

**FOR PUBLICATION**  
**UNITED STATES COURT OF APPEALS**  
**FOR THE NINTH CIRCUIT**

GEORGE THEOFEL; HOWARD TEIG;  
DAVID KELLEY; INTEGRATED  
CAPITAL ASSOCIATES, INC., A  
Delaware Corporation; NANCY  
RILETT; RYAN TAM; CLAUDIA  
ENGLISH; TERESA PATTERSON;  
TANYA YOUNG; ROBERTO  
MARSELLA; REGINA OVENDEN; EMIL  
PESIRI; ERIC SULLIVAN; DOUGLAS H.  
WOLF; RICHARD BUCKINGHAM,  
*Plaintiffs-Appellants,*

v.

ALWYN FAREY-JONES; IRYNA A.  
KWASNY,  
*Defendants-Appellees.*

No. 02-15742  
D.C. No.  
CV-01-04166-MMC

GEORGE THEOFEL; HOWARD TEIG;  
DAVID KELLEY; INTEGRATED  
CAPITAL ASSOCIATES, INC., A  
Delaware Corporation; NANCY  
RILETT; RYAN TAM; CLAUDIA  
ENGLISH; TERESA PATTERSON;  
TANYA YOUNG; ROBERTO  
MARSELLA; REGINA OVENDEN; EMIL  
PESIRI; ERIC SULLIVAN; DOUGLAS H.  
WOLF; RICHARD BUCKINGHAM,  
*Plaintiffs-Appellants,*

v.

ALWYN FAREY-JONES; IRYNA A.  
KWASNY,  
*Defendants-Appellees.*

No. 03-15301  
D.C. No.  
CV-01-04166-MMC  
OPINION

Appeal from the United States District Court  
for the Northern District of California  
Maxine M. Chesney, District Judge, Presiding

Argued and Submitted  
April 2, 2003—San Francisco, California

Filed August 28, 2003

Before: Betty B. Fletcher, Alex Kozinski and  
Stephen S. Trott, Circuit Judges.

Opinion by Judge Kozinski

**COUNSEL**

Pamela Urueta, Kerr & Wagstaffe LLP, San Francisco, California, argued for appellants. James M. Wagstaffe, Kerr &

Wagstaffe LLP, and Richard Idell and Jennifer Marone, Idell, Berman & Seitel, joined her on the brief.

Robert E. White, San Francisco, California, argued for appellees. Susan C. Rushakoff joined him on the brief.

---

### OPINION

KOZINSKI, Circuit Judge:

We consider whether defendants violated federal electronic privacy and computer fraud statutes when they used a “patently unlawful” subpoena to gain access to e-mail stored by plaintiffs’ Internet service provider.

#### Background

Plaintiffs Wolf and Buckingham, officers of Integrated Capital Associates, Inc. (ICA), are embroiled in commercial litigation in New York against defendant Farey-Jones. In the course of discovery, Farey-Jones sought access to ICA’s e-mail. He told his lawyer Iryna Kwasny to subpoena ICA’s ISP, NetGate.

Under the Federal Rules, Kwasny was supposed to “take reasonable steps to avoid imposing undue burden or expense” on NetGate. Fed. R. Civ. P. 45(c)(1). One might have thought, then, that the subpoena would request only e-mail related to the subject matter of the litigation, or maybe messages sent during some relevant time period, or at the very least those sent to or from employees in some way connected to the litigation. But Kwasny ordered production of “[a]ll copies of emails sent or received by anyone” at ICA, with no limitation as to time or scope.

NetGate, which apparently was not represented by counsel, explained that the amount of e-mail covered by the subpoena

was substantial. But defendants did not relent. NetGate then took what might be described as the “Baskin-Robbins” approach to subpoena compliance and offered defendants a “free sample” consisting of 339 messages. It posted copies of the messages to a NetGate website where, without notifying opposing counsel, Kwasny and Farey-Jones read them. Most were unrelated to the litigation, and many were privileged or personal.

When Wolf and Buckingham found out what had happened, they asked the court to quash the subpoena and award sanctions. Magistrate Judge Wayne Brazil soundly roasted Farey-Jones and Kwasny for their conduct, finding that “the subpoena, on its face, was massively overbroad” and “patently unlawful,” that it “transparently and egregiously” violated the Federal Rules, and that defendants “acted in bad faith” and showed “at least gross negligence in the crafting of the subpoena.” He granted the motion to quash and socked defendants with over \$9000 in sanctions to cover Wolf and Buckingham’s legal fees. Defendants did not appeal that award.

