might also be construed to include not just the actual authorized recipients of a communication, but also its intended recipients. This usage would be consistent with portions of the Wiretap Act that, for example, permit service providers to divulge the contents of communications "with the lawful consent of the originator or any addressee or intended recipient of such communication." 18 U.S.C. § 2511(3)(b)(ii); <u>see also id.</u> at § 2702(b)(3) (permitting divulgence of stored communications "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service.").

Yet it would still be a mistake under this broader definition to characterize Wong as an intended recipient of the contents of Konop's website merely because Konop included Wong's name on the list of pilots eligible to create passwords and log in. The additional steps that one with such an account

233

had to take in order to gain access to the site indicate that the intended recipients of Konop's website contents were not all Hawaiian pilots for whom such provisional accounts had been provided, but only those who agreed to Konop's terms of use. Because Wong was at most a potential recipient at the time that Davis initially viewed the contents of the website, Wong was not one of the "parties to the communication " of the website's contents under even a broad construction of the term.

Hawaiian claims alternatively that, even if Wong's consent to view the website were not effective, Davis later received consent to view the site from another Hawaiian pilot, Gardner. The circumstances under which Gardner obtained a password for Davis are not at all clear, and may require factual development on remand. Gardner did not in any case give Davis "<u>prior</u> consent," <u>id.</u> at§ 2511(2)(d), that could excuse Davis' earlier acts of interception using Wong's log-in account.

Hawaiian also argues that Konop himself gave implied consent to viewing by Davis when he failed to disable Wong's and Gardner's names after learning of Davis' actions. Consent "may be implied in fact from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance." <u>U.S. v. Van Poyck</u>, 77 F.3d 285, 292 (9th Cir. 1996) (quotations omitted).

> The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private. And the ultimate determination must proceed in light of the prophylactic purpose of [the Wiretap Act]--a purpose which suggests that consent should not casually be inferred.

234

<u>Griggs-Ryan v. Smith</u>, 904 F.2d 112, 117 (1st Cir. 1990) (cited in <u>Van Poyck</u>, 77 F.3d at 292). The existence of implied consent is a question of fact that can be resolved on summary judgment only when "the events material to the issue of prior consent are straightforward, hence effectively uncontroverted." <u>Id.</u> at 117.

Here, Konop explains that although he suspected that Hawaiian management accessed his system shortly after the first incursion occurred, he did not know how and by whom this had been accomplished until months later. The circumstances surrounding Konop's efforts to restrict access to his website are sufficiently open to interpretation that the question of implied consent should have gone to the finder of fact. In any event, like Gardner's after-the-fact consent, any implied consent by Konop was not given prior to Davis' initial visit to the website.

E. Conclusion.

The contents of secure websites are "electronic communications" in intermediate storage that are protected from unauthorized interception under the Wiretap Act. Konop has raised material issues of fact whether Davis had appropriate consent to view Konop's website. Because Konop has raised material issues of fact regarding his claims of interception under the Wiretap Act, he has also raised material issues of fact regarding his claims that Davis committed the lesser included offense of unauthorized access in violation of the Stored Communications Act. The district court erred in granting summary judgment for Hawaiian on Konop's Wiretap Act and Stored Communications Act claims.

II. Railway Labor Act Claims.

Konop appeals the district court's grant of summary judgment to Hawaiian on his claims under the Railway Labor Act, 45 U.S.C. §§ 151-188 ("RLA"). The RLA prohibits "in-

235

terference, influence, or coercion by either party over the designation of representatives by the other." 45 U.S.C. § 152 (Third). It also declares "it shall be unlawful for any carrier to interfere in any way with the organization of its employees, or to use the funds of the carrier in maintaining or assisting or contributing to any labor organization, labor representative, or other agency of collective bargaining. . . ." <u>Id.</u> at § 152 (Fourth). Konop asserts three claims under 45 U.S.C. §§ 152 (Third) and (Fourth) of the RLA. First, Konop alleges that Hawaiian interfered with his organizing efforts by viewing his website under false pretenses. Second, Konop alleges that Hawaiian wrongfully assisted a labor group by disclosing the contents of Konop's website to a union leader who supported the concessionary contract. Third, Konop alleges that Hawaiian engaged in coercion and intimidation by threatening to file a defamation suit against Konop based on statements contained on Konop's website. The district court dismissed these claims on the alternative grounds that it lacked jurisdiction over the RLA claims, and that Konop failed to support them with evidence sufficient to withstand summary judgment.

