

---

# CONSENT AND DISCOVERY UNDER THE STORED COMMUNICATIONS ACT

BY TIMOTHY G. ACKERMANN

---



Several recent decisions remind litigators that, even in the rush to “e-discovery,” it is worth recalling the black-letter law governing discovery. One such principle is that the responsive documents may include those that are merely under the “control” of the target of discovery and are not limited to those in the party’s possession or custody.

E-discovery commonly includes e-mail and attached documents, voice mail messages, and other documents stored in electronic form that are communications or contain them. If you need those communications, consider seeking discovery from whoever controls, rather than possesses, the electronic files. Why should you look to control, rather than actual possession? In short, you may need to get consent from the controlling party before the party in possession of the files can produce the documents. So why won’t discovery requests to the latter suffice?

The Stored Communications Act (SCA), 18 U.S.C. §§ 2701–12,<sup>1</sup> “creates a zone of privacy to protect [I]nternet subscribers from having their personal information wrongfully used and publicly disclosed” while balancing that interest with the needs of the government and law enforcement agencies. *In re Subpoena Duces Tecum to AOL LLC*, 550 F. Supp. 2d 606, 610 (E.D. Va. 2008) (citing legislative history). The SCA applies in civil litigation, including in state courts. *See O’Grady v. Superior Court*, 44 Cal. Rptr. 3d 72, 83–84, 89 (Cal. Ct. App. 2006) (SCA rendered California state court subpoenas unenforceable). The SCA also prohibits certain parties (and nonparties) in civil litigation<sup>2</sup> from disclosing certain aspects of the electronic communications that they may possess.

## The Stored Communications Act

Section 2702(a) of the SCA specifically prohibits persons from disclosing the contents of communications in either of two cases, unless an exception applies. The first case involves persons providing an electronic communication service (ECS)—a service that enables one to send or receive wire or electronic communications—to the public. 18 U.S.C. § 2510(15) and § 2711 (adopting definitions in § 2510). Generally, wire communications include a human voice transmitted (at least in part) by a wire or cable or the like; whereas electronic communications do not contain the human voice and include e-mail and text messages. *See* 18 U.S.C. §§ 2510(1), (12), (18).

An ECS provider may not knowingly divulge the contents of any communication while it holds the communication in electronic storage. 18 U.S.C. § 2702(a)(1). The legislative history explains that “knowingly” merely refers to awareness of the conduct and awareness of or a firm belief in the existence of the requisite circumstances and the substantial certainty of the result. *Freedman v. America Online Inc.*, 329 F. Supp. 2d 745, 748–49 (E.D. Va. 2004) (citing H.R. Rep. No. 99-647, at 64 (1986)). The statute defines “content” as information “concerning the substance, purport, or meaning” of a communication. 18 U.S.C. § 2510(8), but the definition does not include the existence of the communication or identities of the parties to it. S. Rep. No. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567 (deleting existence and identity from the definition). The definition of “electronic storage” is limited to communications either in “temporary, intermediate storage” for transmitting a message or in storage by an ECS as “backup

protection.” 18 U.S.C. § 2510(17).

Many online communications fall into this category. Leading cases hold that e-mail already opened by the user, but still stored by the e-mail provider, is in electronic storage. See *O’Grady*, 44 Cal. Rptr. 3d at 84 n.9 (but noting a split). Those courts consider copies of opened e-mails to be retained for “backup protection” and thus in “electronic storage.”<sup>3</sup> See *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075–77 (9th Cir. 2004). The opposing view is that these e-mails are not stored for “backup protection” and are not in “electronic storage.” *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff’d on other grounds*, 352 F.3d 107, 114 (3rd Cir. 2003) (questioning the district court’s reasoning but not deciding the issue); *cf. In re DoubleClick Inc. Privacy Litig.* 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001). Thus, e-mail services (such as those an Internet service provider offers), text-messaging services, and services that host an electronic bulletin board holding unopened e-mail have all been found (or agreed) to be an ECS.<sup>4</sup> The statute’s legislative history explicitly envisions that telephone companies act as ECS providers, including for voice mail. *State Wide Photocopy Corp. v. Tokai Financial Services Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995); see *U.S. v. Steiger*, 318 F.3d 1039, 1048 (11th Cir. 2003) (citing *Konop v. Hawaiian Airlines Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (voice mail to be protected as a stored communication)); see *U.S. v. Councilman*, 418 F.3d 67, 78–79 (1st Cir. 2005) (en banc) (noting that the 2001 amendment plainly placed voice mail under the SCA).

