Bloomberg BNA

Digital Discovery & e-Evidence®

BNA INSIGHT

The explosion in the number of companies providing services that store data ''in the cloud'' provides new challenges for applying outdated laws to new technologies. Carlton Fields attorneys James B. Baldinger and Chas Short examine the difficulties presented by the lack of clear legal guidance on disclosure of customer information by these companies.

Uncertainty in the Cloud: Changing Requirements for Disclosing Customer Data

BY JAMES B. BALDINGER AND CHAS SHORT

Rapid advances in communications technology has resulted in a surge in the amount and types of data maintained by the wide range of companies that provide services to consumers and businesses. Accessing the information stored by those companies is quickly becoming essential to law enforcement agencies, resulting in a tremendous increase in requests for access to emails, text messages, social media messages, and other customer information. Cell phone carriers alone report that in 2011 they responded to 1.3 million law enforcement requests for information such as text messages, caller location data, and subscriber information.[1]

Unfortunately, the law has not kept pace with the advances in technology, resulting in confusion and uncertainty about how companies should respond to requests for access to their customers' information. The explosion in the number of companies providing services that store data ''in the cloud'' provides new challenges for applying outdated laws to new technologies. This article examines the difficulties presented by the lack of clear legal guidance on disclosure of customer information by these companies.

Statutory Framework

Disclosure of customer information by ''electronic communication services'' and ''remote computing services'' is governed by the federal Stored Communications Act, 18 U.S.C. § 2701 *et seq.* (''SCA''), which was enacted by Congress in 1986 as part of the Electronic Communications Privacy Act. The SCA supplies rules for when companies may disclose, must disclose, and

[1] *Markey: Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers*, website of Congressman Ed Markey, http://markey.house.gov/press-release/markey-law-enforcement-collecting-information-millions-americans-mobile-phone-carriers (Last visited Oct. 19, 2012). Congressman Markey asked nine wireless carriers about their practices in response to requests by law enforcement for subscriber information. Congressman Markey's website includes his letters to carriers and their responses. *Id.*

 ISSN 1941-3882

are prohibited from disclosing the contents of communications and non-content records in response to subpoenas, court orders or other legal process.

Although Congress has updated the SCA several times, it is often not clear whether and how service providers should comply with law enforcement requests for customer information.[2] One essential step in determining what standards apply under the SCA is driven by whether a provider is considered an ''electronic communication service'' or a ''remote computing service'' (or neither), and whether the information sought is ''content'' or customer subscriber or transactional ''records'' of communications.

Unfortunately, the key definitions under the statute are based on an outdated view of technology, and determining how they apply to cloud computing services is especially murky. The lack of guidance (and sometimes, inconsistent guidance) from courts compounds the problem.

Businesses that provide cloud computing services must critically evaluate where they fall under the SCA's definitions, which will drive whether and how they must comply with requests from government entities. Though the law is far from settled, it is important for cloud computing services to fall *somewhere* under the SCA's definitions, so companies can determine what compliance is required.

Failure to properly comply with law enforcement disclosure requests—whether by revealing too much or too little information—is fraught with risk. Adverse publicity can result from a company failing to protect its customers' data or from failing to help law enforcement catch a criminal.

The SCA also provides the ability for anyone harmed by a violation of its terms to file a lawsuit. However, companies that disclose customer information in compliance with the SCA receive immunity from legal liability.

Uncertainty about their status under the SCA also risks exposing cloud computing companies to more voluminous requests for information from government entities and civil litigants.