A. Subject Matter Jurisdiction.

Federal courts lack subject matter jurisdiction over disputes which are "grounded in the collective bargaining agreement" and "involve controversies over the meaning of an existing collective bargaining agreement in a particular fact situation." <u>Hawaiian Airlines, Inc. v. Norris</u>, 512 U.S. 246, 252-53, 256 (1994) (internal alterations omitted). Such disputes, labeled "minor" disputes under the RLA, are subject to mandatory arbitration. <u>Id.</u> at 253. Hawaiian argues, and the district court agreed, that Konop's RLA claims are grounded in the collective bargaining agreement ("CBA") and, therefore, subject to mandatory arbitration. We disagree.

In <u>Fennessy v. Southwest Airlines</u>, 91 F.3d 1359 (9th Cir. 1996), we addressed whether the district court had jurisdiction

236

over the plaintiff's statutory claim under the RLA. The plaintiff in <u>Fennessy</u> alleged that the carrier violated 45 U.S.C. § 152 (Fourth) by terminating his employment in retaliation for his efforts to replace the existing union. <u>Id.</u> at 1360-61. We held that "because his claim is based on a statutory provision rather than on the collective bargaining contract, it is not a minor dispute that must be brought to [arbitration]; it is a statutory claim that he may bring directly in district court." <u>Id.</u> at 1362. The plaintiff's unsuccessful arbitration of a related contractual claim under the CBA did not alter this conclusion. Because the statutory claims were not "grounded in the collective-bargaining agreement," and the statutory rights were "independent of the CBA," we found the district court had jurisdiction. <u>Id.</u> Hawaiian argues that, unlike the statutory claim in <u>Fen-</u><u>nessy</u>, Konop's statutory claims are grounded in and dependent on the CBA. To support this position, Hawaiian focuses on conduct which Konop alleged as violating the CBA. Specifically, in the RLA section of Konop's complaint, Konop alleges that Hawaiian violated the CBA by suspending him from work, reducing his employee benefits, requiring him to submit to physical and psychological testing, and giving certain pilots paid opportunities to campaign in favor of the concessionary contract.

On appeal, however, Konop does not argue that the above RLA claims fall within this court's jurisdiction. Instead, the RLA claims Konop presses on appeal involve allegations that Hawaiian violated the RLA by (1) accessing his website under false pretenses, (2) disclosing the website's contents to the rival union faction, and (3) threatening to sue Konop for defamation based on statements on the website. Hawaiian never explains how these RLA claims are grounded in the CBA, except to say that Konop merely presents them as a precursor to the alleged CBA violations. Nothing, however, requires this cramped reading of Konop's allegations. Konop, like the plaintiff in <u>Fennessy</u>, presents his statutory claims as

237

independent violations of the RLA. The RLA statutory claims Konop presses on appeal in no way depend upon a finding that Hawaiian, at some later time, violated Konop's contractual rights under the CBA.

Accordingly, we hold that the RLA claims which Konop presses on appeal are not grounded in the CBA, are not subject to mandatory arbitration and, therefore, fall within the court's jurisdiction.

