



## I. BACKGROUND<sup>1</sup>

1  
2 Optiver is a trading firm. In the underlying proceeding in the Federal Court of Australia,  
3 Optiver alleges that several of its former employees copied Optiver's proprietary source code, left  
4 Optiver, and used the code to found Tibra in 2006. In the Australian proceeding, Optiver sought  
5 discovery from Tibra of emails sent and received by individual parties related to the Optiver source  
6 code. Tibra produced a number of emails, but Optiver suspected that key emails relating to the  
7 allegedly stolen code were previously deleted. In response, the Federal Court of Australia ruled  
8 Tibra's responses were inadequate and ordered further discovery. The court's order specifically  
9 contemplated Optiver seeking leave of a United States court to allow Optiver to obtain discovery  
10 from Google.<sup>2</sup>

11  
12 On October, 9, 2012, Optiver filed ex parte for judicial assistance pursuant to 28 U.S.C. §  
13 1782 to serve a subpoena upon Google for documents to be used in the foreign proceeding.<sup>3</sup> The  
14 court granted Optiver's ex parte application.<sup>4</sup> Soon thereafter, Optiver issued a subpoena to  
15 Google regarding a number of electronic communications sent or received by certain Gmail  
16 accounts allegedly used by employees of Tibra. Optiver's requests consist of two requests:<sup>5</sup>

17  
18 **Request One:** Documents sufficient to identify the recipient(s), sender, subject, date sent,  
19 date received, date read, and date deleted of emails, email attachments, or Google Talk messages  
20 that contain either of the terms "PGP" or "Optiver" (case insensitive) sent or received between  
21

22  
23 <sup>1</sup> Unless otherwise noted, the factual background undisputed and is taken from Optiver's  
24 "Memorandum in Support of Motion for Judicial Assistance Pursuant to 28 U.S.C. Section 1782."  
*See* Docket No. 2, 3.

25 <sup>2</sup> The court understands that discovery from Google under the authority of the Australian Court  
was unavailing. *See* Docket No. 3 ¶ 8.

26 <sup>3</sup> *See* Docket No. 1.

27 <sup>4</sup> *See* Docket No. 6.

28 <sup>5</sup> *See* Docket No. 5, 11-12.

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

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

8  
9 Tibra now moves to quash the subpoena.

## 10 II. LEGAL STANDARD

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

15 The SCA prohibits service providers from knowingly disclosing the contents of a user’s  
16 electronic communications.<sup>8</sup> The SCA states that “a person or entity providing an electronic  
17 communication service to the public shall not knowingly divulge to any person or entity the  
18 contents of a communication while in electronic storage by that service.”<sup>9</sup> The “contents” of a  
19

20  
21  
22  
23 <sup>6</sup> See *Theofel v. Farey-Jones*, 359 F.3d 1066, 1071-72, 1077 (9th Cir. 2004) (holding that the SCA  
24 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).

25 <sup>7</sup> *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir.2008) (rev’ed in part on  
26 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)).

27 <sup>8</sup> See 18 U.S.C. § 2701, *et seq.*

28 <sup>9</sup> *Id.* subsection (a)(1).

1 “wire, oral, or electronic communication” is defined as “any information concerning the substance,  
2 purport, or meaning of that communication.”<sup>10</sup>

### 3 III. DISCUSSION

#### 4 A. Request One Impermissible Seeks Content by Requesting Communications 5 Containing the Terms “PGP” or “Optiver” in the Substance of the 6 Communication

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

15 Optiver misses the point. The SCA prohibits any knowing disclosure by service providers  
16 of the content of electronic communications, no matter how insignificant. The search proposed by  
17 Optiver would necessarily reveal that the emails identified contain the terms “PGP” or “Optiver,”  
18 which are words contained in the body of the communications. These terms constitute content, or  
19 information concerning the “substance, purport, or meaning” of the communications. However  
20 trivial, this is exactly the sort of information the SCA sought to protect.<sup>11</sup>

21  
22  
23  
24  
25  
26 <sup>10</sup> See 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(8).

