Optiver Austraila Pty Ltd. & Anor. v. Tibra Trading Pty Ltd. & Ors. Doc. 16

United States District Court
For the Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

OPTIVER AUSTRALIA PTY. LTD. & ANOR., Plaintiff, v. TIBRA TRADING PTY. LTD. & ORS., Defendant.	Case No.: C 12-80242 EJD (PSG) **ORDER GRANTING-IN-PART MOTION TO QUASH SUBPOENA IN A CIVIL CASE** **(Re: Docket No. 11)**

Before the court is the persnickety, but persistent, question of exactly what qualifies as "content," whose disclosure by service providers is prohibited under the Stored Communications Act. On November 7, 2012, Tibra Trading Pty Ltd. & Ors. ("Tibra") moved to quash a subpoena issued by Optiver Australia Pty. Ltd. & Anor. ("Optiver") to obtain certain discovery from Google, Inc. ("Google") for use in a foreign proceeding. Optiver opposes the motion. On December 18, the parties appeared for oral argument. Having reviewed the papers and considered the arguments of counsel, the court GRANTS-IN-PART Tibra's motion.

Dockets.Justia.com

I. BACKGROUND[1]

Optiver is a trading firm. In the underlying proceeding in the Federal Court of Australia, Optiver alleges that several of its former employees copied Optiver's proprietary source code, left Optiver, and used the code to found Tibra in 2006. In the Australian proceeding, Optiver sought discovery from Tibra of emails sent and received by individual parties related to the Optiver source code. Tibra produced a number of emails, but Optiver suspected that key emails relating to the allegedly stolen code were previously deleted. In response, the Federal Court of Australia ruled Tibra's responses were inadequate and ordered further discovery. The court's order specifically contemplated Optiver seeking leave of a United States court to allow Optiver to obtain discovery from Google.[2]

On October, 9, 2012, Optiver filed ex parte for judicial assistance pursuant to 28 U.S.C. § 1782 to serve a subpoena upon Google for documents to be used in the foreign proceeding.[3] The court granted Optiver's ex parte application.[4] Soon thereafter, Optiver issued a subpoena to Google regarding a number of electronic communications sent or received by certain Gmail accounts allegedly used by employees of Tibra. Optiver's requests consist of two requests:[5]

Request One: Documents sufficient to identify the recipient(s), sender, subject, date sent, date received, date read, and date deleted of emails, email attachments, or Google Talk messages that contain either of the terms "PGP" or "Optiver" (case insensitive) sent or received between

---

[1] Unless otherwise noted, the factual background undisputed and is taken from Optiver's "Memorandum in Support of Motion for Judicial Assistance Pursuant to 28 U.S.C. Section 1782." See Docket No. 2, 3.

[2] The court understands that discovery from Google under the authority of the Australian Court was unavailing. See Docket No. 3 ¶ 8.

[3] See Docket No. 1.

[4] See Docket No. 6.

[5] See Docket No. 5, 11-12.

January 1, 2006 and December 31, 2007 for the following email addresses: (email addresses omitted).

Request Two: Documents sufficient to show the recipient(s), sender, subject, date sent, date received, date read, and date deleted of emails, email attachments, or Google Talk messages sent or received between November 3, 2005 to December 31, 2009 that were sent to or from the above-listed email addresses and to or from the following email addresses: (email addresses omitted).

Tibra now moves to quash the subpoena.

II. LEGAL STANDARD

By now it is well-established that civil subpoenas, including those issued pursuant to 28 U.S.C. § 1782, are subject to the prohibitions of the Stored Communications Act ("SCA").[6] Congress passed the SCA in 1986 because "the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address."[7]

The SCA prohibits service providers from knowingly disclosing the contents of a user's electronic communications.[8] The SCA 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."[9] The "contents" of a

[6] See Theofel v. Farey-Jones, 359 F.3d 1066, 1071-72, 1077 (9th Cir. 2004) (holding that the SCA applies in the civil subpoena context); Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 718 (9th Cir. 2011) (holding that the SCA applies to a subpoena issued under 28 U.S.C. § 1782).

[7] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir.2008) (rev'ed in part on other grounds) (citing Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L.Rev. 1208, 1209–13 (2004)).

[8] See 18 U.S.C. § 2701, et seq.

[9] Id. subsection (a)(1).

"wire, oral, or electronic communication" is defined as "any information concerning the substance, purport, or meaning of that communication."[10]

III. DISCUSSION

A. Request One Impermissible Seeks Content by Requesting Communications Containing the Terms "PGP" or "Optiver" in the Substance of the Communication

Optiver's Request One seeks information pertaining to emails, email attachments and Google Talk messages containing the terms "PGP" or "Optiver." Tibra argues that by requesting emails and such containing these terms, Optiver is requesting content of the communications in violation of the SCA. Optiver responds that "PGP" is the name of an encryption system, not content. Optiver also argues it wants documents mentioning "Optiver" not to discover the substance of the communications, but to locate communications that might be relevant to the foreign litigation. Optiver notes that if the email has been encrypted through PGP, it cannot access the content without the proper encryption key and pass phrase, which it does not have.