B. Protected Activity.

Hawaiian contends that even if Hawaiian managers accessed Konop's website under false pretenses, conveyed this information to a rival union leader, and threatened to sue Konop for defamation, such conduct would not violate the RLA because it would not interfere with any protected organizing activity. The organizing activity in which Konop engaged principally involved the publication of articles on a secure website. As discussed above, only employees who agreed to the confidentiality terms were allowed access; managers and union representatives were categorically excluded. Konop's website publication vigorously criticized managers of Hawaiian and their proposal for wage concessions to the existing collective bargaining agreement. Because the incumbent union, Air Line Pilots Association, supported the concessionary contract, Konop sought to encourage consideration of alternative union representation.

There is no dispute that Konop's website publication would ordinarily constitute protected union organizing activity under the RLA. Hawaiian argues, however, that Konop forfeited any protection he would otherwise enjoy because his articles contained malicious, defamatory and insulting material known to be false. In <u>Linn v. United Plant Guard Workers of Amer., Local 114</u>, 383 U.S. 53, 61 (1966) ("<u>Linn</u>"), the Supreme Court held that a party forfeits his protection under the National Labor Relations Act ("NLRA") by "circulating

238

defamatory or insulting material known to be false. "<u>See also</u> <u>Old Dominion Branch No. 496, Nat'l Ass'n of Letter Carriers</u> <u>v. Austin</u>, 418 U.S. 264, 286 (1974) ("<u>Letter Carriers</u>"); <u>San</u> <u>Antonio Comm. Hosp. v. Southern Cal. Dist. Council of Car-</u> <u>penters</u>, 125 F.3d 1230, 1237 (9th Cir. 1997). **4**

While Hawaiian claims that many of the statements on Konop's website were defamatory and known to be false, it fails to identify the challenged statements in the"Discussion" section of its brief. Presumably, Hawaiian is referring to the alleged false statements contained in the "Facts " section. There, Hawaiian indicates that Konop published the following false statements: (1) Nobles does his "dirty work. . . like the Nazis during World War II"; (2) "Soviet Negotiating Style Essential to Nobles Plan!"; (3) Nobles is "one incompetent at the top"; (4) Nobles "has little skill and little ability with people In fact, with as few skills as Nobles possesses, it is difficult to imagine how he got this far"; and (5) "Nobles Suspected in Fraud!" and "Hawaiian Air president, Bruce Nobles, is the prime suspect in an alleged fraud which took place in 1991."

The first two statements, referencing the Nazis and Soviets, are simply "rhetorical hyperbole" protected by federal labor laws. <u>See Letter Carriers</u>, 418 U.S. at 286 ("rhetorical hyperbole" protected). The second two statements, commenting on Nobles' competence and people skills, are opinion also protected by federal labor laws. <u>See id.</u> at 284 (opinion protected); <u>San Antonio Comm. Hosp.</u>, 125 F.3d at 1237 (same). Konop did not forfeit his protection under the Railway Labor Act, as Hawaiian suggests, simply by publish-

4 While employers covered under the RLA are not subject to the provisions of the NLRA, courts look to the NLRA and the cases interpreting it for guidance in interpreting the RLA. <u>Brotherhood of Railroad Trainmen v. Jacksonville Terminal Co.</u>, 394 U.S. 369, 383 (1969). We see no reason why the rule announced in <u>Linn</u>, 383 U.S. at 61, regarding protected activities, should not apply in the context of the RLA.

239

ing statements that were critical of and insulting to Nobles. "`[F]ederal law gives a union license to use intemperate, abusive, or <u>insulting</u> language without fear of restraint or penalty. ...'" <u>San Antonio Comm. Hosp.</u>, 125 F.3d at 1235 (quoting <u>Letter Carriers</u>, 418 U.S. at 283) (emphasis added); <u>see also</u> <u>Linn</u>, 383 U.S. at 58 ("representation campaigns are frequently characterized by bitter and extreme charges, countercharges, unfounded rumors, vituperations, personal accusations, misrepresentations and distortions").**5**

