White Paper

pillsbury

Global Sourcing

Privacy, Data Security & Information Use

Litigation

Cloud Computing

Information Law & Electronic Discovery

March 17, 2011

Taking Corporate Email to the Cloud: The Stored Communications Act and Control

by Wayne C. Matus, John L. Nicholson and Shawn P. Thomas*

While there is essentially no case law directly addressing discovery of corporate email held by Cloud providers, there are some instructive analogs found in cases involving third-party email providers under the Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA") and in cases addressing the concept of "control" under Fed. R. Civ. P. 34(a) that should be considered by large corporations thinking of migrating email to the Cloud.[1]

The Stored Communications Act

In general, courts have held that the SCA prohibits third-party email service providers from disclosing without authorization the contents of users' email accounts, even to comply with civil subpoenas. Those courts have focused on whether email account holders who are parties in the underlying litigation can be ordered to authorize access to their email accounts. The prevailing answer is that, the SCA notwithstanding, such users can be so compelled.

A particularly illuminating Illinois case is *Thayer v. Chiczewski*, No. 07 C 1290, 2009 WL 2957317 (N.D. Ill. Sept. 11, 2009). *Thayer* was a civil rights suit against the city of Chicago (the "City") in which the City served a subpoena on America Online ("AOL") seeking production of several of the plaintiff's emails. *Id.* at *1. The plaintiff and AOL objected to the subpoenas and the City moved to compel. *Id.* at **1-2. After excoriating both the plaintiff and (especially) AOL for the ineptitude and inconsistency of their submissions opposing the motion to compel, *Id.* at **4-5, the court granted the motion. *Id.* at *9.

*This paper was originally prepared for the Fifth Annual Sedona Conference® Institute program on Staying Ahead of the eDiscovery Curve, held March 17-18, 2011 in San Diego, CA. Reprinted with permission.

[1] The concept of "control" for the purpose of document discovery, including electronic discovery, comes from Fed. R. Civ. P. 34(a): “A party may serve on any other party a request ... to produce ... the following items in the responding party's possession, custody, or *control*: ... ” (emphasis added). *See Thayer*, 2009 WL 2957317, at *6.

The court first acknowledged that the SCA usually prevents enforcement of such civil subpoenas against third parties. *Id.* at *5. ("The Court agrees that, although decisions analyzing the SCA have defined its parameters in sometimes competing ways, most courts have concluded that third parties cannot be compelled to disclose electronic communications pursuant to a civil-as opposed to criminal-discovery subpoena."). The court went on to state that because the plaintiff would be required to produce relevant emails if he were in possession of them, and AOL would be obliged to produce the emails at the plaintiff's request, the emails were under the plaintiff's "control" for discovery purposes. *Id.* at *6. In the course of their attempt to fight enforcement of the subpoena, AOL noted that the plaintiff had authorized AOL to turn over at least one responsive email. *Id.* at *7. Since the plaintiff had authorized the production of at least one email and had put his mental state at the time of the relevant events at issue (which arguably would be shown by contemporaneous emails), the court assumed that the plaintiff had authorized disclosure of all of his relevant emails. *Id.*

A recent California case concerning the SCA and third-party email providers is *Chasten v. Franklin*, No. C10-80205 MISC JW (HRL), 2010 WL 4065606 (N.D. Cal. Oct. 14, 2010). While stating the rule more categorically than other courts, the District Court for the Northern District of California did not break new ground in deciding that the SCA prohibited an email service provider from turning over emails in response to a third-party civil subpoena. However, the court's failure to discuss whether the email account holder could be forced to consent to the emails' disclosure was unique among courts that have considered the question.

Chasten involved a defendant in a civil rights case serving on Yahoo a subpoena seeking the plaintiff's emails. *Id.* at *1. The plaintiff argued that the SCA prohibited Yahoo from disclosing his emails. *Id.* The court agreed and quashed the subpoena. *Id.* at *2. ("Because no exception applies, compliance with the [third-party] subpoena would be an invasion of the specific interests that the SCA seeks to protect.") (internal citations omitted). The court did not examine whether the plaintiff could or should be ordered to consent to Yahoo's producing the emails.