Some companies, however, are perhaps better described as ECS consumers, rather than providers. For instance, a company that merely maintains a Web site allowing for the transmission of electronic communications between itself and its customers was not considered an ECS provider. *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 307 (E.D.N.Y. 2005); see *Kaufman v. Nest Seekers LLC*, 2006 U.S. Dist. LEXIS 71104, \*14–\*15 (S.D.N.Y. Sept. 26, 2006). One of the earliest courts to consider the issue concluded that merely buying access to, but not independently providing, Internet services is not sufficient, and that providing e-mail access to a contractor is not the same as providing these services to “the public.” *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998). Another court explained that a key question is whether access to the Internet is provided. *In re Broadcast.Com Inc. Privacy Litig.*, 2001 U.S. Dist. LEXIS 26212, at \*6–\*8 (E.D. Tex. Dec. 11, 2001).

The second case involves persons providing a remote computing service (RCS)—computer storage or processing service that uses an electronic communications system—to the public. 18 U.S.C. § 2711(2). Under the statute, the term “electronic communications system” is broad and includes both electronic devices used for transmission and computers and electronics used for storage. 18 U.S.C. § 2510(14). An RCS provider may not knowingly divulge the contents of a communication that meets each of two tests. (1) Is the communication held by the RCS for a subscriber or customer and was it received electronically from that subscriber (or created from an electronic communication from that subscriber)? (2) If the RCS provider has authorized access only for storage

or processing, is the communication held solely for providing those services to the subscriber or customer? 18 U.S.C. § 2702(a)(2). Certain online services fall into this category, such as an archive of a text-messaging service (when messaging services are no longer being provided), and the YouTube.com video-sharing service. *Flagg v. City of Detroit*, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (text-message archive); *Viacom International Inc. v. YouTube Inc.*, 253 F.R.D. 256, 265 (S.D.N.Y. 2008). The legislative history also identifies electronic files stored in off-site data banks or sent to remote computers for “sophisticated data processing services.” See S. Rep. No. 99-541, at 3 and 10–11 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557, and 3564–65.

It bears repeating that the Stored Communications Act’s particular prohibitions on disclosure to nongovernmental entities apply only to the contents of stored communications. 18 U.S.C. § 2702(a). The SCA, moreover, expressly permits an ECS or RCS provider to divulge customer records (to nongovernmental entities) if the files do not include such content. 18 U.S.C. § 2702(c)(6).

The SCA also includes exceptions that permit an ECS or RCS provider to divulge the contents of communications that it stores. Most of the exceptions, provided in 18 U.S.C. § 2702(b), are less relevant for civil litigation. In general, the statute allows the provider to carry out the intended communications or remote computing services (subsections (1), (4), and (5)) or are included for governmental or law enforcement purposes (subsections (2) and (6)–(8)). It is important to note that § 2702 of the SCA does not provide a general exception for complying with civil discovery. For instance, one court recently refused to find an implicit exception for civil discovery, rejecting the argument that § 2702(b)(5), which permits the provider to protect its own rights and property, would permit disclosure whenever the provider was faced with the cost of a subpoena or the threat thereof. *O’Grady*, 44 Cal. Rptr. 3d at 84–85, 86–87, and 89.

Section 2702(b)(3) of the SCA does, however, create an exception based on lawful consent that applies to civil discovery. The SCA authorizes an ECS or RCS provider to divulge the contents of communications when “lawful consent” has been given to do so. Who may give consent depends on whether the service is an ECS or RCS. In both instances, the originator, addressee, and intended recipient of a communication may each give consent; the subscriber to the RCS holding the communication—that is, the account holder—may also give consent. 18 U.S.C. § 2702(b)(3).<sup>5</sup> As an example, the sender (originator) of an e-mail as well as any intended recipients may give consent to disclose the communication. It should be noted that the issue is one of the legal capacity to give consent, not whether doing so might breach some other obligation, such as a contract. See *In re American Airlines Inc., Privacy Litig.*, 370 F. Supp. 2d 552, 560–61 (N.D. Tex. 2005).

