

## Securing Communications on the Cloud

*Nolan M. Goldberg and Martha Wilson-Byrne, Proskauer Rose LLP*

*U.S. v. Weaver*, a recent opinion by the U.S. District Court for the Central District of Illinois, illustrates a potential vulnerability in the legal protections afforded to communications stored on the cloud, which essentially involves any hosted service delivered over the Internet.<sup>1</sup>

Web-based e-mail services for personal use have been around for some time now. Given today's economic environment, efforts have ramped up considerably to market these services to businesses as replacements for internally hosted e-mail systems. In such arrangements, an organization no longer needs to purchase, operate, and maintain its own e-mail servers and software. Instead, under the "cloud computing" model, a third party supplies this functionality as a service, pursuant to a contractual agreement, often using systems external to the customer.

This paradigm shift highlights the importance of securing cloud-hosted electronic information from both a technical and legal perspective.<sup>2</sup> Putting technical concerns aside, this article focuses on the Stored Wire and Electronic Communications and Transactional Records Access Act (SCA), 18 U.S.C. § 2701, et seq. The SCA protects, amongst other things, the contents of remotely-stored communications against access by both governmental entities and private litigants.

Significantly, the *Weaver* court appears to have diminished some of these protections by allowing governmental entities to obtain cloud-based e-mails (and other electronic communications) directly from the service provider with only a trial subpoena and not a warrant as previously required.

After a discussion of the *Weaver* case, this article examines best practices that can offset some of the resulting concerns.

### *The SCA and Weaver*

The SCA prohibits providers of electronic communications services, 18 U.S.C. § 2702(a)(1), and providers of remote computing services, 18 U.S.C. § 2702(a)(2), from disclosing the contents of electronic communications unless one of the exceptions enumerated in 18 U.S.C. § 2702(b) is met.<sup>3</sup> Among these exceptions are those authorized by 18 U.S.C. §§ 2517, 2511(2)(a), and 2703. See 18 U.S.C. § 2702(b)(2). The *Weaver* court's focus was on one of these listed exceptions, disclosures to governmental entities authorized by § 2703.

In *Weaver*, the Government sought to discover previously opened e-mails that were less than 180 days old from an MSN Hotmail account using a trial subpoena.

Microsoft, the provider of the Hotmail service, challenged the subpoena, and refused to turn over the e-mails. Microsoft argued that the e-mails were in "electronic storage," as that term is used in § 2703(a), and accordingly, it could not produce them absent a warrant. The Government, on the other hand, asserted that the e-mails were held or maintained "solely for the purpose of providing storage or computer processing services," § 2703(b)(2), and accordingly, a trial subpoena was sufficient.

The *Weaver* court, citing the definitions provided by 18 U.S.C. § 2510(17), noted that for a communication to be in "electronic storage," the storage has to be either temporary or intermediate, or for purposes of backup protection. As these e-mails were already opened, the court concluded that the storage could not be temporary or intermediate. Accordingly, the question of whether the requested e-mails were in "electronic storage" boiled down to whether they were in storage for purposes of backup protection.

Microsoft's position relied largely on a Ninth Circuit case, *Theofel v. Farey-Jones*, which held that previously opened e-mails that were less than 180 days old were in storage for backup purposes, and accordingly, fell within the warrant requirement.<sup>4</sup> In distinguishing Hotmail from the e-mail system at issue in *Theofel*, the *Weaver* court noted that the prior decision was based on the assumption that users downloaded e-mails from the remote server to their own computer, and therefore, the opened emails remaining on the server were inherently held for back-up purposes. Distinguishing web-based e-mail, the *Weaver* court pointed out that with modern e-mail, such as Hotmail, the "remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes." Accordingly, the court concluded that the requested e-mails were not in "electronic storage," and the Government only needed a trial subpoena, and not a warrant, to compel Microsoft to produce the e-mails.

The significance of this decision lies in the differences between a trial subpoena and a warrant. For a warrant, the Government must show that it has probable cause to require access to the requested materials. Procuring a trial subpoena, by contrast, only requires the lesser showing that the requested materials are evidentiary or relevant. While a judge always reviews the application for and signs a warrant — ensuring prior judicial review, trial subpoenas are issued by either the attorneys themselves or court clerks. Accordingly, for a trial subpoena, typically there is no prior judicial review, and the target, at its burden and expense, must make any challenge to the propriety and scope of the request. By diminishing the applicability of the warrant requirement in the cloud context, *Weaver* potentially makes it easier for the Government to obtain electronic communications stored on remote servers.

