

Case No. 07-56640

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

**JUSTIN BUNNELL, FORREST PARKER,
WES PARKER and VALENCE MEDIA, LTD.,**
Plaintiffs-Appellants,

v.

MOTION PICTURE ASSOCIATION OF AMERICA,
Defendant-Appellee.

Appeal from the United States District Court
for the Central District of California

The Honorable Florence Marie Cooper, United States District Judge
Case No. CV-06-03206-FMC

**BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION
IN SUPPORT OF PLAINTIFFS-APPELLANTS**

Kevin Bankston (State Bar No. 217026)
Marcia Hofmann (State Bar No. 250087)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Paul Ohm (State Bar No. 205374)
Associate Professor
UNIVERSITY OF COLORADO
SCHOOL OF LAW
401 UCB
Boulder, CO 80309
Telephone: (303) 492-0384
Facsimile: (303) 492-1200

Attorneys for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
CORPORATE DISCLOSURE STATEMENT	vii
STATEMENT OF AMICUS CURIAE	1
INTRODUCTION	2
ARGUMENT	2
I. ANDERSON “INTERCEPTED” PLAINTIFFS’ EMAILS IN VIOLATION OF THE WIRETAP ACT.....	2
A. Anderson “Intercepted” Plaintiffs’ Emails Based on The Wiretap Act’s Plain Language	2
B. Anderson’s Conduct Also Satisfies the Narrow Judicial Interpretation of “Intercept” As Being Limited to Acquisitions That Are Contemporaneous With Transmissions	6
II. THE NINTH CIRCUIT’S DECISION IN <i>KONOP V. HAWAIIAN AIRLINES, INC.</i> DOES NOT RESOLVE THIS CASE	9
A. The District Court Misapplied <i>Konop</i> Because Plaintiffs’ Emails Were Not in “Electronic Storage” When Intercepted.....	9
B. The Ninth Circuit’s Holding in <i>Konop</i> Was Narrow and Does Not Squarely Resolve This Case.....	12
C. <i>Konop</i> ’s Exclusion of Communications in “Electronic Storage” From the Definition of “Electronic Communication” Was Incorrect on the Plain Language of the Statute	15

D. *Konop* Is Not Dispositive Because This Case Presents
A Matter of First Impression18

III. IF PERMITTED TO STAND, THE DISTRICT COURT’S DECISION WILL
HAVE DIRE CONSEQUENCES FOR THE PRIVACY OF ELECTRONIC
COMMUNICATIONS.....25

CONCLUSION28

CERTIFICATE OF COMPLIANCE..... 1a

PROOF OF SERVICE.....2a

TABLE OF AUTHORITIES

CASES

<i>Bartnicki v. Vopper</i> , 532 U.S. 514 (2001)	22
<i>Berger v. New York</i> , 388 U.S. 41 (1967)	passim
<i>Export Group v. Reef Industrial, Inc.</i> , 54 F.3d 1466 (9th Cir. 1995)	8, 13
<i>George v. Carusone</i> , 849 F. Supp. 159 (D. Conn. 1994)	11
<i>Hall v. EarthLink Network, Inc.</i> , 396 F.3d 500 (2nd Cir. 2005)	3, 5, 6
<i>Jacobson v. Rose</i> , 592 F.2d 515 (9th Cir. 1978).....	11
<i>Konop v. Hawaiian Airlines, Inc.</i> , 302 F.3d 868 (9th Cir. 2002), <i>cert. denied</i> , 537 U.S. 1193 (2003).....	passim
<i>McDaniel v. Sanchez</i> , 452 U.S. 130 (1982).....	13
<i>Quon v. Arch Wireless Operating Co., Inc.</i> , 445 F. Supp. 2d 1116, <i>reversed in part on other grounds</i> , 2008 U.S. App. LEXIS 12766 (9th Cir. June 18, 2008)	20
<i>Sanders v. Robert Bosch Corp.</i> , 38 F.3d 736 (4th Cir. 1994).....	11
<i>Sibron v. New York</i> , 392 U.S. 40 (1968).....	23
<i>Steve Jackson Games, Inc. v. United States Secret Service</i> , 36 F.3d 457 (5th Cir. 1994)	1, 19, 20
<i>TRW v. Andrews</i> , 534 U.S. 19 (2001).....	16
<i>Theofel v. Farey-Jones</i> , 359 F.3d 1066 (9th Cir. 2004)	3, 20
<i>United States v. Councilman</i> , 418 F.3d 67 (1st Cir. 2005).....	passim

<i>United States v. Crawley</i> , 837 F.2d 291 (2nd Cir. 1988).....	13
<i>United States v. Johnson</i> , 256 F.3d 895 (9th Cir. 2001).....	14
<i>United States v. Lewis</i> , 406 F.3d 11 (1st Cir. 2005)	11
<i>United States v Luong</i> , 471 F.3d 1107 (9th Cir. 2006), <i>cert. denied</i> , 128 S. Ct. 532 (2007)	11
<i>United States v. Rodriguez</i> , 968 F.2d 130 (2nd Cir. 1992).....	11
<i>United States v. Smith</i> , 155 F.3d 1051 (9th Cir. 1998).....	7, 17
<i>United States v. Turk</i> , 526 F.2d 654 (5th Cir. 1976)	4, 6, 7, 8
<i>United States v. Warshak</i> , 490 F.3d 455 (6th Cir. 2007), <i>vacated en banc</i> , No. 06-4092, 2008 WL 2698177, 2008 U.S. App. LEXIS 14717 (6th Cir. July 11, 2008)	1

