LITIGATION MINUTE: SUBPOENAS AND THE STORED COMMUNICATIONS ACT

Date: 18 November 2021

U.S. Complex Commercial Litigation and Disputes Alert

By: Philip M. Guess, Aaron E. Millstein, Andrew N. Stokes

WHAT YOU NEED TO KNOW IN A MINUTE OR LESS

"Our business runs an electronic communication system and we got a subpoena for something that one of our users stores on our system. Can't we just produce it?" STOP! The *content* (explained below) of an electronically stored communication is treated differently under federal law than hard copy content or *non-content information* (e.g., information other than the content of a message, such as a username or the date the last user accessed the system.)

In-house counsel at companies that provide electronic communication services or remote computing services must consider the Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq*. when they receive subpoenas. An electronic communication service is any service that provides users with the ability to send or receive wire or electronic communications. A remote computing service is the provision to the public of computer storage or processing services by means of an electronic communication system. So, a business that provides an email system or a social network may be covered by the SCA.

The SCA governs access to “electronic communication services” and “remote computing services.” Because of the increasing volume of information stored in these services, in-house counsel and their outside litigators should be familiar with the provisions of the SCA.

What is the Stored Communications Act?

The SCA prohibits providers of an electronic communication service or a remote computing service from disclosing the contents of the information stored on their systems, except under certain circumstances. It also prohibits unauthorized access to an electronic communication service.

When Does the SCA Apply?

Companies that provide covered services should be alert to the SCA whenever they consider disclosing information provided by a user, customer, or subscriber. This includes disclosures pursuant to civil subpoenas or requests from the government. A company may be regulated by the SCA even if its primary business is something other than communication or internet services. For example, a company that provides an internal social network for employees may be covered, even if that company's primary business has nothing to do with electronic communication or remote computing services.

The SCA also comes into play when requesting information from a covered business, whether in litigation against that entity or via a third-party subpoena. The SCA establishes procedures for requests by the government.

Accessing electronically stored information without authorization, such as stealing a user's password in order to access their email account, may violate the SCA.

Content vs. Non-Content Data.

The SCA distinguishes between content (the text of an email or social media message) and other information (the identity of the sender or the date the message was sent). While the SCA bars production of content, it does not bar production of other information, including information provided by the user. This may include information like usernames or IP addresses.

Tips for Navigating the SCA.

- **Obtain User Consent**. The SCA authorizes disclosure with the consent of the user, customer, or subscriber. If practicable, obtain user consent before requesting data. But note, an employer may not be able to consent to the release of its employees' data.
- **Request Data from the User**. Request data (*e.g.*, social media information) directly from the user, rather than from the provider.
- **Request Non-Content Information**. Requesting non-content information may help you to identify other parties to the communication at issue who may be willing to consent to its release.
- **Use the SCA as a Shield**. Businesses covered by the SCA may be able to invoke the law to decline to produce requested documents.
- **Control Data Access**. Companies should maintain robust data controls. This will make it easier to show a violation of the SCA in the event of unauthorized access.

What Happens if the SCA is Violated?

Any person aggrieved by a violation of the SCA has a civil cause of action and may recover equitable or declaratory relief, damages not less than US$1,000 and possibly including punitive damages and lawyer's fees. SCA violations may also result in criminal liability. If an SCA violation results in criminal charges against the victim, suppression of the wrongly disclosed evidence will likely not be available as a remedy.

KEY CONTACTS

PHILIP M. GUESS
PARTNER

SEATTLE, PORTLAND
+1.206.370.5834
PHILIP.GUESS@KLGATES.COM

AARON E. MILLSTEIN
PARTNER

SEATTLE
+1.206.370.8071
AARON.MILLSTEIN@KLGATES.COM

