

TEXAS LAWYER

OCTOBER 5, 2015

An ALM Publication

www.texaslawyer.com

OUT_{of} | ORDER

Opinion • Commentary • Humor

Production of Electronic Records in Global Market

BY JULIE MACHAL-FULKS

Law enforcement officers regularly use the Stored Communications Act, (Title II of the Electronics Communications Privacy Act of 1986) to compel email providers to produce customers' email records to aid in criminal investigations. In a case pending in the Second Circuit Court of Appeals, Microsoft is testing the limits of exactly how far officers can reach in their investigations.

Recently, the Second Circuit heard oral arguments between Microsoft and federal prosecutors regarding whether officers can use the SCA to compel an email hosting company to produce the secured email records of one of its customers that are stored solely in Ireland.

Foreign officials are carefully watching the outcome of this matter, and the case has already generated negative publicity both locally and overseas. Both Ireland and the EU have strong laws related to protecting the privacy of

data. Procedures already exist for federal officers to seek production of foreign data directly from the jurisdiction where it is stored.

But, officers chose to circumvent the established international process in favor of seeking an order from a magistrate judge to compel Microsoft to produce the foreign-stored data directly to officers in the United States. Not surprisingly, Microsoft and others balked at the request. After a district court adopted the magistrate judge's recommendation and held Microsoft in contempt for failing to produce the records, Microsoft appealed.

What is at Stake?

Some of the questions raised by the appeal include: 1. Can Congress authorize the extra-territorial application of a statute without expressly including it in the statute? 2. Where is a search warrant "executed"? And 3. Do customer emails stored on



E-DISCOVERY

Microsoft servers constitute Microsoft's business records?

Because email is prevalent and because large email providers like Microsoft are growing and their reaches expanding across multiple jurisdictions, these issues could have far-reaching implications for other industries as well.

For example, if a global accounting firm has multiple offices around the world and generally stores its clients' data in the datacenter closest to the client, can the U.S. Department of Justice compel the accounting firm to produce records relating to a British citizen merely because the accounting firm also has an office in the United States?

The district court determined that Microsoft's business records include the contents of Microsoft's customers' secured and password-

records? If the answer is yes, any hosting provider's customer data could be subject to seizure by law enforcement officers, and potentially sought in discovery as the hosting provider's business records.


To further complicate matters, if the Second Circuit upholds the district court's decision in the Microsoft matter, the current location of the data could potentially become irrelevant.

In some instances, the procurement or technology teams do not consult with counsel prior to executing a hosting agreement. Sometimes, the company merely relies on the click-wrap agreement.

If production of stored data would be problematic for a company, the company must ensure that its teams are aware of the potential issues and are actively addressing those issues before the hosting provider has possession of any data.

Regardless of the outcome of the Microsoft matter, companies that are interested in outsourcing any of their IT functions to third parties should carefully consider the potential implications and negotiate as many protections as possible in the agreements with the hosting provider.

Any requirements related to data security or responses to warrants, subpoenas, and discovery requests should be disclosed to the provider at the outset of negotiations. Many of these requirements result in an increased cost to use the services.

Careful review of the hosting provider's agreements can help minimize some of the risks that are inherent with outsourcing data storage to a third party. 

Because email is prevalent and because large email providers like Microsoft are growing and their reaches expanding across multiple jurisdictions, these issues could have far-reaching implications for other industries as well.

protected email accounts, and thus, must be produced.

Microsoft does not offer only email services to its customers. It also provides hosting services for word-processing functions, spreadsheets, presentation slides, accounting services and many other hosted offerings.

If customers take advantage of Microsoft's popular Office 365 offering, either directly from Microsoft or from one of its many resellers, most of the clients' correspondence, documents, drafts, financial data, and other information are generally stored on Microsoft's servers. The same is true for other providers hosting similar workplace solutions.

Would all of this data also constitute the provider's business

Minimize the Risks

Many agreements with hosting providers include provisions requiring the provider to give notice to the customer if any third party seeks the customer's data from the hosting provider. Without those protections, the customer may not be aware of the request and may have no opportunity to challenge the discovery request, subpoena, or warrant.

Now, more than ever, it is critical for corporate counsel to help information technology teams ensure that hosting and outsourcing agreements contain as many provisions as possible outlining the hosting provider's responsibilities in the event that a third party seeks production of a customer's information.



Julie Machal-Fulks is a partner in Scott & Scott in Southlake, where she leads a team of attorneys in representing and defending clients in legal matters relating to information technology.