The SCA does create a civil cause of action for “knowing or intentional” violations of the law. 18 U.S.C. § 2707(a).<sup>6</sup> Disclosure of a communication’s contents, however, will not necessarily result in liability. For instance, “good faith reliance” on a court order—even if the order is ultimately

found not to be valid—is a “complete defense” to liability.<sup>7</sup> 18 U.S.C. § 2707(e)(1); *cf. Freedman v. America Online Inc.*, 325 F. Supp. 2d 638, 649–50 (E.D. Va. 2004) (good faith reliance standard relate to a warrant), superseded in part on other basis by *Freedman v. America Online Inc.*, 329 F. Supp. 2d 745, 749–40 (E.D. Va. 2004). But the mere possibility that granting such an order might create a defense to liability does not prospectively authorize disclosure of the communication or permit compulsory disclosure that would violate the SCA. *See O’Grady*, 44 Cal. Rptr. 3d at 85. Thus, such a defense will typically only arise if the holder of the documents discloses them despite the provisions of the Stored Communications Act.

### Subpoenas to Internet Service Providers

What happens if someone relies on the SCA and refuses to produce the electronically stored documents, and the party seeking discovery has not obtained the consent necessary to allow production of the documents? Several recent district court cases involving third-party Internet service providers (ISPs)—ECS providers such as Microsoft, Google, Yahoo!, or AOL—illustrate what can result in such a situation.

In April 2008, in *In re Subpoena Duces Tecum to AOL LLC*, 550 F. Supp. 2d 606 (E.D. Va. 2008), a U.S. district judge affirmed the magistrate judge’s order quashing a subpoena to an ISP. State Farm Insurance Company had sought communications by two individuals (the Rigsbys), who were witnesses in another case. State Farm issued a subpoena to AOL, because the Rigsbys allegedly e-mailed State Farm’s confidential information to their own AOL accounts and then forwarded the file. The Rigsbys objected to the disclosure, and State Farm evidently lacked consent from anyone else. The magistrate judge granted the Rigsbys’ motion to quash the subpoena, ruling that the SCA prohibited AOL from producing the e-mails under the subpoena. The district court agreed, ruling that the “clear and unambiguous language of § 2702” prohibited AOL from divulging those e-mails because receiving a Rule 45 subpoena is not among the exceptions to the SCA. *Id.* at 608–12 and n.2 (discussing *Theofel*, 359 F.3d at 1071–74; *FTC v. Netscape Comms. Corp.*, 196 F.R.D. 559, 559–61 (N.D. Cal. 2000); and *O’Grady*, 44 Cal. Rptr. 3d at 86–89).

In July 2008, a U.S. magistrate judge quashed a subpoena directed to an ISP in an employment discrimination case, *Hone v. Presidente U.S.A. Inc.*, No. 5:08-mc-80071-JF, 2008 U.S. Dist. LEXIS 55722 (N.D. Cal. July 21, 2008) (labeled as “Not for citation”). The defendants sought e-mails from the plaintiff’s personal Yahoo! account, to which the plaintiff objected. The court quashed the subpoena because, absent the consent necessary to permit Yahoo! to divulge the communications, compliance would require an “impermissible disclosure of information.” *Id.* at \*1–\*2, \*4.

In August 2008, a U.S. magistrate judge quashed subpoenas issued to three ISPs in *J.T. Shannon Lumber Co. v. Gilco Lumber Inc.*, No. 2:07-cv-119, 2008 WL 3833216 (N.D. Miss. Aug. 14, 2008), *reconsideration denied*, 2008 WL 4755370, at \*1 (N.D. Miss. Oct. 29, 2008). The plaintiff sought all e-mails in the three individual defendants’ personal Microsoft, Yahoo!, and Google accounts. The court

found the “statutory language [] clear and unambiguous” and ruled that a Rule 45 subpoena does not constitute an exception to the SCA allowing an ECS provider to divulge the contents of communications. *Id.* at \*1–\*2.