27 <sup>11</sup> Cf. *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 969 (C.D. Cal 2010) (quashing  
28 subpoena that sought all communications referring to certain keywords).

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

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

5                   It is clear from the purpose and nature of the subject line that it is “content” intended to fall  
6                   under the protection of the SCA. The subject lines of emails and other electronic communications  
7                   serve to convey a substantive message about the body of the email. In the sense that they  
8                   communicate information concerning the “substance, purport, or meaning” of the topic of the  
9                   email, subject lines are no different from the body of the email. In contrast to, say, subscriber  
10                  information,<sup>12</sup> revealing the subject line would necessarily reveal information about the substance  
11                  of the communication.<sup>13</sup> In fact, a message’s subject line is nothing less than a pithy summary of  
12                  the message’s content.

13                  Materials from the U.S. Department of Justice and the legislative history of the SCA  
14                  underscore the notion that subject lines are content. The U.S. Department of Justice manual  
15                  advises United States Attorneys that subject lines are considered “content” under the SCA.<sup>14</sup> The  
16                  legislative history of the SCA shows that Congress appreciated that subject lines would be included  
17                  18

19  
20  
21                  <sup>12</sup> See *Mintz v. Mark Bartelstein & Associates, Inc.*, Case No. 12-02554 SVW SSX, 2012 WL  
22                  3553351 (C.D. Cal. Aug. 14, 2012).

23                  <sup>13</sup> Cf. *In re United States for an Order Authorizing the Use of a Pen Register & Trap*, 396 F. Supp.  
24                  2d 45, 48 (D. Mass. 2005) (holding that “the information contained in the ‘subject’ would reveal  
25                  the contents of the communication and would not be properly disclosed pursuant to a pen register  
26                  or trap and trace device”). While this case considered the Wiretap Act and not the SCA, the SCA  
27                  explicitly adopted the definition of the “content” set forth in the Wiretap Act. See 18 U.S.C. §  
28                  2711(1).

29                  <sup>14</sup> See U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Evidence in Criminal*  
30                  *Investigations*, 123, 148 at n.15 (2001). See also Kerr, *supra*, at 1228 (noting “[i]t is also fairly  
31                  clear that the subject line of the e-mail counts as ‘contents,’ as the subject line generally carries a  
32                  substantive message.”)

1 within the meaning of “content”: the House Report on the USA PATRIOT Act and the PATRIOT  
2 Act amendments state that email subject lines are “clearly content.”<sup>15</sup>

### 3 **C. Optiver is Entitled to Non-Content Metadata**

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

## 12 **IV. CONCLUSION**

13 The SCA offers broad protection against disclosure of content by service providers.  
14 Optiver’s Request One is invalid because it seeks disclosure of the terms “Optiver” and “PGP,” so  
15 Tibra’s motion to quash Request One is GRANTED. Request Two violates the SCA insofar as it  
16 seeks the subject of the communications, but the remainder is permissible. Accordingly, consistent  
17 with the remainder of the subpoena, Google is required to provide only the following information:  
18 “Documents sufficient to show the recipient(s), sender, date sent, date received, date read, and date  
19

20  
21 <sup>15</sup> H.R. Rep. No. 107-236, Part 1, at p. 53 (2001) (“Thus, for example, an order under the [SCA]  
22 could not authorize the collection of email subject lines, which are clearly content”).

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

26 <sup>16</sup> Docket No. 13 at 3.

27 <sup>17</sup> *See Beluga Shipping GMBH & Co. KS BELUGA FANTASTIC v. Suzlon Energy LTD.*, Case No.  
28 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).

1 deleted of emails, email attachments, or Google Talk messages sent or received between November  
2 3, 2005 to December 31, 2009 that were sent to or from” the email addresses listed.

3 **IT IS SO ORDERED.**

4 Dated: January 23, 2013

5 

6 \_\_\_\_\_  
7 PAUL S. GREWAL  
8 United States Magistrate Judge  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

United States District Court  
For the Northern District of California