Optiver misses the point. The SCA prohibits any knowing disclosure by service providers of the content of electronic communications, no matter how insignificant. The search proposed by Optiver would necessarily reveal that the emails identified contain the terms "PGP" or "Optiver," which are words contained in the body of the communications. These terms constitute content, or information concerning the "substance, purport, or meaning" of the communications. However trivial, this is exactly the sort of information the SCA sought to protect.[11]

[10] See 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(8).

[11] Cf. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 969 (C.D. Cal 2010) (quashing subpoena that sought all communications referring to certain keywords).

B. Requests One and Two Seek the Subject Lines of the Emails, Which are Content under the SCA

Tibra next contends that both Requests One and Two violate the SCA because they seek the subject lines of the email communications and Google Talk messages.

It is clear from the purpose and nature of the subject line that it is "content" intended to fall under the protection of the SCA. The subject lines of emails and other electronic communications serve to convey a substantive message about the body of the email. In the sense that they communicate information concerning the "substance, purport, or meaning" of the topic of the email, subject lines are no different from the body of the email. In contrast to, say, subscriber information,[12] revealing the subject line would necessarily reveal information about the substance of the communication.[13] In fact, a message's subject line is nothing less than a pithy summary of the message's content.

Materials from the U.S. Department of Justice and the legislative history of the SCA underscore the notion that subject lines are content. The U.S. Department of Justice manual advises United States Attorneys that subject lines are considered "content" under the SCA.[14] The legislative history of the SCA shows that Congress appreciated that subject lines would be included

[12] See Mintz v. Mark Bartelstein & Associates, Inc., Case No. 12-02554 SVW SSX, 2012 WL 3553351 (C.D. Cal. Aug. 14, 2012).

[13] Cf. In re United States for an Order Authorizing the Use of a Pen Register & Trap, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) (holding that "the information contained in the 'subject' would reveal the contents of the communication and would not be properly disclosed pursuant to a pen register or trap and trace device"). While this case considered the Wiretap Act and not the SCA, the SCA explicitly adopted the definition of the "content" set forth in the Wiretap Act. See 18 U.S.C. § 2711(1).

[14] See U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations, 123, 148 at n.15 (2001). See also Kerr, supra, at 1228 (noting "[i]t is also fairly clear that the subject line of the e-mail counts as 'contents,' as the subject line generally carries a substantive message.")

within the meaning of "content": the House Report on the USA PATRIOT Act and the PATRIOT Act amendments state that email subject lines are "clearly content."[15]

C. Optiver is Entitled to Non-Content Metadata

In the event the court finds that the requests seek impermissible content, Optiver asks that the court only quash the portion that violates the SCA. The court struggles to understand how such information would be helpful to Optiver, who states its goal in requesting this information is to "seek[] data regarding these email accounts to potentially support its arguments in the Federal Court of Australia that Tibra has intentionally destroyed evidence that indicates it stole Optiver's source code."[16] But Optiver is entitled to such non-content metadata, and such metadata it shall receive.[17]

IV. CONCLUSION

The SCA offers broad protection against disclosure of content by service providers. Optiver's Request One is invalid because it seeks disclosure of the terms "Optiver" and "PGP," so Tibra's motion to quash Request One is GRANTED. Request Two violates the SCA insofar as it seeks the subject of the communications, but the remainder is permissible. Accordingly, consistent with the remainder of the subpoena, Google is required to provide only the following information: "Documents sufficient to show the recipient(s), sender, date sent, date received, date read, and date

---

[15] H.R. Rep. No. 107-236, Part 1, at p. 53 (2001) ("Thus, for example, an order under the [SCA] could not authorize the collection of email subject lines, which are clearly content").

Tibra further argues Requests One and Two impermissibly seek the file names of email attachments, which it argues are content under the SCA. In its response, however, Optiver explicitly disclaims any interest in the attachments, mooting the argument. See Docket No. 13 at 6.

[16] Docket No. 13 at 3.

[17] See Beluga Shipping GMBH & Co. KS BELUGA FANTASTIC v. Suzlon Energy LTD., Case No. 10-80034 JW PVT, 2010 WL 3749279 (N.D. Cal. Sept. 23, 2010) (holding that Google, as a service provider, was only required to produce non-content information such as names of the email account holders, when the email accounts were created, and the countries from which the email accounts were created).

deleted of emails, email attachments, or Google Talk messages sent or received between November 3, 2005 to December 31, 2009 that were sent to or from" the email addresses listed.

IT IS SO ORDERED.

Dated: January 23, 2013

PAUL S. GREWAL
United States Magistrate Judge

United States District Court
For the Northern District of California