The focus here on “communications” should not obscure the availability under the SCA of information that does not concern “the substance, purport, or meaning” of a communication (at least to nongovernmental litigants). *See supra* re: 18 U.S.C. §§ 2702(c)(6) and (a)(3). Even though the content may be important, it may not be the only valuable information pertaining to an electronic communication. For instance, in *Viacom International*, 253 F.R.D. at 264–65, the plaintiffs successfully forced YouTube to produce information such as the number of times that certain “private” videos had been viewed or made accessible, even though YouTube was able to protect the videos themselves—that is, their content—from production.

### Flagg v. City of Detroit and Rule 34 “Control”

Another recent decision made by a district court points to a more effective way, in most instances, to obtain electronically stored communications and their contents. Direct the discovery to a sender, recipient, addressee, or subscriber who also exercises control over the communications. This approach harks back to black-letter law: documents under one’s “control”—in addition to those in one’s possession or custody—are subject to discovery. FED. R. CIV. P. 34(a)(1) (“in the responding party’s possession, custody, or control”); *see* FED. R. CIV. P. 45(a)(1)(A)(iii). In these circumstances, “control” typically means control over the stored communications by their originator, addressee, and/or intended recipients.

The discovery fight in *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008), began with typical subpoenas for documents issued to Skytel under Rule 45 of the Federal Rules of Civil Procedure. SkyTel had previously provided text-messaging services to the city and to city officials and still retained a copy of at least some text messages. The city, two of the individual defendants, and SkyTel all argued that the SCA prohibited SkyTel, a third party, from producing any text messages under the subpoenas. But rather than taking on this question directly, the district court found it “best to avoid” the question of document production sought directly from a third party by a subpoena. *Id.* at 347–48, 366 and n.2.

In *Flagg*, the court analyzed the entire dispute as though the plaintiff had sought the SkyTel text messages by a Rule 34 request that the city produce the files. The court concluded that was the “more straightforward path” and ordered the plaintiff to do just that. *Id.* at 366; *see id.* at 358. Focusing on Rule 34, the district court analyzed the dispute largely in terms of the consent needed under the SCA to allow SkyTel to divulge the content of the text messages created by the city’s personnel.<sup>8</sup> There were two inquiries: who could give consent and who retained control over the documents.

To answer the first question, the district court analyzed SkyTel’s services to decide whether it was providing an RCS or an ECS. After discussing in detail two influential Ninth Circuit cases on the question of whether a party was

an RCS or ECS provider, the *Flagg* court ruled that a provider could provide both an ECS and an RCS. Thus, the question of RCS or ECS provider was not decided merely because SkyTel had been an ECS provider when providing text-messaging services. *Id.* at 359–63.<sup>9</sup>

The *Flagg* court concluded that, at the time of the proceeding, SkyTel provided only an RCS. SkyTel's archive of the city's text messages was the only existing copy of the files. The court explained that the archive was not kept for purposes of "backup protection" and thus could not meet the "electronic storage" requirement of § 2702(a)(1) of the Stored Communications Act. *Flagg* at 363. Therefore, in addition to the originator, addressee, and/or intended recipients of the messages, the city—as the subscriber—could give its consent to divulging the communications; but the city objected to doing so, leading to the question of control.<sup>10</sup>

The *Flagg* court analyzed the second question, concluding that the city had control over the archived text messages held by SkyTel. In reaching that conclusion, the court discussed Rule 34 "control" over documents. The court noted that control includes the "legal right to obtain the documents on demand" and also a party's "affirmative duty to seek that information reasonably available to him from his employees, agents, or others subject to his control." *Id.* at 353 (quoting *In re Bankers Trust Co.*, 61 F.3d 465, 469 (6th Cir. 1995) and *Gray v. Faulkner*, 148 F.R.D. 220, 223 (N.D. Ind. 1992) (internal quotations omitted)). The court also cited examples of what might constitute control, including a contractual right to access and documents held by a party's agent. *Id.* (citing, for example, *Anderson v. Cryovac Inc.*, 862 F.2d 910, 928–29 (1st Cir. 1988) and *In re Ruppert*, 309 F.2d 97, 98 (6th Cir. 1962)).

Turning to the text messages in the SkyTel archive, the court concluded that the city had a contractual right to retrieve them, because they were evidently preserved based on SkyTel's contractual relationship with the city. The city, however, expressly asserted that it could withhold its consent, thus preventing disclosure of the messages. Not surprisingly, the court seized upon the city's claim to conclude that the city could also give consent. Relying on that ability, the court ruled that the city had the legal right to obtain those messages from SkyTel and thus exercised control over them for purposes of Rule 34. *Id.* at 354–55, 357.