Wolf, Buckingham and other ICA employees whose e-mail was included in the sample also filed this civil suit against Farey-Jones and Kwasny. They claim defendants violated the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, the Wiretap Act, 18 U.S.C. § 2511 *et seq.*, and the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, as well as various state laws. The district court held that none of the federal statutes applied, and dismissed the claims without leave to amend. It declined jurisdiction over the state law claims under 28 U.S.C. § 1367(c)(3). Plaintiffs now appeal.

### Analysis

[1] 1. The Stored Communications Act provides a cause of action against anyone who “intentionally accesses without authorization a facility through which an electronic communi-

cation service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage.” 18 U.S.C. §§ 2701(a)(1), 2707(a). “[E]lectronic storage” means either “temporary, intermediate storage . . . incidental to . . . electronic transmission,” or “storage . . . for purposes of backup protection.” *Id.* § 2510(17). The Act exempts, inter alia, conduct “authorized . . . by the person or entity providing a wire or electronic communications service,” *id.* § 2701(c)(1), or “by a user of that service with respect to a communication of or intended for that user,” *id.* § 2701(c)(2).

[2] The district court dismissed on the ground that NetGate had authorized defendants’ access. It held that this consent was not coerced, because the subpoena itself informed NetGate of its right to object. Plaintiffs contend that NetGate’s authorization was nonetheless invalid because the subpoena was patently unlawful. Their claim turns on the meaning of the word “authorized” in section 2701. We have previously reserved judgment on this question, *see Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 n.8 (9th Cir. 2002), while other circuits have considered related issues, *see, e.g., EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001) (holding access might be “unauthorized” under the Computer Fraud and Abuse Act if it is “not in line with the reasonable expectations” of the party granting permission (internal quotation marks omitted)); *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (holding access unauthorized where it is not “in any way related to [the system’s] intended function”).

[3] We interpret federal statutes in light of the common law. *See Beck v. Prupis*, 529 U.S. 494, 500-01 (2000). Especially relevant here is the common law of trespass. Like the tort of trespass, the Stored Communications Act protects individuals’ privacy and proprietary interests. The Act reflects Congress’s judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at

a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, *cf. Prosser and Keeton on the Law of Torts* § 13, at 78 (W. Page Keeton ed., 5th ed. 1984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.

[4] A defendant is not liable for trespass if the plaintiff authorized his entry. *See Prosser & Keeton* § 13, at 70. But “an overt manifestation of assent or willingness would not be effective . . . if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature and quality of the invasion intended.” *Id.* § 18, at 119; *cf. Restatement (Second) of Torts* §§ 173, 892B(2). Thus, the busybody who gets permission to come inside by posing as a meter reader is a trespasser. *J.H. Desnick, M.D., Eye Servs., Ltd. v. ABC*, 44 F.3d 1345, 1352 (7th Cir. 1995). So too is the police officer who, invited into a home, conceals a recording device for the media. *Cf. Berger v. Hanlon*, 129 F.3d 505, 516-17 (9th Cir. 1997), *vacated*, 526 U.S. 808 (1999), *reinstated in relevant part*, 188 F.3d 1155, 1157 (9th Cir. 1999).

[5] Not all deceit vitiates consent. “[T]he mistake must extend to the essential character of the act itself, which is to say that which makes it harmful or offensive, rather than to some collateral matter which merely operates as an inducement.” *Prosser & Keeton* § 18, at 120 (footnote omitted). In other words, it must be a “substantial mistake[ ] . . . concerning the nature of the invasion or the extent of the harm.” *Restatement (Second) of Torts* § 892B(2) cmt. g. Unlike the phony meter reader, the restaurant critic who poses as an ordinary customer is not liable for trespass, *Desnick*, 44 F.3d at 1351; nor, unlike the wired cop, is the invitee who conceals only an intent to repeat what he hears, *cf. Dietemann v. Time, Inc.*, 449 F.2d 245, 249 (9th Cir. 1971) (invasion of privacy claim). These results hold even if admission would have been refused had all the facts been known.

[6] These are fine and sometimes incoherent distinctions. *See Med. Lab. Mgmt. Consultants v. ABC*, 30 F. Supp. 2d 1182, 1201-04 (D. Ariz. 1998), *aff'd*, 306 F.3d 806 (9th Cir. 2002). But the theory is that some invited mistakes go to the essential nature of the invasion while others are merely collateral. Classification depends on the extent to which the intrusion trenches on “the specific interests that the tort of trespass seeks to protect.” *Desnick*, 44 F.3d at 1352; *see also Lewis v. United States*, 385 U.S. 206, 211 (1966); *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 517-18 (4th Cir. 1999).

