FOR PUBLICATION

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

SUZLON ENERGY LTD., *Petitioner-Appellant,* and RAJAGOPALAN SRIDHAR, *Intervenor-Defendant-Appellee,* v. MICROSOFT CORPORATION, *Respondent-Appellee.*	No. 10-35793 D.C. No. 2:10-cv-0170-MJP OPINION

Appeal from the United States District Court
for the Western District of Washington
Marsha J. Pechman, District Judge, Presiding

Argued and Submitted
August 3, 2011—Seattle, Washington

Filed October 3, 2011

Before: John T. Noonan and Milan D. Smith, Jr.,
Circuit Judges, and Andrew J. Guilford,* District Judge.

Opinion by Judge Guilford

*The Honorable Andrew J. Guilford, United States District Judge for the Central District of California, sitting by designation.

COUNSEL

Jeremy J. O. Harwood, New York, New York, for the petitioner-appellant.

Blake Marks-Dias, Seattle, Washington, for the respondent-appellee.

Michael A. Barcott, Seattle, Washington, for the intervenor-defendant-appellee.

OPINION

GUILFORD, District Judge:

While the parties in this case raise issues of international policy, constitutional rights, and the fortuities of the Internet age, this case ultimately turns on the plain language of the relevant statute. Suzlon Energy Ltd. ("Suzlon") has demanded that Microsoft Corp. ("Microsoft") produce documents from the Microsoft Hotmail email account of Rajagopalan Sridhar, an Indian citizen imprisoned abroad. Microsoft objected to the production and the district court agreed, finding that Sridhar was entitled to the protection of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510-2522, even though he was a foreign citizen. We affirm.

BACKGROUND

The facts of this case are straightforward and largely undisputed, with any disputed facts not affecting the resolution of this case. Suzlon sought emails under 28 U.S.C. § 1782 to use in a civil fraud proceeding pending against Sridhar and others in the Federal Court of Australia (the "Australian Proceedings"). Although Sridhar is a citizen of India and is imprisoned abroad, the relevant emails are stored on a domestic server by a domestic corporation, Microsoft. The district court initially granted Suzlon's petition for production of documents ("Production Order"). In response, Microsoft filed objections that the district court deemed to be a motion to quash.

Microsoft and Sridhar raised several arguments below to support the motion to quash. First, Microsoft argued that the documents sought must be discoverable in the foreign proceeding. The district court rejected this argument based on *Intel Corp. v. Advanced Micro Devices, Inc.*, 542 U.S. 241 (2004), which held that nothing in the text of § 1782 imposed such a limitation. *Id.* at 260. Second, Microsoft argued that

the subpoenas must comply with the Federal Rules of Civil Procedure. But § 1782 states that the Federal Rules of Civil Procedure only apply to the extent the order granting discovery does not provide other procedures, and the Production Order specified a procedure. Thus, the district court rejected the second argument as well. Third, Microsoft and Sridhar argued that production of the emails would violate the ECPA. The district court agreed with this third argument, held that the plain terms of the statute applied the ECPA to all persons, and granted the motion to quash ("Quash Order"). Suzlon now appeals the district court's finding that the ECPA applies to foreign citizens such as Sridhar, focusing on the third argument. Suzlon also argues that Sridhar's participation in this suit is an implied consent to the production of documents.

DISCUSSION

1. ECPA

The threshold question in this case is whether the plain language of the ECPA extends to foreign citizens. *See, e.g.*, *Lamie v. U.S. Trustee,* 540 U.S. 526, 534 (2004) ("The starting point in discerning congressional intent is the existing statutory text[.]") If the Court finds that the plain language of the statute is clear on its face, the Court does not need to consider the legislative history and policy of the ECPA, although they may still be instructive. *See id.* at 539 (finding it "unnecessary to rely on the legislative history" when the plain language of the statute was clear, but finding it an "instructive" way to "lend support" to its holding); *see also Am. Rivers v. FERC*, 201 F.3d 1186, 1204 (9th Cir. 1999) ("[W]e are mindful that this Court steadfastly abides by the principle that 'legislative history—no matter how clear—can't override statutory text.' ") (quoting *Hearn v. W. Conference of Teamsters Pension Trust Fund*, 68 F.3d 301, 304 (9th Cir. 1995)).