The court took merely a "short step" from finding control to concluding that the city must give consent to disclosure to permit production of the documents. Rule 34's obligation to produce documents within a party's control, the court noted, overcomes a party's disinclination to exercise its control over documents. That party's "consent" to disclosure of the document is compulsory. *Id.* at 363.<sup>11</sup>

The city's "consent" removed the last obstacle to SkyTel's disclosure of the contents of the communications (at least based on the *Flagg* court's artificial analysis of the dispute as though the request had been made directly to the city). Accordingly, the court ruled that the city "*must give any consent that might be required* under the SCA in order to permit SkyTel to retrieve communications from this archive and forward them" for production. *Id.* (emphasis added).

## Discovery and Consent

Few lawyers will be surprised that a court might order a person to produce documents. But can a court order a person to give consent so that someone else can disclose communications in their possession? In a word, yes. The *Flagg* court so ruled, and the *O'Grady* court explicitly suggested as much, and both courts did so in the context of the Stored Communications Act. *O'Grady*, 44 Cal. Rptr. 3d at 88. Analogous cases, moreover, demonstrate the broad application of this principle.

In 2003, a district court found that the defendant had control over a document because he had the right to execute a form permitting its release, and the court ordered him to do so. In *Preservation Products LLC v. Nutraceutical Clinical Labs. Int'l Inc.*, 214 F.R.D. 494, 494–95 (N.D. Ill. 2003), Preservation Products sought a copy of the defendant's statement to the Securities and Exchange Commission as well as related documents, which the SEC refused to disclose without his consent. The court granted a motion to compel the defendant's consent, even without a subpoena, and concluded that his obligations under Rule 34 as well as his practical ability to control the document compelled him to produce the documents himself or to cooperate in doing so.

What if the controlling entity is not a "party," that is, is not subject to Rule 34 discovery? Even in this case, one may seek discovery from the entity controlling the documents. For instance, in 2004, a district court concluded that two subpoenaed third parties had control over documents held by their banks (also third parties) and ordered the parties to produce the documents. In *Thomas v. Deloitte Consulting LP*, No. 3:02-cv-0343-M, 2004 WL 1372954, at \*4 (N.D. Tex. June 14, 2004), the court noted that the third parties might not have affirmatively asked their banks for checks and statements sought by the subpoena. Relying on cases under Rule 34, the court concluded that the meaning of "control" in Rule 45 means that the subpoena encompasses any documents that the third parties can obtain, including the bank documents, and ordered the third parties to give the defendant their consent to obtain the documents directly if the parties did not obtain and produce them for the defendant.<sup>12</sup>

Just because a court can order consent, however, does not mean that it will do so. On reconsideration in *J.T. Shannon Lumber Co.*, No. 2:07-cv-119, 2008 WL 4755370, at \*1 (N.D. Miss. Oct. 29, 2008), after the magistrate judge quashed subpoenas issued to the three ISPs, the plaintiff sought to compel the defendant and its employees to give their consent. The court refused to allow an "end run around the statute," noting that the Stored Communications Act lacks an exception for complying with civil subpoenas and also pointing to the effect that the requested relief would have on the "zone of privacy" the SCA was meant to create around electronic communications.

The *Flagg* court's approach also points out another circumstance in which control affects production of documents subject to the SCA: when the entity exercising control over the documents is related to the target of discovery. In ruling for the party seeking discovery, the *Flagg* court

hedged its bets. The court also analyzed the matter based on an alternative conclusion: that SkyTel was providing an ECS (rather than the actual conclusion—that it was providing an RCS). In that case, the city could not itself give consent; it was not an originator, addressee, or intended recipient. *Cf.* 18 U.S.C. § 2702(b)(3). At least some of the individuals fitting those descriptions were employees or officers of the city, however, and this fact established a relationship between the city and the individuals. The court concluded that the relationship obliged—and enabled—the city to get city employees' consent to disclose the information. *Flagg*, 252 F.R.D. at 363, 354. In reaching that conclusion, the *Flagg* court discussed Rule 34 control in cases that presented situations where a party had indirect control over documents.