[7] We construe section 2701 in light of these doctrines. Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances. Section 2701(c)(1) therefore provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access.

[8] Under this standard, plaintiffs have alleged facts that vitiate NetGate’s consent. NetGate disclosed the sample in response to defendants’ purported subpoena. Unbeknownst to NetGate, that subpoena was invalid. This mistake went to the essential nature of the invasion of privacy. The subpoena’s falsity transformed the access from a bona fide state-sanctioned inspection into private snooping. *See Restatement (Second) of Torts* § 174 (addressing “consent induced by fraud or mistake as to the validity of purported legal authority”); *cf. Bumper v. North Carolina*, 391 U.S. 543, 549 (1968) (“A search conducted in reliance upon a warrant cannot later be justified on the basis of consent if it turns out that the warrant was invalid.”). The false subpoena caused disclosure of documents that otherwise would have remained private; it effected an “invasion . . . of the specific interests that the [statute] seeks to protect.” *Desnick*, 44 F.3d at 1352.

[9] Defendants had at least constructive knowledge of the subpoena's invalidity. It was not merely technically deficient, nor a borderline case over which reasonable legal minds might disagree. It "transparently and egregiously" violated the Federal Rules, and defendants acted in bad faith and with gross negligence in drafting and deploying it.<sup>1</sup> They are charged with knowledge of its invalidity. *See Prosser & Keeton* § 18, at 119 (consent likely vitiated where defendants "ought to have known in the exercise of reasonable care" of the mistake).<sup>2</sup>

That NetGate could have objected is immaterial. The subpoena may not have been coercive, but it was deceptive, and that is an independent ground for invalidating consent. *See Restatement (Second) of Torts* § 892B(2)-(3). It was a piece of paper masquerading as legal process. NetGate produced the sample in response and doubtless would not have done so had it known the subpoena was void—particularly in light of its own legal obligation not to disclose such messages to third parties, *see* 18 U.S.C. § 2702(a)(1). That NetGate could have objected proves disclosure was not an inevitable consequence, but it was still a foreseeable one (and the intended one).

Allowing consent procured by known mistake to serve as

---

<sup>1</sup>Defendants had a full and fair opportunity to litigate the validity and good faith of the subpoena in the sanctions proceedings. Those proceedings were filed as a miscellaneous action on a separate docket from both the underlying New York litigation and the instant suit; defendants did not appeal. The magistrate's findings are therefore preclusive. *Cf.* 18 James Wm. Moore et al., *Moore's Federal Practice* § 132.03[4][k][vii], at 132-126 (3d ed. 1997) (judgment of contempt is issue preclusive); 3 Ronald E. Mallen & Jeffrey M. Smith, *Legal Malpractice* § 21.14, at 286 (5th ed. 2000) (attorney disciplinary proceedings may be issue preclusive).

<sup>2</sup>Prosser and Keeton say that constructive knowledge of a mistake is only "probably" sufficient to vitiate consent. *Prosser & Keeton* § 18, at 119. Whether or not ordinary negligence would suffice, the gross negligence and bad faith in this case are enough to charge defendants with constructive knowledge of the subpoena's invalidity.

a defense would seriously impair the statute's operation. A hacker could use someone else's password to break into a mail server and then claim the server "authorized" his access. Congress surely did not intend to exempt such intrusions—indeed, they seem the paradigm of what it sought to prohibit. *Cf. Morris*, 928 F.2d at 510 (access gained by guessing someone else's password is not "authorization" under the Computer Fraud and Abuse Act).

The subpoena power is a substantial delegation of authority to private parties, and those who invoke it have a grave responsibility to ensure it is not abused. Informing the person served of his right to object is a good start, *see* Fed. R. Civ. P. 45(a)(1)(D), but it is no substitute for the exercise of independent judgment about the subpoena's reasonableness. Fighting a subpoena in court is not cheap, and many may be cowed into compliance with even overbroad subpoenas, especially if they are not represented by counsel or have no personal interest at stake. Because defendants procured consent by exploiting a mistake of which they had constructive knowledge, the district court erred by dismissing based on that consent.