1.1 Statutory Framework of the ECPA

As noted, Suzlon filed a petition for production of documents to assist in the Australian Proceedings. Suzlon sought this relief under 28 U.S.C. § 1782, which states in part:

> The district court of the district in which a person resides or is found may order him to give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal, including criminal investigations conducted before formal accusation. The order may be made pursuant to a letter rogatory issued, or request made, by a foreign or international tribunal or upon the application of any interested person and may direct that the testimony or statement be given, or the document or other thing be produced, before a person appointed by the court. . . .

[1] The Ninth Circuit has previously held that the ECPA limits § 1782 by making it illegal for an entity that provides an electronic communication service to the public to produce the contents of its stored communications. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1071-72, 1077 (9th Cir. 2004) (finding that a civil subpoena to plaintiff's internet service provider violated the ECPA). The relevant provision of the ECPA states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). The ECPA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). The ECPA defines a "user" as "*any person* or entity who — (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13) (emphasis added).

[2] The question now presented is whether the protections of the ECPA extend to the contents of communications of *foreign citizens.* In other words, does the mere fact that Sridhar happens to lack U.S. citizenship mean that Microsoft has to produce his emails under a § 1782 order? The answer depends on the proper interpretation of "any person" in § 2510(13). To resolve this dispute, the Court turns to the plain text of the statute.

1.2 Plain Text of the ECPA

[3] The Court affirms the district court's finding that the plain text of the ECPA applies its terms to "any person," without qualification. 18 U.S.C. § 2510(13). Any person means any person, including foreign citizens.

The Court also finds that the statute as a whole confirms that Congress intended the term "any person" to cover non-citizens. Two strong arguments bolster this conclusion. First, 18 U.S.C. § 2702(b) and (c) list numerous exceptions to the rule as set forth in § 2702(a), which prohibits the knowing divulgence of the contents of a communication while in electronic storage. But neither § 2702(b) nor (c) list citizenship as an exception.

[4] Second, 18 U.S.C. § 2510(13) defines a user as "any person or entity who — (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." The statute starts with the very broad term "any person or entity" and then limits it with two conjunctive qualifications. Microsoft and Sridhar argue that Congress could have added other requirements, such as U.S. citizenship, if that were the intent behind the ECPA. The fact that Congress did not do so indicates that it did not want to impose any additional limitations.

The reasoning of *O'Rourke v. U.S. Dept. of Justice*, 684 F. Supp. 716 (D.D.C. 1988) supports the Court's analysis. In

O'Rourke, the court found that the phrase "any person" in the Freedom of Information Act ("FOIA"), 5 U.S.C. §§ 551 *et seq.*, should be read according to its plain meaning. *Id.* at 718. The court stated, "On its face, then, the statute's provisions are not restricted to citizens." *Id.* The *O'Rourke* court contrasted the FOIA language with a provision in the Privacy Act, 5 U.S.C. § 552a(a)(2), which specified that its provisions apply only to "a citizen of the United States or an alien lawfully admitted." *Id.* The *O'Rourke* court concluded that "Congress thus distinguishes between a 'citizen' and 'any person' when it wishes to do so." *Id.* Like the FOIA statute, the ECPA does not facially restrict its applicability to U.S. citizens. And as the court recognized in *O'Rourke*, Congress knows how to explicitly limit a statute to U.S. citizens when it intends to do so.

[5] The Court finds that the plain language of the ECPA extends its protections to non-citizens. The Court is therefore obligated to enforce the statute as written. *See Lamie*, 540 U.S. at 534 ("It is well established that when the statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms.") (quoting *Hartford Underwriters Ins. Co. v. Union Planters Bank, N. A.*, 530 U.S. 1, 6 (2000) (internal quotation marks omitted)).

1.3 Legislative History of the ECPA

Because we find that the plain language of the ECPA is clear, we accept the district court's finding that it did not need to consider the legislative history of the ECPA. Stated otherwise, "[l]egislative history cannot trump the statute." *Bonneville Power Admin. v. FERC*, 422 F.3d 908, 920 (9th Cir. 2005).

Still, the Court will analyze the statute's history for its instructive value. Suzlon argues that the ECPA was enacted

against a backdrop of Fourth Amendment protections, citing the following passage:

> With the advent of computerized record keeping systems Americans have the ability to lock away a great deal of personal and business information . . . [T]he law must advance with technology to ensure the continued vitality of the fourth amendment. . . . Congress must act to protect the privacy of our citizens . . . The Committee believes that [this Act] represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.