In another case, *Herbst v. Able*, 63 F.R.D. 135, 138 (S.D.N.Y. 1972), the court ruled that the plaintiffs could request the corporate defendant, Douglas Aircraft, to ask its employees to request a copy of their own testimony from the Securities and Exchange Commission so that Douglas could produce the information for the plaintiffs. Here, the court reasoned that Douglas retained control over its employees (who themselves retained control over the documents) and that their testimony related to the company's business.<sup>13</sup> In still another case, *Riddell Sports Inc. v. Brooks*, 158 F.R.D. 555, 559 (S.D.N.Y. 1994), the court ruled that Riddell retained control of the documents because they were created in connection with a corporate officer's functions as an employee and that officer had possession of the files. The court reasoned that the records belonged to the company and that the officer had a duty to turn them over on demand. Thus, as these cases show, even indirect control may suffice, if the documents are controlled by, or are possessed by, a person found to be controlled by the target of discovery.

In conclusion, if seeking electronic documents that may fall under the Stored Communications Act, parties need to analyze who can give consent to their disclosure. If that person does not possess them, does the person exercise control? If not, parties should consider who else has both the ability to consent and even indirect control over the documents. If that person resists discovery, parties should point out the fact of control and demand that the person either give consent to disclosure by the other entity or collect the documents for the requesting party.

What once was old is new again. Despite the changes wrought by e-discovery, one can benefit by looking back to first principles. **TFL**

*Tim Ackermann is an associate in the Dallas office of Patterson & Sheridan LLP. He practices primarily patent and trademark litigation in the federal courts, and also works on appeals to the Court of Appeals for the Federal Circuit. Ackermann is a member of the Dallas chapter of the FBA.*



## Endnotes

<sup>1</sup>Chapter 121 of Title 18, U.S. Code (Stored Wire and Electronic Communications and Transactional Records Access) was enacted in 1986 as Title II, § 201 of the Electronic Communications Privacy Act of 1986 (Pub. Law No. 99-508, 100 Stat. 1860, 1860–68 (1986)).

<sup>2</sup>The SCA permits government entities (including law enforcement) greater access to stored electronic communications but imposes additional limitations and requirements on such access. *See, e.g.*, 18 U.S.C. §§ 2702(a)(3); 2703–05. However, examining the application of the SCA to government entities is beyond the scope of this article.

<sup>3</sup>In addition, a record of communication (such as an e-mail or a text message) that no longer exists elsewhere may be in “electronic storage.” *See Theofel v. Farey-Jones*, 359 F.3d at 1076–77 (9th Cir. 2004); *Flagg v. City of Detroit*, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (discussed in the text).

<sup>4</sup>*Theofel*, 359 F.3d at 1075 (e-mail); *In re Subpoena Duces Tecum to AOL*, 550 F. Supp. 2d at 611 (E.D. Va. 2008) (e-mail); *FTC v. Netscape Comms. Corp.*, 196 F.R.D. 559, 560 (N.D. Cal. 2000) (e-mail); *J.T. Shannon Lumber Co. v. Gilco Lumber Inc.*, No. 2:07-cv-119, 2008 WL 3833216, at \*1 (N.D. Miss. Aug 14, 2008) (e-mail), reconsideration denied, 2008 WL 4755370, at \*1 (N.D. Miss. Oct. 29, 2008); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 902–03 (9th Cir. 2008) (text messages); *petitions for cert. filed*, 77 U.S.L.W. 3619 (Apr. 27, 2009) (No. 08-1332), 77 U.S.L.W. 3760 (May 29, 2009) (No. 08-1472); *Steve Jackson Games Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 461–62 (5th Cir. 1994) (unopened messages stored on a BBS pending delivery, and thus in “temporary, intermediate storage”); *see Kaufman v. Nest Seekers LLC*, 2006 U.S. Dist. LEXIS 71104, \*15–\*20 (S.D.N.Y. Sept. 26, 2006) (private site that offered the public Web-based access to post listings and use internal e-mail could be a BBS). *Cf. U.S. v. Steiger*, 318 F.3d 1039, 1049–50 (11th Cir. 2003) (interpreting the relationship between the Wiretap Act and the SCA and concluding that most electronic communications on computers will be stored communications (and thus outside the purview of the Wiretap Act); adopting the reasoning of the ruling in *Steve Jackson Games*, 36 F.3d at 462–64 and *Konop v. Hawaiian Airlines Inc.*, 302 F.3d 868, 879–80 (9th Cir. 2002)); *but see U.S. v. Councilman*, 418 F.3d 67, 79–80 (1st Cir. 2005) (en banc) (rejecting the argument that an electronic communication copied while in transient storage was not “intercepted” on the grounds that the file was not acquired “contemporaneous with transmission” and rejecting the reasoning in *Steiger*, *Steve Jackson Games*, and *Konop*, *supra*).