CONSTITUTIONAL PROVISION

U.S. Constitution, amendment IV	passim
---------------------------------------	--------

FEDERAL STATUTES

18 U.S.C. § 2510 <i>et seq.</i> , The Wiretap Act, <i>amended by</i> Electronic Communications Privacy Act (“ECPA”)	passim
18 U.S.C. § 2510(4)	passim
18 U.S.C. § 2510(5)	5
18 U.S.C. § 2510(8)	4
18 U.S.C. § 2510(12)	3, 16
18 U.S.C. § 2510(17)	15, 16
18 U.S.C. § 2511(2)	17, 26
18 U.S.C. § 2515	17
18 U.S.C. § 2517	17
18 U.S.C. § 2701, <i>et seq.</i> , Stored Communications Act (“SCA”).....	passim
18 U.S.C. § 2701(a)	15

18 U.S.C. § 2701(c)	26, 27
18 U.S.C. § 2702(b)	17
18 U.S.C. § 2703(a)	23
1968 U.S.C.C.A.N.	
§ 2112.....	22
§ 2153.....	22

OTHER AUTHORITIES

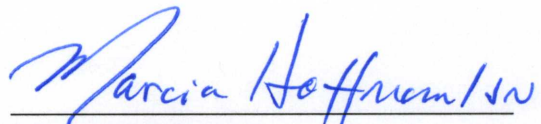
<i>American Heritage Dictionary</i> , 4th ed. (2000).....	4, 8, 11
Dep’t of Justice, <i>Searching and Seizing Computers and Obtaining Electronic Evidence</i> (July 2002).....	6
Kerr, Orin A., <i>A User’s Guide to the Stored Communications Act— And a Legislator’s Guide to Amending It</i> , 72 <i>Geo. Wash. L. Rev.</i> 1208 (2004).....	23, 24
Kerr, Orin A., <i>Lifting the “Fog” of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law</i> , 54 <i>Hastings L.J.</i> 805 (2003).....	25
LaFave, Wayne R., 2 <i>Crim. Proc.</i> (2007-2008).....	14, 17, 23
S. Rep. No. 99-541, 99th Cong., 2d Sess. (1986).....	3
S. Rep. No. 1097, 90th Cong., 2d Sess. (1968)	22

CORPORATE DISCLOSURE STATEMENT

Pursuant to FRAP 26.1, amicus Electronic Frontier Foundation (“EFF”) reports that it is a 501(c)(3) non-profit corporation incorporated in the State of California and makes the following disclosure:

1. EFF is not a publicly held corporation or other publicly held entity.
2. EFF has no parent corporations.
3. No publicly held corporation or other publicly held entity owns 10% or more of EFF.

Dated: August 1, 2008



Marcia Hofmann
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110

STATEMENT OF AMICUS CURIAE

The Electronic Frontier Foundation (“EFF”) is a non-profit civil liberties organization working to protect free speech and privacy rights in the online world. With more than 10,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

As part of its mission, EFF has served as counsel or amicus in key cases addressing electronic privacy statutes and the Fourth Amendment as applied to the Internet and other new technologies. *See, e.g., Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1193 (2003); *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (*en banc*); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994); *United States v. Warshak*, 490 F.3d 455 (6th Cir. 2007), *vacated en banc*, No. 06-4092, 2008 WL 2698177, 2008 U.S. App. LEXIS 14717 (6th Cir. July 11, 2008).

The parties have consented to the filing of this brief.

INTRODUCTION

Amicus EFF respectfully urges reversal of the district court’s holding that Rob Anderson, by using the Plaintiffs’ email server to acquire copies of Plaintiffs’ emails contemporaneous with their transmission, did not “intercept” Plaintiffs’ emails in violation of the Wiretap Act. *See Bunnell v. Motion Picture Ass’n of America*, slip op. at 8:11-12, 2:06-cv-03206-FMC-JCx (C.D. Cal. Aug. 22, 2007). The district court’s holding is contrary to the plain language of the statute, misapplies the law of this Circuit, and, by setting a precedent for the government and others to engage in similar conduct without regard to the Wiretap Act’s prohibitions, dangerously undermines the statutory and constitutional privacy rights of every Internet user.

ARGUMENT

I. ANDERSON “INTERCEPTED” PLAINTIFFS’ EMAILS IN VIOLATION OF THE WIRETAP ACT

A. Anderson “Intercepted” Plaintiff’s Emails Based on the Wiretap Act’s Plain Language

The plain language of the Wiretap Act as amended by the Electronic Communications Privacy Act (“ECPA”), 18 U.S.C. § 2510 *et seq.*, when applied to the undisputed facts, demonstrates that Anderson’s use of Plaintiffs’ email server to acquire Plaintiffs’ communications constituted

“intercepts” of those communications. “Neither party disputes” the key fact “that Anderson configured the ‘copy and forward’ function on Plaintiffs’ email server so that he,” in addition to the intended recipients of the emails, “would receive copies of all Plaintiffs’ emails in his Google [email] account.” *Bunnell*, slip op. at 5:23-25. The Wiretap 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) (emphasis added). Application of this plain language is straight-forward: “through [his] use of [a] device,” *i.e.*, the reconfigured email server, Anderson “acquired” the “contents” of Plaintiffs’ emails, which are “electronic communications.” *See id.*

As an initial matter, there is no question that Plaintiffs’ emails are “electronic communications.”¹ *Bunnell*, slip op. at 5:25-26 (“The parties also do not dispute that the emails are ‘electronic communications’ as defined by