S. Rep. No. 99-541, at 3557-59 (1986).

This passage indicates that Congress' primary intent in passing the ECPA was to protect the privacy interests of American citizens. Suzlon therefore argues that the intent of the ECPA was to protect *only* American citizens. But the fact that the ECPA was intended to shore up Fourth Amendment rights does not mean that Congress specifically intended to exclude foreign citizens from the scope of the Amendment.

To the contrary, to fully protect American citizens it might be necessary to extend the ECPA to all domestic communications, regardless of who sent them. Further, Suzlon's restrictive reading of the ECPA would put email service providers in an untenable position. By limiting the ECPA only to those people entitled to Fourth Amendment protection, as urged by Suzlon, an email service provider would need to assess whether a particular account holder was at all times a U.S. citizen, or later became a citizen, or was a resident alien with some Fourth Amendment protection, or if there were other reasons to provide Fourth Amendment rights. This would be a costly, fact-intensive, and difficult determination. But under Microsoft's interpretation of "any person," it's clear that the ECPA at least applies whenever the requested documents are

stored in the United States. The Court does not address here whether the ECPA applies to documents stored or acts occurring outside of the United States. *See Zheng v. Yahoo! Inc.*, 2009 WL 4430297 at *4, No. C-08-1068 MMC (Dec. 2, 2009) (finding that the EPCA does not cover acts outside of the United States).

Suzlon also argues that nowhere in the legislative history or text of the ECPA does Congress address civil litigation, indicating that perhaps Congress intended for the ECPA to only apply to government law enforcement. This argument ignores Ninth Circuit cases holding exactly the opposite. *Theofel*, 359 F.3d at 1071-72, 1077 (applying the ECPA to subpoena requests). As before, even if Congress' most pressing concern was law enforcement agencies issuing subpoenas, that does not mean that Congress was not also concerned about civil litigants issuing discovery requests. Declaring an implicit exception to the ECPA for civil litigation would erode the safety of the stored electronic information and trigger Congress' privacy concerns. *See id.* at 1073-74 (finding that because the "subpoena caused disclosure of documents that otherwise would have remained private[,]" it invaded "the specific interests that the [EPCA] seeks to protect." (citations and quotation marks omitted)).

[6] We conclude that nothing in the legislative history clearly refutes the plain language of the text. In fact, the underlying policy implications of the statute are most consistent with the plain text of the ECPA. Thus, the Court remains firm in its initial finding that the ECPA unambiguously applies to foreign citizens.

2. IMPLIED CONSENT

[7] As a further argument, Suzlon claims that Sridhar gave his implied consent to the production of his documents. The district court's Quash Order did not address this point, per-

haps failing, as does this Court, to see the logic of Suzlon's claim.

Suzlon argues that under Australian civil litigation rules, a litigant is obligated to list and disclose documents that would include the emails at issue, much as a party in the United States has a duty to produce certain documents under the Federal Rules of Procedure. Sridhar is a defendant in a case in Australia. Thus, Suzlon argues that Sridhar has somehow consented to the production of his emails because he has a duty to produce documents under the Australian rules of court.

Under Suzlon's own reasoning, *Sridhar* himself is the person who should be responsible for disclosing his own emails. Suzlon's supposed implied consent argument has no bearing on its efforts to get those emails from Microsoft, who is not a party to the litigation. Not surprisingly, Microsoft takes no position on the issue of whether Sridhar could be deemed to have given implied consent in this particular case.

[8] In contrast, Sridhar vigorously argues—both in his papers and at oral argument—that his actions do not establish implied consent. Sridhar argues that he has consistently objected to the disclosure of his Hotmail emails and, accordingly, has not consented to their production.

[9] Nor has Sridhar consented to Microsoft producing his emails on his behalf. He reasonably relied upon his Hotmail service agreement, which stated that his emails would be disclosed only according to U.S. law and under other circumstances not relevant here. Microsoft never told Sridhar that his communications might be monitored or disclosed. Thus, there is no argument that Sridhar waived his reasonable expectation of privacy by continuing to use the service after such notice. *See, e.g., Flagg v. City of Detroit*, 252 F.R.D. 346, 366 (E.D. Mich. 2008) (finding that implied consent rests on a theory of waiver, such as when a person uses a service after being informed of a policy of disclosure and monitoring.)

[10] We find that Suzlon's argument for implied consent fails.

CONCLUSION

The ECPA protects the domestic communications of non-citizens like Sridhar. Thus, the decision of the district court denying the production of documents is **AFFIRMED**.