Overview of the Stored Communications Act

The SCA generally prohibits providers of communication services to the public from divulging private communications, subject to a number of exceptions. A provider of ''an electronic 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.''[3]

Similarly, one who provides remote computing services to the public:

> shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.[4]

The SCA also prohibits electronic communication services and remote computing services from divulging customer records or other non-content information to a government entity.[5] As the SCA makes explicit elsewhere, however, a provider may disclose non-content ''record[s] or other information'' to any person other than a governmental entity.[6]

Exceptions. The SCA establishes a significant number of exceptions to these general prohibitions. For example, disclosures can be made with the consent of the customer or subscriber, or if disclosure is necessary for providing the service or for the protection of the service provider.[7] Significantly, the act does *not* contain an exception that allows disclosure of the contents of communication to civil litigants.[8]

As discussed below, both content and non-content information must be disclosed when the government sup-

[2] H.R. 6529, A bill introduced on September 21, 2012, by Congresswoman Zoe Lofgren, would clarify these issues. H.R. 6529 would require among other things, that the government obtain a warrant before compelling a service provider to disclose an individual's private online communications. Though H.R. 6529 seems unlikely to be passed by Congress this session, it is encouraging to see that at least some members of Congress are looking critically at the flaws in the Stored Communications Act.

James B. Baldinger is shareholder in the Carlton Fields law firm in West Palm Beach, Florida. He has a nationwide practice in commercial litigation and advises companies on security and electronic surveillance matters. From 1995 to 2003 Mr. Baldinger worked for AT&T Wireless Services as in-house litigation counsel and Vice President for Business Security.

Chas Short, an associate in Carlton Fields' Miami office, focuses his practice on the defense of white collar prosecutions and investigations including FCPA issues, tax controversies, banking and securities issues, health care issues, and other regulatory matters. He also conducts corporate internal investigations and assists businesses in developing compliance programs.

The authors thank Kim Thibault, University of Michigan, J.D. expected 2014 for her research assistance.

[3] 18 U.S.C. § 2702(a)(1).
[4] 18 U.S.C. § 2702(a)(2).
[5] 18 U.S.C. § 2702(a)(3); 18 U.S.C. § 2703(c).
[6] 18 U.S.C. § 2702(c)(6).
[7] *See* 18 U.S.C. § 2702(b)-(c).
[8] *See, e.g., Viacom International Inc. v. YouTube, Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (prohibiting disclosure of information pursuant to a civil subpoena because the act ''contains no exception for disclosure of such communications pursuant to civil discovery requests''); *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008) (language of SCA ''does not include an exception for the disclosure of electronic communications pursuant to civil discovery procedures'').

  DDEE ISSN 1941-3882

plies appropriate legal process under 18 U.S.C. § 2703. However, in emergency situations the SCA permits disclosure to law enforcement before legal process is obtained.[9]

Compliance with the SCA is important. The SCA establishes a cause of action for ''any provider of electronic communication service, subscriber, or other person aggrieved'' by a knowing or intentional violation of the act against any person or entity, except the government.[10] Courts can award successful claimants equitable or declaratory relief, money damages, and attorney fees and costs.[11] However, the SCA provides immunity for providers of wire or electronic communication services and their employees and agents for disclosing information or providing assistance ''in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.''[12]

Civil lawsuits are not the only risks presented by improper disclosures of communications. Section 2701 of the SCA criminalizes unlawful access to stored communications, and provides for the imposition of fines and up to 10 years imprisonment. A good faith reliance defense is set out in 18 U.S.C. § 2707(e), and provides immunity to civil and criminal liability for disclosures made in reliance on a request made under applicable law.

Though beyond the focus of this article, the SCA also addresses the preservation of evidence and backups,[13] requirements for a government entity to provide (and in some situations delay) notice to subscribers of information it requests,[14] cost reimbursement for provider's compliance efforts,[15] counterintelligence access to telephone toll and transactional records,[16] wrongful disclosure of video tape rental or sale records,[17] and civil actions against the United States for willful violations.[18]

Compulsory Disclosures by Cloud Computing Services to the Government

The SCA establishes several possible mechanisms by which the government can require providers of electronic communication services or remote computing services to disclose information. Determining which mechanism applies depends on the type of information the government seeks, and whether the information is held by an electronic communication service or a remote computing service.

The law provides no express guidance for determining where cloud computing services fit within the SCA's definitions, yet the answer can be critically important.