¹ The Wiretap Act in relevant part defines an “electronic communication” as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, electromagnetic, photoelectronic or photooptical system” 18 U.S.C. § 2510(12). This broad definition includes emails. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1076-77 (9th Cir. 2004) (treating email as “electronic communication”); *United States v. Councilman*, 418 F.3d 67, 72-79 (1st Cir. 2005) (en banc) (same); *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 503-04 (2d Cir. 2005) (same). Legislative history also explicitly states that the definition of “electronic communication” covers email. S. Rep. No. 99-541, at 14 (1986).

the ECPA.”). Nor does anyone dispute that the information forwarded to Anderson included the “content” of the forwarded emails, *i.e.*, “information concerning the substance, purport, or meaning of th[ose] communication[s].” *See* 18 U.S.C. § 2510(8). The remaining question is whether Anderson “acquired” those contents “through the use of...[a] device.” § 2510(4). “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.’” *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 880 (9th Cir. 2002). The statute also does not define “acquire,” which in its ordinary meaning is to “gain possession of.”² It is undisputed that Anderson gained possession of Plaintiffs’ emails (or else he could not have disclosed those same emails to defendants), and that he employed the reconfigured email server for that purpose, putting it into his service by reconfiguring it to forward Plaintiffs’ emails to himself. *Bunnell*, slip op. at 5:23-25 (“Anderson configured the ‘copy and forward’ function on Plaintiffs’ email server so that he would

² *See The American Heritage Dictionary*, 4th ed. (2000), available at <http://www.bartleby.com/61/23/A0062300.html> (defining “acquire”). Several courts have gone beyond this plain language meaning of the term “acquire” as used in the “intercept” definition to include an unspoken requirement that the “acquisition” occur contemporaneously with the transmission of the communication. *See, e.g., United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976). However, as discussed in the next section, Anderson’s conduct also satisfies this narrow reading of the “intercept” definition.

receive copies of all Plaintiffs' emails....").

The only remaining question is whether or not Plaintiffs' email server, as reconfigured and used by Anderson, constituted an "electronic, mechanical, or other device" (hereinafter "interception device"). That phrase *is* defined in the Wiretap Act, albeit in a somewhat circular fashion, as the definition refers back to the term "intercept." *See* 18 U.S.C. § 2510(5). The definition provides that an "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication...." *Id.* The reconfigured email server as used by Anderson to acquire Plaintiffs' emails meets this definition.³

³ The definition carves out a very narrow exception for "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic service in the ordinary course of its business." *See* 18 U.S.C. § 2510(5). This exception does not apply in this case for several reasons. First, Anderson was not acting as "a provider" when he reconfigured the email server to spy on the Plaintiffs. This was an *ultra vires* act. Second, reconfiguring an email server to spy on email recipients can in no way be interpreted as an act done "in the ordinary course of business." Although the mail server was also being used to legitimately deliver mail, it was simultaneously used for a surreptitious and invasive second purpose that can in no way be called "the ordinary course of business." *Cf. Hall*, 396 F.3d at 505 (analyzing separately different acts performed with a single email server to determine if each act fell within the "ordinary course of business exception."). Finally, the exception appears to apply only to "telephone or telegraph" instruments, equipments, or facilities. The instant facts involved no telephone or telegraph equipment whatsoever.

Although the Second Circuit in *Hall* did extend this exception to Internet services, it relied on a questionable reading of legislative history. *Id.* This

In conclusion, the email server as it was “used” by Anderson—*i.e.*, to “acquire” the “contents” of Plaintiffs’ “electronic communications”—qualifies as an “electronic, mechanical, or other device,” fully satisfying the plain language definition of “intercept.”

B. Anderson’s Conduct Also Satisfies the Narrow Judicial Interpretation of “Intercept” As Being Limited to Acquisitions That Are Contemporaneous with Transmission

In addition to satisfying the plain language meaning of the term “intercept,” Anderson’s conduct also satisfies the narrower “judicial definition of ‘intercept’ as *acquisition contemporaneous with transmission*” that has been adopted by the Ninth Circuit and other courts. *Konop*, 302 F.3d at 878 (emphasis added); *see also id.* at 876-78 (discussing other cases adopting the same requirement). This so-called “contemporaneity requirement” originated in *United States v. Turk*, where the Fifth Circuit held that the definition of “intercept” requires “participation by the one charged with an ‘interception’ in the *contemporaneous acquisition of the*

interpretation is at odds with the Department of Justice’s reading of the statute, which interprets this as an exception solely about “extension telephones.” Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence* § IV.D.3.e (July 2002) available at <http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm>. At any rate, *Hall* is also distinguishable because the court found that the provider was acting “in the ordinary course of its business,” *id.*, which is not true for Anderson. For all of these reasons, amicus urges this court to decline to follow *Hall*.

communication through the use of the device,” such that the recording of the telephone conversations at issue was an interception, but the replaying of the recorded conversations was not. 526 F.2d 654, 658 (5th Cir. 1976) (emphasis added).