[10] Defendants ask us to affirm on the alternative ground that the messages they accessed were not in "electronic storage" and therefore fell outside the Stored Communications Act's coverage. *See* 18 U.S.C. § 2701(a)(1). The Act defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id.* § 2510(17), *incorporated by id.* § 2711(1). Several courts have held that subsection (A) covers e-mail messages stored on an ISP's server pending delivery to the recipient. *See In re Doubleclick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001); *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 635-36 (E.D. Pa. 2001); *cf. Steve Jackson*

*Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461-62 (5th Cir. 1994) (messages stored on a BBS pending delivery). Because subsection (A) applies only to messages in “temporary, intermediate storage,” however, these courts have limited that subsection’s coverage to messages not yet delivered to their intended recipient. See *Doubleclick*, 154 F. Supp. 2d at 512; *Fraser*, 135 F. Supp. 2d at 636.

[11] Defendants point to these cases and argue that messages remaining on an ISP’s server after delivery no longer fall within the Act’s coverage. But, even if such messages are not within the purview of subsection (A), they do fit comfortably within subsection (B). There is no dispute that messages remaining on NetGate’s server after delivery are stored “by an electronic communication service” within the meaning of 18 U.S.C. § 2510(17)(B). Cf. *Doubleclick*, 154 F. Supp. 2d at 511 (holding that subsection (B) did not apply because the communications at issue were not being stored by an electronic communication service). The only issue, then, is whether the messages are stored “for purposes of backup protection.” 18 U.S.C. § 2510(17)(B). We think that, within the ordinary meaning of those terms, they are.

[12] An obvious purpose for storing a message on an ISP’s server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user’s own computer. The ISP copy of the message functions as a “backup” for the user. Notably, nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user. Storage under these circumstances thus literally falls within the statutory definition.<sup>3</sup>

---

<sup>3</sup>That defendants did not read the messages until NetGate posted them to a website is immaterial. Defendants’ unlawful subpoena caused NetGate to retrieve the messages from electronic storage and make them available. That constitutes “access” within the meaning of the Act.

One district court reached a contrary conclusion, holding that “backup protection” includes only temporary backup storage pending delivery, and not any form of “post-transmission storage.” See *Fraser*, 135 F. Supp. 2d at 633-34, 636. We reject this view as contrary to the plain language of the Act. In contrast to subsection (A), subsection (B) does not distinguish between intermediate and post-transmission storage. Indeed, *Fraser*’s interpretation renders subsection (B) essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as “temporary, intermediate storage” within the meaning of subsection (A). By its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission.

[13] Because plaintiffs’ e-mail messages were in electronic storage regardless of whether they had been previously delivered, the district court’s decision cannot be affirmed on this alternative ground.<sup>4</sup>

[14] 2. Plaintiffs also claim a violation of the Wiretap Act, which authorizes suit against those who “intentionally intercept[ ] . . . any wire, oral, or electronic communication.” 18 U.S.C. §§ 2511(1)(a), 2520(a). We recently held in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002), that the Act applies only to “acquisition contemporaneous with transmission.” *Id.* at 878. Specifically, “Congress did not intend for “intercept” to apply to “electronic communications” when those communications are in “electronic stor-

---

<sup>4</sup>Defendants urge us to affirm on the additional ground that the complaint at one point alleges they “access[ed] . . . Plaintiffs’ computer systems through which electronic communications systems are provided.” Resp. Br. of Def./Appellee at 16 (emphasis added). Plaintiffs’ computers, they note, are not “facilities” covered by 18 U.S.C. § 2701(a)(1). *Id.* at 15. We construe complaints liberally, however, see *Lynn v. Sheet Metal Workers’ Int’l Ass’n*, 804 F.2d 1472, 1482 (9th Cir. 1986), and the substance of plaintiffs’ claims is that defendants improperly accessed *NetGate*’s servers.

age.’ ’ ’” *Id.* at 877 (quoting *Steve Jackson Games*, 36 F.3d at 462). *Konop* is dispositive, and the district court correctly dismissed the claim.

**[15]** 3. Plaintiffs finally claim a violation of the Computer Fraud and Abuse Act, which provides a cause of action against one who, inter alia, “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication.” 18 U.S.C. § 1030(a)(2)(C), (g). The conduct must involve one of five factors listed in 18 U.S.C. § 1030(a)(5)(B), which include a loss in excess of \$5000. *Id.* § 1030(a)(5)(B)(i), (g).<sup>5</sup>

The district court dismissed without leave to amend on the theory that the Act does not apply to unauthorized access of a third party’s computer. It also dismissed for failure to allege damages or loss, though it noted that this omission might be cured by amendment. Plaintiffs do not dispute the latter defect, but urge us to reverse as to the former ground so they can amend.