With respect to the final challenged statement, indicating that Nobles was suspected of fraud, Hawaiian fails to argue or present any evidence that Konop published the statement with knowledge of its falsity or with reckless disregard for the truth. Federal labor law protects even false and defamatory statements unless such statements are made with actual malice -- <u>i.e.</u>, knowledge of falsity or with reckless disregard for the truth. <u>See Letter Carriers</u>, 418 U.S. at 281; <u>Linn</u>, 383 U.S. at 61 (protection under labor law maintained"even though the statements are erroneous and defame one of the parties to the dispute"). With no evidence or argument that Konop acted with actual malice, Hawaiian cannot demonstrate as a matter of law that Konop forfeited his protection under the RLA.

<u>NLRB v. Pincus Brothers, Inc.</u>, 620 F.2d 367 (3rd Cir. 1980), upon which Hawaiian principally relies, provides little support for Hawaiian's position. In <u>Pincus Brothers</u>, the Third

5 We recognize that some organizing activity may be "so flagrant, violent or extreme" or so "egregious," "opprobrious," "offensive," "obscene" or "wholly unjustified" that it loses the protection of the RLA. <u>See Reef</u> <u>Indust., Inc. v. NLRB</u>, 952 F.2d 830, 837 (5th Cir. 1991); <u>Timekeeping</u> Sys., Inc. and Lawrence Leinweber, 323 N.L.R.B. 244, 248-50 (1997). It is not clear whether Hawaiian is contending that Konop's conduct falls within one of these more amorphous standards. Assuming Hawaiian does so contend, we nevertheless find Hawaiian has failed to demonstrate that, as a matter of law, Konop's activities were so intolerable as to lose their protection under the RLA.

240

Circuit merely concluded that, under the particular facts of that case, it was "at least arguable" that the employee published a defamatory statement known to be false. <u>Id.</u> at 376. For Hawaiian to prevail on summary judgment, however, it must do more than show it is "at least arguable " that Konop knew the challenged statement was false. It must demonstrate this as a matter of law. As Hawaiian presents no evidence or argument that Konop acted with the requisite malice, Hawaiian falls short of demonstrating that Konop's activity was unprotected as a matter of law.

Accordingly, we find that Konop has raised a material triable issue of fact with respect to whether the development and maintenance of his website constituted protected activity under the Railway Labor Act.

C. Specific Violations.

Konop argues that Hawaiian managers: (1) interfered with Konop's organizing efforts by viewing the website under false pretenses, (2) wrongfully supported one labor group in favor of another by informing the opposing labor faction of the website's contents, and (3) engaged in coercion and intimidation by threatening to sue Konop for defamation, all in violation of the Railway Labor Act. Hawaiian argues, and the district court agreed, that Konop failed to present sufficient evidence to withstand summary judgment on these claims. We disagree.

1. Access of Website.

Konop argues that Davis interfered with Konop's organizing efforts by viewing the website under false pretenses. Absent a legitimate justification, employers are generally prohibited from engaging in surveillance of union organizing activities. <u>California Acrylic Indus., Inc. v. NLRB</u>, 150 F.3d 1095, 1100 (9th Cir. 1998). The reason for this general proscription is that employer surveillance"tends to create 241

fear among employees of future reprisal" and, thus, "chills an employee's freedom to exercise" his rights under federal labor law. <u>Id.</u> at 1099.

In <u>NLRB v. Unbelievable, Inc.</u>, 71 F.3d 1434 (9th Cir. 1995), we upheld the Board's finding that the employer "engaged in unfair labor practices by eavesdropping on private conversations between employees and [a] Union representative," which occurred in the employee break room. Id. at 1438-39. We see no principled distinction between the employer's eavesdropping in <u>Unbelievable</u> and Hawaiian's access of Konop's secure website. This conclusion is supported by our determination that Hawaiian's access of Konop's website raises a triable issue with respect to Konop's claims under the Wire Tap Act (as amended by the Electronic Communications Privacy Act) and the Stored Communications Act.