Importantly, the *Turk* decision located this contemporaneity requirement in the same terms at issue here when discussing Anderson’s conduct: “acquisition...through the use of any...device.” *Id.* Therefore it was unnecessary for the court in *Konop* to rely on the definition of “electronic communication”—which it read to exclude communications in “electronic storage,” *see* 302 F.3d at 878—to reach the conclusion that an interception must occur contemporaneous with transmission, as that requirement was already present in the definition’s other terms, regardless of which type of communication was at issue. *Turk*, 526 F.2d at 658.⁴ Therefore, to the extent *Konop* may be read to conclude that a

⁴ The Ninth Circuit has previously held that the *Turk*’s recognition of a contemporaneity requirement in the “intercept” definition “is no longer of any real persuasive force” because it was “statutorily overruled,” at least in regard to wire communications, by Congress’ amendment of the wire communication definition to include stored communications. *See United States v. Smith*, 155 F.3d 1051, 1057 n. 11 (9th Cir. 1998). However, as recognized in *Konop*, Congress has since reversed that amendment to the wire communication definition. 302 F.3d at 878. Therefore *Turk*’s interpretation of “intercept,” whereby the contemporaneity requirement is inherent in the terms “acquisition...through the use of any...device,” is valid once again. 526 F.2d at 658.

communication cannot be intercepted while in “electronic storage” *even when* the acquisition is contemporaneous with transmission, such conclusion is best read as a dictum. *See Export Group v. Reef Indus., Inc.*, 54 F.3d 1466, 1472 (9th Cir. 1995) (holding that conclusion reached in previous Ninth Circuit opinion was “not necessary to the decision” of that case and therefore had “no binding or precedential impact”).

Also notably, *Turk* did not equate “contemporaneous”⁵ with “simultaneous.”⁶ The recording at issue in *Turk* did not strictly occur at the exact same instant as the utterances that were recorded, but only “*almost*” at the same instant, yet the recording was still held to be “contemporaneous” with the communication. 526 F.2d at 658 n. 2 (emphasis added). Put another way, even though there were milliseconds of difference between the moment the communication was uttered and the moment those sound waves reached and were acquired by the recorder, such that the acquisition was not “simultaneous” with the communication, the acquisition was still “contemporaneous.” Therefore it is immaterial to the contemporaneity

⁵ *See The American Heritage Dictionary*, 4th ed. (2000), available at <http://www.bartleby.com/61/79/C0597900.html> (defining “contemporaneous” as “originating, existing, or happening during *the same period of time*”) (emphasis added).

⁶ *See The American Heritage Dictionary*, 4th ed. (2000), available at <http://www.bartleby.com/61/12/S0421200.html> (defining “simultaneous” as “happening, existing, or done at *the same time*”) (emphasis added).

requirement whether Anderson’s “interception” of Plaintiffs’ emails may have occurred a few milliseconds *after* those communications were transmitted to the server and placed in electronic storage. However, as described in the next section, that is not when the “interception” occurred as a legal matter, and the district court’s holding that Plaintiffs’ emails were “acquired *while* in ‘electronic storage’” was incorrect as a matter of law. *Bunnell*, slip. op. at 6:1 (emphasis added).

II. THE NINTH CIRCUIT’S DECISION IN *KONOP V. HAWAIIAN AIRLINES, INC.* DOES NOT RESOLVE THIS CASE

A. The District Court Misapplied *Konop* Because Plaintiffs’ Emails Were Not in “Electronic Storage” When Intercepted

The district court concluded that Anderson acquired Plaintiffs’ communications “*while* in ‘electronic storage,’” and therefore applied *Konop*’s holding that communications cannot be intercepted while in electronic storage. *Bunnell*, slip op. at 6:1 (emphasis added); *see also id.* at 8:11-22. As already noted, that *Konop* holding should be construed as dicta, considering it was unnecessary to the result, which would have been the same had the court simply applied the judicial interpretation of “intercept” as containing a contemporaneity requirement. However, even accepting *arguendo* that communications cannot be intercepted while in electronic storage, that holding is inapplicable here. That is because the district court’s

conclusion that the relevant moment of acquisition occurred *while* the communications were in storage was incorrect as a matter of law. Rather, the acquisition occurred *before* the communications were placed in storage on the server, when the server first acquired them.

In holding that the relevant acquisition occurred while the communications were in electronic storage, the district court focused on the moment that the reconfigured email server copied and forwarded the messages. *Bunnell*, slip op. at 8:25-27 (“In the instant case, Plaintiffs’ server stored the emails before they were copied and forwarded to Anderson’s email account.”). In doing so, the district court fundamentally misunderstood which moment was the legally relevant moment of acquisition. The legally relevant moment of acquisition was not when the emails were copied and forwarded by the reconfigured server, but rather, when the reconfigured server first acquired the emails transmitted to it. To “intercept” is to acquire using a device; as already explained, the relevant device here was the reconfigured email server being used by Anderson; therefore, the relevant “acquisition” was the initial acquisition by the email server.

The district court’s holding otherwise—that Anderson “acquired” the communications when the server forwarded the emails to Anderson, rather

than when the server acquired them for Anderson—contradicts the settled understanding of the term “intercept.” As this Circuit has held, “redirection”—here, the server’s copying from memory and forwarding of Plaintiffs’ emails—“presupposes interception.” *United States v Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006), *cert. denied*, 128 S. Ct. 531, 169 L. Ed. 2d 371 (2007) quoting *United States v. Rodriguez*, 968 F.2d 130, 136 (2nd Cir. 1992) (concluding that interception occurred where the tapped phone was located) (emphasis added). Therefore, the legally relevant moment is the moment that the interception device first acquires the communication, which necessarily *precedes* the storage or redirection of the communication by that device.⁷ See *Luong*, 471 F.3d at 1109, quoting *Rodriguez*, 968 F.2d at 136 (when a communication is “captured or redirected in any way, an interception occurs at that time”); *United States v. Lewis*, 406 F.3d 11, 18 n.5 (1st Cir. 2005) (phone call intercepted when recorded, not when listened to); *Jacobson v. Rose*, 592 F.2d 515, 522 (9th Cir. 1978) (listening to recording of phone conversation not necessary to constitute an intercept); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir. 1994) (contents of phone call acquired when recorded); *George v. Carusone*, 849 F. Supp.