Non-Content Requests. When the government seeks only non-content records or other information related to a customer the issue is relatively straightforward. The government can obtain such information from either an electronic communication service or a remote computing service with a warrant, with a court order issued per § 2703(d) (which requires the government to demonstrate ''specific and articulable facts'' showing that there are reasonable grounds to believe that the information is relevant and material to an ongoing criminal investigation), or with the consent of the subscriber or customer.[19] If the government seeks the disclosure of certain basic subscriber information, it can use a subpoena.[20] Basic subscriber information includes only the name, address, telephone connection records/records of session times and durations, type and length of service, subscriber number or identity, including any temporarily assigned network address, and means and source of payment.[21]

Requests for Content. The more difficult questions arise when the government seeks to access the contents of communications. Under the SCA, communications held by an electronic communication service are entitled to greater protection than communications stored by a remote computing service. To obtain the disclosure of the contents of communication held by an electronic communication service in electronic storage for 180 days or less, the government must use a warrant.[22]

If a communication has been in electronic storage for 181 days or more, the government can instead obtain its contents with a § 2703(d) order or a subpoena.[23] The government can obtain the contents of a communication held by a remote computing service with either a warrant, a § 2703(d) order, or a subpoena—the SCA contains no '180 days' provision with respect to communications in a remote computing service.[24]

Definitional Dilemma: Is a Cloud Computing Service an 'Electronic Communication Service' or a 'Remote Computing Service'?

Unfortunately, cloud computing services do not fit neatly into the SCA's definitions of electronic communication service or remote computing service. Court decisions have further complicated the issue by holding that a provider can be an electronic communication service with respect to some subscriber communications, and a remote computing service with respect to others.[25]

Federal statutes define ''electronic communication services'' broadly as ''any service which provides to us-

[9] 18 U.S.C. § 2702(b)(8); 18 U.S.C. § 2702(c)(4).
[10] 18 U.S.C. § 2707(a).
[11] 18 U.S.C. § 2707(b)-(c).
[12] 18 U.S.C. § 2703(e).
[13] 18 U.S.C. §§ 2703(f) and 2704.
[14] 18 U.S.C. § 2705.
[15] 18 U.S.C. § 2706.
[16] 18 U.S.C. § 2709.
[17] 18 U.S.C. § 2710
[18] 18 U.S.C. § 2712

[19] 18 U.S.C. § 2703(c).
[20] 18 U.S.C. § 2703(c)(2).
[21] 18 U.S.C. § 2703(c)(2)(A)-(F).
[22] 18 U.S.C. § 2703(a).
[23] 18 U.S.C. § 2703(a)-(b). A government entity using a § 2703(d) order or a subpoena must give notice to the subscriber or customer. However, that notice may be delayed per § 2705(d).
[24] 18 U.S.C. § 2703(c).
[25] *See, e.g., Flagg v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008) (Provider ''may be deemed to provide both an ECS and an RCS to the same customer.''); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010) (Social media websites were electronic communication services with respect to messages that were not yet opened, and remote computing services with respect to messages that have been opened and retained by the account holder).

ers thereof the ability to send or receive wire or electronic communications.''[26]

At first blush, this definition seems relatively straightforward. However, its applicability in the context of the SCA is complicated by the definitions of other terms in the statute.

The general prohibition against disclosing the contents of communications by an electronic communication service applies to communications ''in electronic storage by that service.''[27] Likewise, § 2703(a) sets out how the government may require the disclosure of the contents of a communication ''in electronic storage in an electronic communications system.''

The trouble is that ''electronic storage'' does not have a common sense definition. According to the SCA, electronic storage is

> ''(A) any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.''[28]

This definition was created with a long out-dated view of email in mind; in 1986, email messages were temporarily copied and stored before being downloaded to the recipient's computer. Today, cloud computing services allow users to permanently store communications on the web so they can access their information from any computer.

Variations. Interpretations of the ''electronic storage'' definition vary. The Department of Justice (''DOJ'') adopts a narrow interpretation. According to the DOJ, a communication is not electronic storage unless it is stored in the course of transmission.[29] Communications held by an electronic communication service, but not opened or accessed by the addressee, are in electronic storage.