<sup>5</sup>An RCS subscriber's ability to separately give consent may be dispositive. *See Quon*, 529 F.3d at 903.

<sup>6</sup>Any action against the United States is governed by 18 U.S.C. § 2712.

<sup>7</sup>The SCA also expressly denies a cause of action for acts “in accordance with the terms of a court order, ... [or] subpoena, ... under [Chapter 121, the SCA].” § 18 U.S.C. § 2703(e). Compliance with just any subpoena or order, however, may not suffice. Despite the general reference to a “subpoena”—as distinguished from the trial, grand jury, or administrative subpoenas used by the government (*cf.* §§ 2703(b)(1)(B)(i) &

(c)(2)—and “court order,” the legislative history expressly states that any “warrant or other court order [must be] issued under this chapter,” *i.e.* the SCA. *See* S. Rep. No. 99-541, at 39 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3593. This strongly suggests that the subpoena must be issued under the SCA, as the text of § 2703(e) treats warrants, subpoenas, and court orders identically. Notably, the SCA does not provide for ordinary civil discovery subpoenas nor for any subpoena by a nongovernmental party. *See* 18 U.S.C. § 2703; *FTC v. Netscape Comms.*, 196 F.R.D. at 560–61; *In re Subpoena Duces Tecum to AOL*, 550 F. Supp. 2d at 611. Moreover, that section appears to protect only ECS providers and their officers, employees, and agents, but not RCS providers. 18 U.S.C. § 2703(e) (“provider of wire or electronic communication service”); *cf.* 18 U.S.C. §§ 2510(15) and 2711(2) (defining ECS and RCS, respectively).

<sup>8</sup>The court also discussed whether other parts of § 2702 would permit disclosure to the city even in the absence of consent. *Flagg v. City of Detroit*, 252 F.R.D. 358–59 (E.D. Mich. 2008).

<sup>9</sup>The court cited *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004) and *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), *petitions for cert. filed*, 77 U.S.L.W. 3619 (Apr. 27, 2009) (No. 08-1332), 77 U.S.L.W. 3760, (May 29, 2009) (No. 08-1472). It disagreed, however,

with the Ninth Circuit in the latter and instead agreed with the lower court.

<sup>10</sup>*Cf. Thayer v. Chiczewski*, No. 07-C-1290, 2009 U.S. Dist. LEXIS 84176 at \*13–\*21 (N.D. Ill. Sept. 11, 2009) (analyzing SCA and *Flagg*, and ordering production in response to a subpoena based, in part, on explicit consent but also on lack of objection).

<sup>11</sup>*See Columbia Pictures Indus. v. Fung*, 2007 U.S. Dist. LEXIS 97576, \*30–\*31 (C.D. Cal. June 8, 2007) (a Web site receiving communications directed to it (such IP addresses) may consent to disclose them as a recipient and thus cannot refuse to produce them under the SCA). The *Flagg* district court also noted that consent may be implied in certain circumstances. *Flagg*, 252 F.R.D., at 364–65.

<sup>12</sup>One cannot, however, presume that a person has control over all bank documents relating to that person’s activities. *See U. S. v. D.K.G. Appaloosas Inc.*, 630 F. Supp. 1540, 1561 (E.D. Tex. 1986) (documents are kept for the bank’s benefit, not for the customer), *aff’d* 829 F.2d 532 (5th Cir. 1987).

<sup>13</sup>One should not assume, however, that an employer will be presumed to have control over an employee. *See In re Domestic Air Transp. Antitrust Litig.*, 142 F.R.D. 354, 356–57 (N.D. Ga. 1992) (evidence needed for a finding by the court).