⁷ See *The American Heritage Dictionary*, 4th ed. (2000), available at <http://www.bartleby.com/61/58/P0545800.html> (defining “presuppose” as “to require or involve necessarily as an antecedent condition”).

159, 163 (D. Conn. 1994) (same).

Under these precedents, it is clear that Anderson’s interception of Plaintiffs’ emails did not occur when the reconfigured email server forwarded the emails to him, but rather, when the reconfigured email server—Anderson’s interception device—first acquired them from the wire: *prior* to those communications being stored on the server, and *prior* the copying and forwarding to Anderson. Therefore *Konop*’s purported holding that communications in electronic storage cannot be intercepted was inapplicable. However, even if the acquisition could reasonably be construed to have occurred while the communications were in electronic storage, *Konop* still would not resolve this case.

B. The Ninth Circuit’s Holding in *Konop* Was Narrow and Does Not Squarely Resolve This Case

The purported holding in *Konop*, which is the cornerstone of the district court’s decision, is narrowly limited to the facts of that case: “[w]e 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.” 302 F.3d at 878 (emphasis added). Importantly, *Konop* did not actually hold that the website communications at issue were in “electronic storage” when they were acquired, but instead assumed so based on the agreement of the parties. *See id.* at 879. Here, by

contrast, there is no such agreement. Furthermore, the decision did not involve email communications, and did not consider the issue of acquisitions during storage that also occurred—as the acquisitions in this case occurred—contemporaneous with transmission.

Konop did briefly consider in a footnote whether the term “intercept” applies to emails acquired from storage incident to their transmission, concluding that Congress “considered and rejected this argument” and “chose to afford stored communications less protection than other forms of communication.” *Id.* at 878 n.6. However, this discussion was peripheral to the holding, and therefore not binding precedent. *See Export Group*, 54 F.3d at 1472; *McDaniel v. Sanchez*, 452 U.S. 130, 143 (1982) (finding language in a footnote from prior Supreme Court case to be “dictum unnecessary to the decision in that case” and “therefore, not controlling in this case”); *United States v. Crawley*, 837 F.2d 291, 292-293 (2nd Cir. 1988) (discussing various reasons a court might reject a dictum in a prior case, including that “the passage was unnecessary to the outcome of the earlier case and therefore perhaps not as fully considered as it would have been if it were essential to the outcome.”).

The Ninth Circuit has never squarely considered the question of whether electronic communications are “intercepted” when they are

automatically copied and forwarded during the course of their transmission. Neither the plain language of ECPA nor a proper reading of *Konop* dictates that such email messages cannot be intercepted within the meaning of the Wiretap Act. As one prominent criminal procedure treatise explains:

The Ninth Circuit's decision in *Konop* . . . could be read as drawing the line between a communication that is collected "during transmission" versus one that is collected "while it is in electronic storage." *Konop*, 302 F.3d at 878. To the extent *Konop* is so read, this line is not exactly correct. The scope of the Wiretap Act should be defined by whether the surveillance is undertaken as "a series or a continuous surveillance" rather than as "one limited intrusion," *Berger [v. New York]*, 388 U.S. [41] at 57, not whether the communication was moving or at rest at the moment of acquisition.

Wayne R. LaFave *et al.*, 2 CRIM. PROC. § 4.6(b) n.30 (2007-2008).

Because the holding in *Konop* was extremely narrow and based on a significantly different factual record, the Court's tangential consideration of email interception in that case should not be dispositive here. *United States v. Johnson*, 256 F.3d 895, 915 (9th Cir. 2001) (per curiam) (It may be appropriate for the Court to reexamine a statement made in a prior decision "[w]here it is clear that a statement is made casually and without analysis, where the statement is uttered in passing without due consideration of the alternatives, or where it is merely a prelude to another legal issue that commands the panel's full attention").

C. *Konop*'s Exclusion of Communications in "Electronic Storage" From the Definition of "Electronic Communication" Was Incorrect on the Plain Language of the Statute

In addition to being dicta, *Konop*'s conclusion that communications in "electronic storage" are not "electronic communications" and therefore cannot be "intercepted" under the Wiretap Act was incorrect on the statute's plain language. In fact, the ECPA clearly contemplates circumstances in which electronic communications that are in "electronic storage" still constitute "electronic communications." For example, the definition of "electronic storage" itself includes "(A) any temporary, intermediate *storage* of a wire or *electronic communication* incidental to the electronic transmission thereof" 18 U.S.C. § 2510(17) (emphasis added). Likewise, the Stored Communication Act ("SCA") portion of the ECPA, 18 U.S.C. § 2701 *et seq.*, prohibits unauthorized access to an "*electronic communication* while it is in *electronic storage*" 18 U.S.C. § 2701(a) (emphasis added). Thus, the plain language of the statute makes clear that "electronic communications" in "electronic storage" are still "electronic communications."

This plain language interpretation of "electronic communication" is supported by the fact that Congress chose to craft the definition so that it contains four narrow exceptions, none of which specify communications in

electronic storage.⁸ *See* 18 U.S.C. § 2510(17). As the First Circuit has noted:

Congress knew how to, and in fact did, explicitly exclude four specific categories of communications from the broad definition of “electronic communication.” Yet Congress never added the exclusion . . . “any electronic communication in electronic storage.” This interpretative principle then applies: “Where Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent.” *TRW v. Andrews*, 534 U.S. 19, 28 (2001) (quotation marks and citation omitted).