#### *Securing Cloud-Hosted Information Post-Weaver*

From the point of view of cloud providers and customers, the *Weaver* opinion is not all bad. Significantly, the court noted that Microsoft, in providing its Hotmail service, was acting as both an electronic communication service and as a provider of remote

computing services, and would thus be entitled to the protections of 18 U.S.C. §§ 2702(a)(1) and 2702(a)(2). Accordingly, the *Weaver* opinion affirms that electronic communications stored on the cloud are entitled to the full scope of the SCA's protections with regard to requests from non-governmental entities, such as private litigants.

However, the *Weaver* court's view of the exceptions to the restrictions on production of § 2702 that are authorized by § 2703, and in particular, its diminishment of the warrant requirement, is a potential cause of concern. With only a trial subpoena required to compel a service provider to turn over e-mails entrusted to it, inserting proper contractual provisions into the service agreement to govern the provider's response to a subpoena is the first step in securing hosted information. For example, the provider may be obligated to:

- notify the customer should the provider receive a subpoena requesting the customer's data at the earliest date possible;
- directly resist the subpoena, such as an obligation to challenge requests of unreasonable scope, or give the customer an opportunity to make such a challenge;
- ensure that data produced is subject to appropriate confidentiality restrictions; and
- define all costs associated with a subpoenaed production in advance so that there will be no surprises.

The agreement may also allocate the responsibilities and costs paid by each party should compliance with a trial subpoena impact the operation of the service, such as by requiring the service to preserve data that the normal operation of the service may destroy, or impinge on the rights of another customer of the service, as might happen should the subpoena call for the production of back-up tapes that contain the data of multiple customers of the e-mail service.

These contractual controls are at their most effective when the cloud service is operated by a single party, and the consumer is in a direct contractual relationship with that party. However, this may not be the case in all cloud systems. For example, an applications provider that wishes to offer a cloud version of its service, but does not have its own physical infrastructure, could enter into a contractual arrangement with one or more infrastructure providers. In such a case, the cloud system would have three parties: the consumer, the applications provider, and the infrastructure provider. Notably, the consumer may not be in a direct contractual relationship with the infrastructure provider in such an arrangement. Similarly, an infrastructure provider can itself enter into a contractual arrangement to swap computing capacity with another infrastructure provider (much as an electric company acquires power during peak demand). Finally, a single service can involve multiple applications providers, each implementing their own services through a variable number of sub-parties. The consumer may be in a direct contractual relationship with some parties to the service, but one or more contractual levels removed from other parties that touch its data.

In such circumstances, the contractual protection that the consumer negotiates may not be effective unless they run to every member of the system. For example, an applications provider may not be able to preserve forensic data — even if it is contractually obligated to do so — if it has insufficient contractual rights from its infrastructure provider. Accordingly, a thorough due diligence investigation should identify all parties that might have contact with the consumer's data, and ideally should include a review of the due diligence performed by any participant to the service that has already entered into a contractual relationship, as well as a review of all contracts among the different parties.

As cloud services support many types of communications beyond e-mail, such as Tweets, instant messages, etc., there likely will be an increased focus on the protections provided by the SCA. *Weaver's* possible diminishment of these protections with regard to cloud-based services highlights the importance of contractual provisions governing a service provider's response to legal demands for a consumer's data. Where the consumer is not in a direct contractual relationship with each party of the cloud service that might be considered to have custody of its data, there is an increased risk that the consumer's rights might be unprotected. However, a thorough due diligence process that includes an analysis of every participant to a service may go a long way toward ensuring that the consumer's data is adequately protected.

*Nolan M. Goldberg is IP & Technology Counsel in the Patent Law Group of New York-based Proskauer Rose LLP and a member of the Litigation Department's e-Discovery Task Force. Mr. Goldberg's practice focuses on patent law, intellectual property litigation and counseling, and electronic discovery. He is a frequent author and speaker on cloud computing-related legal issues. Martha Wilson-Byrne is an Associate in the Patent Law Group of Proskauer Rose LLP in Boston. Her practice concentrates on the analysis, protection, and enforcement of intellectual property rights.*

---

<sup>1</sup> 636 F. Supp. 2d 769 (C.D. Ill. July 15, 2009).

<sup>2</sup> Relevant technical concerns include securing the service from intrusion and verifying the identity of users of the service.

<sup>3</sup> The Wiretap Act's definitions are applicable to the SCA. See 18 U.S.C. § 2711(1). An electronic communication service is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. §2510(15). A provider of remote computing services provides "to the public . . . computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

<sup>4</sup> 359 F.3d 1066 (9th Cir. 2004).