Hawaiian suggests that it had a legitimate reason to access Konop's website; namely, to identify and correct any false or misleading statements contained on the website. However, concern for the accuracy of Konop's publications, even if it was the primary motivator of Davis' conduct, cannot justify a violation of the Wire Tap Act and the Stored Communications Act. As we have found a triable issue with respect to these claims, we must also find a triable issue with respect to Konop's RLA claim based on the same conduct.

Hawaiian also argues that Davis' access did not violate the RLA because it did not appreciably limit Konop's organizing activities. Hawaiian emphasizes that, after learning about Davis' access to the website, Konop restricted access for a mere half-day and declined to temper the language in his articles. Hawaiian, however, presents no authority indicating that employees subject to surveillance or eavesdropping must also demonstrate that they consequently limited their organizing activity. It is the <u>tendency</u> to chill protected activities, not the actual chilling of protected activities, that renders eaves-

242

dropping and surveillance generally objectionable under federal labor law. <u>See, e.g., California Acrylic</u>, 150 F.3d at 1099. That a hardy individual might continue his organizing activities undeterred, despite an employer's surveillance, does not render the employer's conduct any less of a violation.**6** Accordingly, we find that Konop has raised a material triable issue of fact whether Hawaiian interfered with Konop's union organizing activity in violation of the RLA by accessing Konop's website.

2. Disclosure to Opposing Union.

Konop argues that Nobles unlawfully assisted Reno Morella, the union leader who supported the concessionary contract, by disclosing the contents of Konop's website. Generally, the RLA prohibits employers from providing assistance to a union or labor faction. <u>See Barthelemy v. Air Lines</u> <u>Pilots Ass'n</u>, 897 F.2d 999, 1009 (9th Cir. 1990); <u>see also</u> <u>NLRB v. Finishline Indus., Inc.</u>, 451 F.2d 1280, 1281-82 (9th Cir. 1971) (NLRA prohibits employer from telling workers to withdraw from one union and join another); <u>NLRB v. L. Ronney & Sons Furniture Mfg. Co.</u>, 206 F.2d 730, 734-35 (9th Cir. 1953) (NLRA prohibits employer from initiating membership drive among his employees for employer-favored union).

Konop argues that Nobles disclosed useful intelligence to a rival union faction in an effort to ensure that Konop's faction, which opposed the concessionary contract, would not prevail. Hawaiian does not seriously dispute that disclosure of the contents of Konop's website to Morella would constitute improper assistance. Instead, Hawaiian argues that Konop failed to present sufficient evidence that Nobles made any

6 Hawaiian also presents this argument to defeat the other two alleged RLA claims discussed in the following sections. We find it is no more persuasive in the context of those claims.

243

such disclosure or that Nobles was even familiar with the contents of Konop's website when he spoke to Morella.

Morella, however, states in his declaration that Nobles contacted him on December 14, 1995 and informed him"that he had just reviewed information which was posted on an internet communications system operated by Hawaiian Airlines Pilot Robert Konop." In addition, Morella states that Nobles also "disclosed to me that Konop's internet communications system contained a third written article concerning Konop's efforts to obtain union representation by a labor organization other than the Air Line Pilots Association." This evidence creates a genuine issue of fact with respect to whether Nobles was familiar with the contents of Konop's website and whether Nobles disclosed the contents of the website to Morella.

Moreover, Nobles confirmed in his declaration that he contacted Morella because he "felt that Reno Morella, the Chairman of the ALPA Master Executive Council, should be aware of the newsletter because of its inaccurate attack on the proposed labor agreements and the unfair effect it could have on the ratification process." Nobles thus effectively concedes that he interceded to help ensure that Morella's faction -- which favored ratification of the concessionary contract -- would prevail over Konop's faction, which opposed the agreement.

Accordingly, we find that Konop has raised a material triable issue of fact with respect to whether Nobles improperly assisted one union faction over another in violation of the RLA.