United States v. Councilman, 418 F.3d 67, 74-75 (1st Cir. 2005) (*en banc*) (internal citations excluded).

The district court also erred when it determined that the Wiretap Act and SCA are mutually exclusive and cannot cover the same communication. Citing *Konop*, the lower court concluded that “at any given time, an electronic communication may either be intercepted and actionable under the Wiretap Act, *or* acquired while in electronic storage and actionable under the SCA,” so that “if Anderson acquired Plaintiffs’ emails while they were

⁸ The Wiretap Act defines “electronic communication” 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) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device; or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds” 18 U.S.C. § 2510(12).

in ‘electronic storage,’ Plaintiffs’ claim under the Wiretap Act necessarily fails.” *Bunnell*, slip op. at 6:12-14 (emphasis in original). *Konop* does not stand for this proposition, however, and nothing in the plain language of the Wiretap Act or SCA suggests that a violation of one statute cannot also be a violation of the other. In fact, this Court explicitly rejected this possibility with respect to interception of wire communications in *United States v. Smith*, recognizing that conduct that violates the Wiretap Act may also violate the SCA:

[W]e conclude that the government's attempt to divide the statutory provisions cleanly between those concerning in-progress wire communications (e.g., § 2515) and those concerning in-storage wire communications (e.g., § 2701) is not a viable one.... “[A]ccess” is, for all intents and purposes, a lesser included offense . . . of “interception.”

155 F.3d at 1058 (emphasis in original).⁹

⁹ LaFave supports this interpretation of the law as well:

[The Wiretap Act and SCA] can in some circumstances regulate access and copying of the same communication. The Wiretap Act regulates prospective continuous surveillance of an account that may result in a particular communication being copied, while the Stored Communications Act regulates a single intrusion to access and copy that communication. The peaceful co-existence of the two statutes is aided by 18 U.S.C.A. § 2702(b)(2) of the Stored Communications Act, which explicitly permits a provider to disclose the contents of communications “as otherwise authorized” in Sections 2511(2)(a) or 2517 of the Wiretap Act.

LaFave, 2 CRIM. PROC. § 4.6(b) n. 30.

As the district court noted in its opinion, there is no dispute that the Plaintiffs' emails are "electronic communications" as defined in the Wiretap Act. *Bunnell*, slip op. at 5:25-26. As such, they can be "intercepted" under the plain language of the Wiretap Act. 18 U.S.C. § 2510(4) (defining "intercept" as the "acquisition of the contents of any . . . electronic . . . communication through the use of any electronic, mechanical, or other device").

D. *Konop* is Not Dispositive Because This Case Presents a Matter of First Impression

Finally, this case presents a matter of first impression for the Ninth Circuit. Neither *Konop* nor the other precedents relied upon by the district court should be blindly applied to determine the outcome of this case, because they were each based on a fundamentally different set of facts.

In *Konop*, an employee of Hawaiian Airlines operated a secure website on which he posted criticisms of the airline. 302 F.3d at 872. The company's vice president used other Hawaiian employees' names to repeatedly access the website, which the Plaintiff had not authorized him to view. *Id.* at 873. The Court held that this conduct did not violate the Wiretap Act because the vice president did not "intercept" an electronic communication within the meaning of the statute. *Id.* at 879.

Both this case and *Konop* involve the Internet, so it is superficially appealing to treat them alike. However, the conduct alleged to be an illegal wiretap in the two cases was fundamentally different. In *Konop* the conduct considered by the Ninth Circuit was an individual's visits to a website, *id.* at 874, not the continuous and contemporaneous acquisition of Internet communications such as the continual copying and forwarding of all emails to and from a plaintiffs' email server. The former scenario concerns access to static information stored on a server, while this case involves Anderson's ongoing and continuous acquisition of Plaintiffs' emails in the same period of time during which they were transmitted.

Each of the other cases cited by the district court are like *Konop* and one another and different from the instant case in the same important way. They all involved acquisitions of communications that were not contemporaneous with the communications' transmission, and what they say about wiretapping should be understood in that context. The district court erred similarly in relying on *Steve Jackson Games v. United States Secret Service*, a case also cited heavily by this Court in *Konop*. 36 F.3d 457 (5th Cir. 1994). *Steve Jackson Games* concerned the government's one-time seizure of 162 email messages stored on an electronic bulletin board system, though not yet retrieved by their intended recipients. *Id.* at 459. Like the

holding in *Konop*, the Fifth Circuit's decision in *Steve Jackson Games* was based upon communications stored on a server for a period of time, and not communications acquired contemporaneous with transmission to their intended recipients. *Id.*

Also inapposite is *Theofel v. Farey-Jones*, which involved the defendant's improper issuance of a subpoena to acquire every email message ever sent or received by anyone at a particular company, and a service provider's subsequent posting of a sample of those messages on a website. 359 F.3d 1066, 1071 (9th Cir. 2004). As in *Konop*, the Ninth Circuit was considering the acquisition of electronic communications that had been stored on a server for some time, not the acquisition of those emails contemporaneous with their transmission. The district court's reliance on *Quon v. Arch Wireless* was misplaced for the same reason. 445 F. Supp. 2d 1116, *rev'd in part on other grounds*, 2008 U.S. App. LEXIS 12766 (9th Cir. June 18, 2008). In that case, the defendant service provider disclosed transcripts of text messages to a police department conducting an audit and investigation of the plaintiffs, who were department employees. 445 F. Supp. 2d at 1125-28. Again, the electronic communications at issue had been stored on the defendant's servers for days or weeks, *id.* at 1126, and were not copied at the same time they were sent or received.