Another recent case in the Northern District of California echoed the Thayer court's reasoning. In *Beluga Shipping GMBH & Co. v. Suzlon Energy, Ltd.*, Misc. Case No. C 10-80034 JW (PVT), 2010 WL 3749279 (N.D. Cal. Sept. 23, 2010), one party to a foreign civil action sought to serve on Google a subpoena seeking access to another party's Gmail account. *Id.* at *1. Google intervened and argued that it could not comply with the subpoena unless it had permission from the account holder. *Id.* at *3. The court agreed with Google and denied the foreign party leave to serve the subpoena without proof of consent by the account holder to disclosure of the emails. *Id.* at **4-5. ("The ECPA [of which the SCA is a part] prohibits Google from disclosing the contents of those email accounts until it receives consents from the email account holders." *Id.* at *4). However, the court did order Google to "disclose documents that reflect ... (1) when the specific email accounts ... were created; (2) the actual names of the email account holders provided to Google during the account creation process; and (3) the countr[ies] from which the specific email accounts ... were created." *Id.* at *5.

There is another recent case from a federal district court in California in which the court agrees with *Chasten's* basic SCA analysis while incorporating the same concepts of control and consent as *Thayer* and *Beluga Shipping*. In *Jimena v. UBS AG Bank*, NO. CV-F-07-367 OWW/SKO, 2010 WL 3749232 (E.D. Cal. Sept. 23, 2010), a civil plaintiff served on Yahoo a third-party subpoena seeking various categories of information from two email addresses purportedly used by the defendant's ex-chief financial officer. *Id.* at **1-2. Yahoo informed the plaintiff that "it ... is precluded by the Stored Communications Act ... from disclosing the contents of electronic communications with certain exceptions, and that the primary disclosure for which disclosure is permitted is subscriber consent." *Id.* at *2. The plaintiff then moved to

compel the defendant to grant its consent for Yahoo to disclose the information. *Id.* Both the motion to compel consent and enforcement of the underlying subpoena were rendered moot by the defendant consenting to Yahoo disclosing the information and Yahoo filing a response stating that it did not have any documents responsive to the subpoena. *Id.* at *3. However, the court did state that "it is unlikely that [the defendant's] consent is effective for purposes of an exemption to disclosure under the SCA for the subscriber IDs that are at issues ... [I]t is not clear that [the defendant] has any authority to consent to disclosure ... ." *Id.* at *3 n.2. This was presumably because there was no indication that the email accounts were owned by the defendant corporation rather than its former CFO in his personal capacity. Albeit dicta, the court's comments on consent indicate that it would consider the SCA to be an impediment to disclosure absent valid consent by the appropriate account holder. Accordingly, *Jimena* should properly be understood as being in accord with *Chasten*, *Thayer*, and *Beluga Shipping*.

Another instructive case comes from the Supreme Court of Suffolk County in which one party sought disclosure of information from social networking sites. *Romano v. Steelcase, Inc.*, 907 N.Y.S. 650 (Sup. Ct. Suffolk Cty. 2010) was a personal injury action in which the defendant moved for an order directing the plaintiff to grant it access to the plaintiff's current and historical Myspace and Facebook accounts. *Id.* at 651. The court "reviewed the submissions ... as well as the applicable federal statutory law, specifically the Stored Communications Act." *Id.* at 651-2. The court ordered the plaintiff to grant whatever consent or authorization was necessary for the defendant to access her Myspace and Facebook accounts. *Id.* at 657. The court's decision rested on: 1) the fact that "the material sought by [the d]efendant ... [was] both material and necessary to the defense of [the] action," *Id.* at 654; 2) "preventing [the d]efendant from accessing [the plaintiff's] postings on Facebook and Myspace would be in direct contravention to the liberal disclosure policy in New York State," *Id.*; and 3) "when [the p]laintiff created her Facebook and Myspace accounts, she consented to the fact that her personal information would be shared with others. ... " *Id.* at 657. Thus, although *Romano* did not involve a third-party subpoena served on an email provider, the court did indicate that the account holder's consent was a key element of the analysis in New York when a party is seeking access to third-party electronic records.