3. Threat of Defamation Suit.

Konop argues that Nobles engaged in unlawful coercion and intimidation by threatening to file a defamation suit against Konop based on statements on Konop's website. An employer's filing or threatened filing of a lawsuit against an

244

employee concerning union organizing activities may, under certain circumstances, violate the RLA. <u>See, e.g., Diamond</u> <u>Walnut Growers, Inc. v. NLRB</u>, 53 F.3d 1085, 1089-90 (9th Cir. 1995) (finding employer's defamation lawsuit against union violated NLRA); <u>GHR Energy Corp.</u>, 294 N.L.R.B. 1011, 1014 (1989), <u>enforced</u>, 924 F.2d 1055 (5th Cir. 1991) (analyzing whether employer's threat to sue employee for defamation violated NLRA).

Hawaiian does not argue that Nobles would be justified in threatening to sue Konop for defamation. Instead, Hawaiian contends that Konop failed to present sufficient evidence that Nobles ever made such a threat. Nobles stated in his declaration that he "did mention to Morella that the gross inaccuracies and lies in the newsletter made by Konop amounted to defamation," but that he "never said that[he] intended to file a lawsuit against Konop." Morella, however, indicates otherwise. Morella states in his declaration, "Nobles advised me that Konop should be cautioned, or informed, of the possibility of a defamation lawsuit by Nobles." Morella also testified, "[I]t was my impression and conclusion that Nobles intended for me to contact Konop, or take other action, for the purpose of opposing Konop's efforts to seek alternative union representation. " Morella then "informed Konop of Mr. Nobles' statements . . . regarding caution with respect to a possible lawsuit against Konop for defamation." Konop confirms the same in his declaration. This evidence is sufficient to raise a material triable issue of fact that Nobles threatened to sue Konop for defamation.

Accordingly, we find that Konop has raised a material triable issue of fact that Nobles engaged in coercion and intimidation in violation of the RLA by threatening to sue Konop for defamation.

D. Conclusion.

We hold that this court has jurisdiction over the RLA claims Konop presses on appeal, that Konop raised a triable

245

issue of fact that he engaged in activity protected under the RLA, and that Konop raised a triable issue whether Hawaiian violated the RLA by accessing his website, disclosing the website's content to a union leader, and threatening to sue Konop for defamation. Accordingly, we hold the district court erred in granting summary judgment against Konop on these RLA claims.

III. Bench Trial on Retaliation Claim.

After trial, the district court entered judgment against Konop on his retaliatory suspension claim. That claim involved Konop's allegation that Hawaiian violated the RLA when it placed him on sick leave in retaliation for protected labor activities. Konop challenges the district court's judgment against him on this claim on the ground that his subpoenas for corroborating witnesses were improperly quashed. We review a district court's order quashing subpoenas for an abuse of discretion. <u>See United States v. Berberian</u>, 767 F.2d 1324, 1324 (9th Cir. 1985). A litigant whose subpoenas have been improperly quashed must also show prejudice. <u>See</u> <u>Casino Foods Corp. v. Kraftco Corp.</u>, 546 F.2d 301, 302 (9th Cir. 1976).

Though there is some dispute regarding whether the district court's remarks in a pretrial hearing constituted an order to quash subpoenas at all, Konop has not suggested what relevant evidence the subpoenaed witnesses might have introduced had they been compelled to testify. Konop therefore has not shown that he was prejudiced as a result of any order by the district court quashing subpoenas.

CONCLUSION

The district court erred in granting summary judgment

to Hawaiian on Konop's Wiretap Act and Stored Communications Act claims, and Konop's Railway Labor Act statutory claims. The district court did not abuse its discretion by

246

quashing Konop's subpoenas of witnesses in connection with the bench trial on Konop's retaliatory suspension claim under the RLA and, therefore, judgment against Konop on that claim was proper.

REVERSED IN PART, AFFIRMED IN PART, and REMANDED.

247