In the years since *Konop* was decided, the First Circuit has considered whether a stored electronic communication can be intercepted under the Wiretap Act under facts nearly identical to those in this case. *Councilman*, 418 F.3d 67. In *Councilman*, the defendant ran Interloc, an online rare and out-of-print book listing service that gave its book dealer customers email accounts. *Id.* at 70. The defendant instructed an employee to configure the mail processing software to copy all messages to Interloc’s customers from Amazon.com, a competitor. *Id.* The employee configured the software to copy each incoming message before it was delivered to the recipient’s inbox and forward the copy to the defendant. *Id.* The defendant was charged with conspiring to violate the Wiretap Act by, *inter alia*, intercepting electronic communications. *Id.* at 71. A divided three-judge appellate panel concluded that the defendant had not violated the Wiretap Act because he could not intercept electronic communications in “electronic storage.” *Id.* The en banc court disagreed with this interpretation, concluding after a lengthy analysis of the text, structure and legislative history of the Wiretap Act that “an e-mail message does not cease to be an ‘electronic communication’ during the momentary intervals, intrinsic to the communication process, at which the message resides in transient electronic storage.” *Id.* at 79.

Read together with *Konop*'s narrow holding that a communication intercepted under the Wiretap Act must be "acquired during transmission," 302 F.3d at 878, *Councilman* refines that principle to state that an electronic communication may be in transient electronic storage while in transmission. 418 F.3d at 79. This situation may arise under circumstances precisely like those at bar: when emails are acquired in an ongoing manner, contemporaneous with their transmission.

The court should also look to Constitutional case law construing the Fourth Amendment, and, in particular, *Berger v. New York*, 388 U.S. 41, 57 (1967), when construing the Wiretap Act's meaning. The legislative history of the Wiretap Act shows that Congress enacted the law with *Berger* in mind. S. Rep. No. 1097 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2153 ("In the course of [*Berger*], the Court delineated the constitutional criteria that electronic surveillance legislation should contain. Title III [the Wiretap Act] was drafted to meet these standards"). *See also Bartnicki v. Vopper*, 532 U.S. 514, 522-23 (2001) (discussing the causal connection between *Berger* and the passage of the Wiretap Act). In *Berger*, the Supreme Court applied the Fourth Amendment where surveillance was performed as "a series [of intrusions] or a continuous surveillance" and not "one limited intrusion." 388 U.S. at 57. As a result, any statute that permits "a series or a

continuous surveillance” must include rigorous privacy protections or may be facially invalid under the Fourth Amendment. *Id.* at 56; *Sibron v. New York*, 392 U.S. 40, 59-60 (1968) (noting that *Berger* struck down a New York statute setting forth a procedure for issuing wiretap warrants, but failing to include necessary safeguards to satisfy Fourth and Fourteenth Amendment scrutiny).

Keeping in mind the relationship between *Berger* and the Wiretap Act, any ambiguity in the Wiretap Act’s language should be construed consistently with *Berger*’s Fourth Amendment requirements. As a leading treatise on criminal procedure notes:

Given the Wiretap Act’s close connection to *Berger*, the meaning of “intercept” should mirror the distinction drawn by the Supreme Court in *Berger*. Acquisition is an intercept when it is part of “a series or a continuous surveillance,” such as ongoing prospective surveillance or its functional equivalent. Exact lines will be difficult to draw, but the essential question should be whether the means of monitoring is the functional equivalent of continuous surveillance or whether it is more like a one-time or otherwise limited access to communications.

LaFare, 2 CRIM. PROC. § 4.6(b).¹⁰

¹⁰ Similarly, Professor Orin Kerr has explained:

When stored communications are accessed in a way that makes the access the functional equivalent of a wiretap, the surveillance should be regulated by the Wiretap Act, not the SCA. For example, if an agent lines up a string of [18 U.S.C. §] 2703(a) orders and serves one order per hour, I think that is the functional equivalent of a wiretap. It is reasonable to infer that

This case involves the continuous, ongoing surveillance of the contents of the Plaintiffs' incoming and outgoing electronic communications. Consistent with *Berger*, this Court should find that this conduct constitutes an "intercept" under the Wiretap Act. Any other holding will authorize warrantless that does not satisfy the requirements of *Berger*, which will create serious constitutional concerns.

In sum, no court in the Ninth Circuit has ever squarely faced the application of the Wiretap Act to the contemporaneous acquisition of communications. As a result, the district court erred insofar as it found that precedent to be dispositive. The Court should treat this case as a matter of first impression and find that any ongoing, prospective surveillance must be regulated by the Wiretap Act, consistent with *Berger*.

///

///

the purpose of the surveillance is to obtain copies of all incoming messages, not to look for communications stored in a target's inbox. Similarly, *it is the functional equivalent of a wiretap if an agent installs software that copies incoming messages a few milliseconds after they arrive.*

Orin Kerr, *A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1232 (2004) (emphasis added).