In summary, courts tend to conclude that email providers are exempt from compliance with third-party civil subpoenas under the SCA. However, courts also make clear that consent by the account-holder must also be considered, and under some circumstances, ordered. Ultimately, the message for email providers is that when faced with a third-party civil subpoena, they are not obligated to turn over emails unless they have either voluntary or court-ordered consent from the subscriber who owns the account. For the corporation, the message is that electronic communications will not be shielded from discovery simply because they are created and stored via a third-party provider and, most likely, even if placed in the Cloud.

Determining 'Control' Over the Third-party Email Account

After concluding that the SCA does not act as a shield to protect email account-holders from discovery of email accounts hosted by third-parties, the next complicating set of issues concerns how related corporate entities will be treated in discovery disputes over third-party email accounts. The SCA's prohibition against unauthorized disclosure of emails by third-party email providers is circumscribed by a courts' ability to compel persons or entities in control of the email accounts to authorize disclosure. In the corporate context, that begs the question of precisely who or what is in control of the email accounts in question.

When dealing with individuals' email accounts, the question of control is relatively easy: if a user opened the account, that user has control over the data and can be compelled to authorize disclosure. *See Thayer, supra*. Where a corporation uses a third-party email provider, the question of control is more complicated. For example, can a subsidiary be said to "control" its parent's third-party email accounts? Can a parent be

said to "control" a subsidiary's third-party email accounts? Research has not uncovered any cases in any jurisdictions in which the issue of control is analyzed in relation to Cloud email accounts.[2] However, cases from various jurisdictions in which courts have analyzed under what circumstances related corporate entities "control" documents for discovery purposes provide some guidance into how a court would analyze the question.

As the United States District Court for the District of Maryland noted in a recent decision, the definitions of "control" used by various courts around the United States in the context of discovery are not entirely consistent. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 523-24 (D. Md. 2010). However, the relevant concept that dominates the analysis throughout the country is that documents are under a party's control when the party "has the right, authority, or practical ability to obtain the documents from a non-party to the action." *Id.* at 523 (internal citations omitted). The key to "control" is a party's "practical ability" to obtain documents. The test "is not limited to whether the corporation has a legal right to those documents." *Zenith Elec. v. Vizio, Inc.*, Misc. No. M8-85, 2009 WL 3094889, at *2 (S.D.N.Y. Sept. 25, 2009). Therefore, "[t]he determination of whether an entity has 'control' over documents under Fed. R. Civ. P. 34(a) is a very fact specific inquiry." *Maniscalco v. Brother Int'l. Corp.*, Civil Action Nos. 3:06-CV04907, 3:07-CV-01905 (FLW), 2010 WL 762194, at *5 (D.N.J. March 5, 2010) (internal citations omitted). In other words, the definition of "control" for document discovery purposes is a functional one rather than a categorical one. It is a question of whether an entity has actual, non-theoretical access to relevant documents in the physical possession of its parent or subsidiary.

With that basic framework established, the question a court is likely to ask when confronted with a request for disclosure of the contents of a corporate Cloud email account is what entities have the practical ability to authorize disclosure of the emails? Furthermore, do any other entities within the corporate family have the practical ability to request that such authorization be given? A review of several cases in which the issue of control has been examined illuminates the way courts may evaluate these questions.