**[16]** The district court erred by reading an ownership or control requirement into the Act. The civil remedy extends to “[a]ny person who suffers damage or loss by reason of a violation of this section.” 18 U.S.C. § 1030(g) (emphasis added). “[T]he word “any” has an expansive meaning, that is, “one or some indiscriminately of whatever kind.’ ’ ” *HUD v. Rucker*, 535 U.S. 125, 131 (2002) (quoting *United States v. Gonzales*, 520 U.S. 1, 5 (1997)). Nothing in the provision’s language supports the district court’s restriction. Individuals other than the computer’s owner may be proximately harmed

---

<sup>5</sup>Defendants argue that subsection (a)(5)(A) prescribes the Act’s only civil offenses. But subsection (g) applies to any violation of “this section” and, while the offense must involve one of the five factors in (a)(5)(B), it need not be one of the three offenses in (a)(5)(A).

by unauthorized access, particularly if they have rights to data stored on it.

Defendants argue in the alternative that NetGate authorized their access. Our earlier discussion disposes of this defense. They further contend that any damages or loss plaintiffs suffered do not fall within the Act's ambit. Because plaintiffs have not yet alleged the damages or loss they suffered, it would be premature to consider the argument.

4. Defendants contend they are immune from liability under the *Noerr-Pennington* doctrine, which exempts petitioning of public authorities from civil liability on First Amendment grounds. See *Manistee Town Ctr. v. City of Glendale*, 227 F.3d 1090, 1092 (9th Cir. 2000); *Kottle v. Northwest Kidney Ctrs.*, 146 F.3d 1056, 1059 (9th Cir. 1998). Lawsuits are protected by the doctrine because they are essentially petitions to the courts for redress of grievances. See *Cal. Motor Transp. Co. v. Trucking Unlimited*, 404 U.S. 508, 510 (1972). The doctrine is typically invoked to immunize the act of petitioning itself—i.e., the filing of the lawsuit. But it has been extended to certain conduct “incidental to the prosecution of the suit,” for example, deciding whether to settle a claim. See *Columbia Pictures Indus., Inc. v. Prof'l Real Estate Investors, Inc.*, 944 F.2d 1525, 1528-29 (9th Cir. 1991), *aff'd*, 508 U.S. 49 (1993). Defendants seize on this language from *Columbia Pictures* and argue that, because the subpoena was incidental to their litigation, they are entitled to immunity.

We are skeptical that *Noerr-Pennington* applies at all to the type of conduct at issue. Subpoenaing private parties in connection with private commercial litigation bears little resemblance to the sort of governmental petitioning the doctrine is designed to protect. Nevertheless, assuming *arguendo* the defense is available, it fails. *Noerr-Pennington* does not protect “objectively baseless” sham litigation. See *Prof'l Real Estate Investors, Inc. v. Columbia Pictures Indus., Inc.*, 508

U.S. 49, 60 (1993). The magistrate judge found that the subpoena was “transparently and egregiously” overbroad and that defendants acted with gross negligence and in bad faith. This is tantamount to a finding that the subpoena was objectively baseless.

Defendants urge us to look only at the merits of the underlying litigation, not at the subpoena. They apparently think a litigant should have immunity for any and all discovery abuses so long as his lawsuit has some merit. Not surprisingly, they offer no authority for that implausible proposition. Assuming *Noerr-Pennington* applies at all, we hold that it is no bar where the challenged discovery conduct itself is objectively baseless.<sup>6</sup>

5. Having dismissed all the federal claims, the district court declined jurisdiction over the pendent state law claims under 28 U.S.C. § 1367(c)(3). Because we reverse dismissal of some of the federal claims, we also reinstate the state claims.

[17] We REVERSE dismissal of the Stored Communications Act claim, AFFIRM dismissal of the Wiretap Act claim, and REVERSE dismissal with prejudice of the Computer Fraud and Abuse Act claim with instructions to dismiss with leave to amend. We also REVERSE dismissal of the state claims.

**AFFIRMED in part, REVERSED in part and remanded. Costs to appellants.**

---

<sup>6</sup>*Noerr-Pennington*'s sham litigation exception also requires proof of subjective intent to use legal process to achieve the evil prohibited by the statute from which exemption is claimed. See *Prof'l Real Estate Investors*, 508 U.S. at 60-61. That prong of the test is also satisfied here; presumably, the purpose of any objectively baseless subpoena is to uncover private information.