III. IF PERMITTED TO STAND, THE DISTRICT COURT'S DECISION WILL HAVE DIRE CONSEQUENCES FOR THE PRIVACY OF ELECTRONIC COMMUNICATIONS

This case is alarming because its implications will reach far beyond a single civil case. The district court's holding would remove a vast amount of communications from the protection of the Wiretap Act. As such, those communications would at best be protected by the SCA, which provides significantly less protection against government access to communications. *See* Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 829 (2003) (discussing how ECPA decisions in the civil context may not translate well to criminal cases and create "surprising and disturbing implications for routine criminal investigations").

Most worrisome is that under the district court's holding, law enforcement officers could engage in the contemporaneous acquisition of emails just as Anderson did, without having to comply with the Wiretap Act's requirements. For example, if the FBI installed a network wiretapping device at a point where electronic communications are stored for milliseconds before continuing to their destination, the Bureau would not have to obtain an intercept order under the Wiretap Act, but could instead proceed under the SCA's less stringent requirements, even though such

surveillance represents “a series [of intrusions] or a continuous surveillance” under *Berger*, 388 U.S. at 57.

The problem is exacerbated by the fact that the SCA and the Wiretap Act treat communications providers very differently. While the Wiretap Act significantly constrains a provider’s ability to intercept except where necessary to provide service or protect its property, 18 U.S.C. § 2511(2)(a)(i), the SCA permits blanket access to communications where that access is “authorized by the person or entity providing a wire or electronic communications service.” 18 U.S.C. § 2701(c)(1). Under the district court’s holding, then, if the FBI wished to contemporaneously acquire emails sent through a particular provider, the Bureau could sidestep the requirements of the SCA by simply obtaining the provider’s consent to install wiretapping devices on its servers. So long as such conduct is not considered to be an “intercept” under the Wiretap Act, and so long as the government obtains sufficient consent from the provider under the SCA, the FBI will be free to monitor the incoming and outgoing messages of any email account it wants, without any legal process at all.

The district court’s holding also has dangerous implications for non-government access to communications. For example, without the threat of liability under the Wiretap Act, Internet service providers could intercept

and use the private communications of their customers, with no concern about liability under the SCA, which provides blanket immunity to providers. *See* 18 U.S.C. § 2701(c)(1). Moreover, individuals could freely monitor others' email for criminal or corporate espionage purposes without running afoul of the Wiretap Act.

In sum, the district court should not have read *Konop* in such a dangerously expansive manner as to stand for the proposition that communications that are contemporaneously acquired are not “intercepted” if they were also acquired while in “electronic storage.” To ensure the ECPA’s continued compliance with *Berger*, and its continued effectiveness as a privacy-protective regime, the district court must be overruled.

///

///

///

///

///

///

///

CONCLUSION

For the foregoing reasons, the Court should vacate the district court opinion and find that Anderson “intercepted” Plaintiffs’ communications under the Wiretap Act.

Dated: August 1, 2008

Respectfully submitted,



Kevin Bankston (SBN 217026)
Marcia Hofmann (SBN 250087)
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Paul Ohm (SBN 205374)
Associate Professor
UNIVERSITY OF COLORADO
SCHOOL OF LAW
401 UCB
Boulder, CO 80309
Telephone: (303) 492-0384
Facsimile: (303) 492-1200

Attorneys for *Amicus Curiae*

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains **6,123** words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6). This brief has been prepared in a proportionally spaced typeface using Microsoft Word 2004 for Mac version 11.2 in Times New Roman, 14-point font.

Dated: August 1, 2008

Respectfully submitted,



Marcia Hofmann
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

PROOF OF SERVICE

I, Joanne Newman, the undersigned, do hereby state that:

I am over the age of eighteen years and not a party to the instant proceeding. My business address is: 559 Nathan Abbott Way, Stanford, California 94305-8610.

On the date set forth below, I caused to be served the following document:

BRIEF OF *AMICUS CURIAE* ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-APPELLANTS

on counsel listed below by depositing two true copies thereof, enclosed in a sealed envelope via Federal Express for overnight delivery, to each person listed below addressed as follows:

For the Plaintiffs-Appellants:

Ira P. Rothken , Esq.
Robert L. Kovsky, Esq.
ROTHKEN LAW FIRM
3 Hamilton Landing
Suite 280
Novato, CA 94949
Telephone: (415) 924-4250
Facsimile: (415) 924-2905

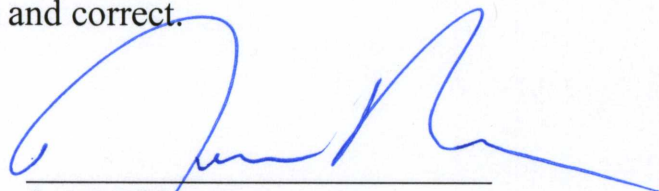
Kirk J. Retz, Esq.
RETZ & HOPKINS, LLP
21535 Hawthorne Boulevard
Suite 200
Torrance, CA 90503-0000
Telephone: (310) 540-9800
Facsimile: (310) 540-9881

For the Defendant-Appellee:

Steven B. Fabrizio, Esq.
Brian Hauck, Esq.
JENNER & BLOCK, LLP
601 Thirteenth Street N.W.
Suite 1200 South
Washington, D.C. 20005
Telephone: (202) 639-6000
Facsimile: (202) 639-6066

Karen Rae Thorland, Esq.
LOEB & LOEB, LLP
10100 Santa Monica Boulevard
Suite 2200
Los Angeles, CA 90067-4164
Telephone: (310) 282-2154
Facsimile: (310) 919-3921

Executed on August 1, 2008 at Stanford, California. I declare under penalty of perjury that the foregoing is true and correct.



Joanne Newman