Cases Considering 'Control' Over Documents

U.S. Int'l Trade Comm'n v. ASAT, Inc., 411 F.3d 245 (D.C. Cir. 2005), was an appeal by a U.S. subsidiary of a Hong Kong based corporation of an order enforcing the U.S. International Trade Commission's ("ITC") subpoena seeking documents in the possession of the Hong Kong corporate parent. *Id.* at 246-47. Initially the administrative law judge ("ALJ") hearing the subsidiary's challenge to the subpoena summarily ordered the parent's documents produced. *Id.* at 247. The District Court affirmed the ALJ's decision and the subsidiary appealed to the D.C. Circuit Court. The Circuit Court reversed, holding that there had been inadequate findings of fact to support the conclusion that the subsidiary had control of its foreign parent's documents. *Id.* at 255. In reaching that conclusion, the court stated that "[c]ontrol is defined as the legal right, authority, or ability to obtain documents upon demand." *Id.* at 254. This definition is in keeping with the prevailing concept of control as more of a factual, practical inquiry than simple possession or corporate structure. The court highlighted the intensely fact-specific nature of the control inquiry by reversing, not because the lower court had gotten the analysis wrong but because it had failed to adduce enough facts to properly analyze at all.

[2] While the plaintiff in *Jimena* sought to have the court compel the corporate defendant to authorize Yahoo to disclose the contents of various email accounts, the court never reached the question of whether the defendant actually had control over the accounts. *Jimena*, 2010 WL 3749232, at *3. However, the court did indicate that it was "unlikely" that the corporate defendant had the authority to authorize Yahoo to disclose the contents of the accounts. *Id.* at *3 n.2. Similarly, while the main defendant in Beluga was a corporate entity, the email accounts at issue were the personal accounts of individual cross-defendants. *Beluga*, 2010 WL 3749279, at *2.

In *Maniscalco*, 2010 WL 762194, a magistrate judge overseeing discovery in a class action suit related to allegedly malfunctioning printers ordered the U.S. subsidiary of a Japanese printer manufacturer to produce technical documents in the possession of the Japanese parent. *Id.* at *1. The U.S. subsidiary sought to have the magistrate's order reversed by the district court. Id. The district court first noted that "Federal Courts construe 'control' very broadly under Rule 34." *Id.* at *4. The court went on to list five grounds on which courts have found control by a subsidiary: "(1) the alter ago doctrine which warranted 'piercing the corporate veil'; (2) the subsidiary was an agent of the parent in the transaction giving rise to the lawsuit; (3) the relationship is such that the agent-subsidiary can secure documents of the principal-parent to meet its own business needs and documents helpful for use in litigation; (4) there is access to documents when the need arises in the ordinary course of business; and (5) subsidiary was marketer and servicer of parent's product (aircraft) in the United States." *Id.* at *5. The court noted also that the burden of proving control is on the party seeking production of the documents. Id. The court stated that the magistrate judge had misapplied the law by shifting the burden to the subsidiary to prove that it did not control the documents in question, and reversed the magistrate's finding that the subsidiary did control the documents. *Id.* at *11, 12. Maniscalco is yet another example of a court reversing a finding of control on the basis that "the factual findings and record [were] insufficient to support a determination as a matter of law" that the subsidiary controlled its parent's documents. *Id.* at *12.

Zenith, 2009 WL 3094889, involved a plaintiff in a Texas patent infringement suit serving a subpoena in New York on a U.S. subsidiary of a Korean corporation. *Id.* at *1. The U.S. subsidiary claimed that the Korean parent "maintain[ed] separate records and archives—both hard-copy and electronic—to which [the subsidiary] does not have access in the ordinary course of business." *Id.* Echoing the opinions described above, the court stated that the test for control was whether the subsidiary had access to or the ability to gain access to the documents rather than whether it had a legal right to them. *Id.* at *2. The court also noted that the burden of proving control was on the party seeking to compel production. *Id.* Here, the party seeking production of the documents offered as evidence of control the parent-subsidiary relationship, the fact that the subsidiary was aware that the parent's products would be used in the U.S., and the fact that the subsidiary communicated an offer from the parent to provide documents if some claims were withdrawn. *Id.* Finding that the evidence the plaintiff put forward was insufficient to prove control, the court denied the plaintiff's motion to compel. *Id.* at *2-3.