However, the DOJ only considers communications stored *by the service provider* prior to delivery to the recipient to be ''backup protection.''[30] Under this construction, an email that a subscriber reads and then chooses to store 'in the cloud' is not protected under the electronic communication service provisions of the SCA.

Conversely, the U.S. Court of Appeals for the 9th Circuit held in *Theofel v. Farey-Jones*[31] that ''backup protection'' includes communications that were already accessed by the recipient but left on the server.[32] The court observed that ''nothing in the Act requires that the backup protection be for the benefit of the ISP rather than the user.''[33]

Under this interpretation, the government would need a warrant to compel disclosure of the content of a communication received through an electronic communication service if it had been stored for 180 days or less, regardless of whether it had been accessed by the recipient. The *Theofel* interpretation generally supports the conclusion that the protections for communications in an electronic communication service apply to the contents of communications that users store in the cloud.[34]

In some circumstances, a cloud computing service may be considered a remote computing service rather than an electronic communication service, which carries different requirements for disclosure of information. For example, in *United States v. Weaver*,[35] the court determined that keeping previously accessed web-based email available online for a user constitutes a remote computing service, not ''electronic storage.''[36] In *Crispin*, the court held that two social media websites were remote computing services with respect to already-viewed messages.[37]

Cloud computing services fit with a common sense definition of a remote computing service, in that they allow a user to store information online as opposed to on the user's personal computer. But as in the case of an ''electronic communication service,'' the statutory definitions related to a ''remote computing service'' are complicated. For the general prohibition against disclosure to apply, a communication must be (1) carried or maintained by a remote computing service on behalf of, and received by electronic transmission from a subscriber and (2) carried or maintained ''*solely* for the purpose of providing storage or computer processing services to such subscriber or customer, *if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing*[.]''[38]

This second element is potentially problematic for cloud computing services. For example, if its terms of service allow a provider of web-based email to use the content of its customers' email to generate text ads targeted to a particular customer, does that mean the web-based email is now authorized to access the contents of communication for purposes of providing a service other than storage or computer processing (i.e. advertising)? Some scholars argue that it does, and that it might therefore mean that a cloud computing service would be neither an electronic communication service nor a remote computing service.[39]

If a cloud computing service's practices or terms of service result in it falling outside of the SCA, it may have to contend with government requests for stored communications, and also the requests of private litigants.

---

[26] 18 U.S.C. § 2510(15); 18 U.S.C. § 2711(1)

[27] 18 U.S.C. § 2702(a)(1).

[28] 18 U.S.C. § 2510(17) (2000).

[29] CCIPS, U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation, 123 (3d ed. 2009)

[30] *Id.* at 124.

[31] 359 F.3d 1066 (9th Cir. 2004).

[32] *Id.* at 1076.

[33] *Id.* at 1075.

[34] Note, however, that the *Theofel* court acknowledged, ''A remote computing service might be the only place a user stores his messages; in that case the messages are not stored for backup purposes.'' *Id.* at 1070.

[35] 636 F. Supp. 2d 769 (C.D. Ill. 2009).

[36] *Id.* at 772-73.

[37] 717 F. Supp. 2d at 987.

[38] 18 U.S.C. § 2703(b)(2)(A)-(B) (emphasis added).

[39] *See*, Ilana R. Kattan, Note, *Cloud Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*,13 Vand. J. Ent. & Tech. Law 617, 640 (2011).

  DDEE ISSN 1941-3882

Conclusion

Cloud computing services must be mindful of these challenges as they negotiate the labyrinthine requirements of the SCA. Because the level of statutory protection afforded to subscriber communications depends on whether the cloud computing service is defined as an electronic communication service, a remote computing service, or neither (and therefore subject not only to government requests but also requests from private litigants), these issues must be carefully considered. Until the law is updated, providers of cloud computing services should be aware of how their service might be classified to avoid improperly disclosing communications and better protect themselves and their customers.