In re Ski Train Fire of Nov. 11, 2000 Kaprun Austria, No. MDL 1428 (SAS)THK, 2006 WL 1328259, (S.D.N.Y. May 16, 2006) involved plaintiffs attempting to compel production of a subsidiary's documents by claiming that they were in control of its U.S. parent. *Id.* at *1. The Austrian subsidiary had already been dismissed from the case for lack of personal jurisdiction. *Id.* The court recited a familiar definition for control: "the legal right, authority, or practical ability to obtain the materials sought upon demand." *Id.* at *5. The court also noted that "many courts have concluded that the parent of a wholly-owned subsidiary is required to produce documents which its subsidiary possesses." *Id.* The court noted that some considerations weighed in favor of a finding of control by the parent (the parent's complete ownership of the subsidiary and the fact that the two entities regularly exchanged documents). *Id.* at *6. On the other hand some considerations weighed in favor of finding no control by the parent (the fact that the two companies did not act as a single entity and the fact that the companies' transactions were at arms-length). *Id.* at *6-7. However, the court ultimately found that the balance tipped in favor of a finding of control based on the parent's total domination of the subsidiary's board of directors. *Id.* at *7. The court reasoned that if the parent needed assistance from the subsidiary in the form of helpful documents, it would not have difficulty obtaining it. *Id.* at *8. Therefore, the parent could not shield those same documents behind a formalistic control analysis. *Id. Ski Train* thus demonstrates that regardless of whether the parent's documents are sought through the subsidiary or vice-versa, the inquiry is a factual one based on what documents parties actually can access in practice.

Applying 'Control' to the Cloud Email Account

Ultimately, the parent-subsidiary control question simply adds another layer of analysis to the question of when emails held by a third-party email service provider will be discoverable. As discussed above, under the SCA an email service provider is not obliged to produce emails unless authorized to do so by the account-holder. However, a court can compel the account-holder to grant such authorization. No courts have yet considered whether a subpoena can reach a third-party email account owned by a parent on the theory that its subsidiary, who is a party to the underlying litigation, "controls" the documents (or, conversely, whether a subpoena can reach an email account owned by a subsidiary because of the parent's "control"). Courts that have considered parent/subsidiary control issues have made clear that the analysis must be a practical, functional one rather than a simple review of the entities' titles or positions on an organizational chart. That type of analysis may carry over into the Cloud email account context. On the other hand, a court could interpret the SCA as strictly requiring the actual account owner ("user of that service" §2701 (c) (2)), and not apply the parent-subsidiary concept of control.

Conclusion

Recent decisions such as *Chasten* may have made third-party email providers appear to be an attractive option for restricting the discovery available against a foreign corporation. However, the apparent protection by the SCA of emails from discovery that *Chasten* describes is a mirage. Courts can still compel parties to authorize disclosure of relevant emails.

In the context of corporate email, there is a possibility of significant litigation over the application of the concept of control under the SCA and, if it applies, which corporate affiliates have the power to execute such authorizations. Against any potential benefits that may flow from moving to a Cloud email provider, any corporation considering such a move should weigh the drawbacks and complications described above and explore if there are creative solutions to this conundrum.

If you have any questions regarding this white paper, please contact the Pillsbury attorney with whom you regularly work or the authors:

Wayne C. Matus (bio)
New York
+1.212.858.1774
wayne.matus@pillsburylaw.com

John L. Nicholson (bio)
Washington DC
+1.202.663.8269
john.nicholson@pillsburylaw.com

Shawn P. Thomas
New York
+1. 212.858.1414
shawn.thomas@pillsburylaw.com