SPRING 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics and cybersecurity needs. With the proliferation of data breaches, we chose to focus this E-Newsletter on the topic of encrypted email and transient messaging technologies and the impact on organizations.

EMAIL AND TRANSIENT MESSAGING – YOU'VE GOT COMPLICATIONS

You've got mail; or maybe, your employees got mail. Perhaps someone you know got mail, and you need to see that mail. Then there's the possibility that somebody got mail they weren't supposed to get. Next thing you know, you've got a subpoena. In the case of hardcopy documents, the process by which those documents are produced for legal discovery were codified long ago and are reasonably straightforward. Unfortunately, electronic mail, or email, isn't quite as cut and dry, especially with technology advancing at a rapid pace.

Email in its simplest form isn't much different from hardcopy mail. A sender creates something tangible, for ease of discussion, a document. The document is sent via a carrier, such as the postal service, and a recipient receives said document. With email, a sender again creates and sends to a receiving party. However, the emailed document is actually a package of digital information that travels from origin to destination over the internet courtesy of a server, not a mail carrier or courier.

As simple as the electronic process is, email presents issues that complicate the legal discovery process.

The Stored Communications Act

Congress passed the Stored Communications Act (SCA) in 1986 as part of the Electronic Communications Privacy Act to address a gap between existing law and burgeoning Internet technology. The Fourth Amendment and its protections against illegal searches and seizures serves as the basis for rules of civil procedure, be those federal or state rules. Unfortunately, the Fourth Amendment reads in spatial terms. "The right of the people to be secure in their persons, houses, papers, and effects," has been interpreted historically as the physical constructs represented by those words. Digital packets of information need not apply for protection under the Fourth Amendment because they don't "exist" as tangible objects.

In *LEONARDO WORLD CORPORATION v. PEGASUS SOLUTIONS, INC.,* (2015), Judge Paul Grewal of the US District Court for Northern California clarifies the role of the SCA in legal discovery. “Civil subpoenas are subject to the restrictions of the SCA. Congress passed the SCA in 1986 because ‘the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.’”

The SCA addresses two services through which email is transacted. The difference between the two is subtle, but important. "Any service which provides to users thereof the ability to send or receive wire or electronic communications,” is an electronic communications service (ECS). An ECS allows you to send and receive email. A remote computing service (RCS) is "the provision to the public of computer storage or processing services by means of an electronic communications system." A clear example of RCS is shared cloud-based storage.

Here’s the tricky part – there’s nothing in the SCA that prevents both definitions from applying to a single entity. Google’s Gmail, for example, can be both ECS and RCS, because once sent, the email can be stored remotely by either sender or receiver (and separately by Google itself for disaster recovery purposes). It’s important to remember, for the purposes of discovery, there are potentially three parties involved with email: the sender, the receiver, and the remote computing service provider.

Discovery under the SCA

In general, the SCA prohibits a public service provider from disclosing the content of an account holder’s communications without the consent of the account holder, or, under a valid subpoena, a valid court order, or a search warrant. There are exemptions that also allow for the disclosure of communications content, but those are outside the realm of discovery.

The SCA allows public service providers to disclose voluntarily some non-content information (metadata) within a narrowly defined scope. A concise explanation of what is allowed appears in *SYSTEMS PRODUCTS AND SOLUTIONS, INC. v. SCRAMLIN*, Dist. Court, ED Michigan 2014:
Metadata associated with electronic communications, however, are not considered to be content protected by the SCA. Chevron Corp. v. Donziger, Case No. 12-mc-80237 CRB (NC), 2013 WL 4536808, at *6 (N.D. Cal. Aug. 22, 2013). In fact, the SCA expressly permits the disclosure of such data. 18 U.S.C. § 2702(c)(6) (an electronic communication service provider "may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications . . .) . . . to any person other than a government entity."). This allowance includes a subscriber's name, address, records of session times and durations, telephone or instrument number, or other subscriber number or identity.

Private service providers, universities for example, which provides ECS/RCS, are not prohibited from disclosing voluntarily either content or non-content information, although subpoenas, orders, and warrants may still be employed to compel discovery.

Getting the Discovery Done Right

It’s valuable to note that the SCA’s governance of email disclosure is directed at ECS/RCS providers. Serving a subpoena on a service provider for email content is possible, but substantiating the need to obtain content information from the service provider is a difficult undertaking.

Discovery rules for email senders and receivers substantially mirror the rules for tangible documentation. Parties to an action are the clearest choice. If either the sender or the receiver is a named party to an action, that party is assumed in possession, custody, and control of the email, and, can be compelled by the courts to produce. However, Judge Grewal reminds us in

Leonard that, “any individual with personal rights and privileges with regard to personal email has standing to request an order quashing a third party subpoena.” What this means is if the sender is subpoenaed, the receiver may object to the disclosure, and vice versa.

Preparing the request with care to the relevant content required, the proper timeframe of the communication, and any applicable email addresses is advisable. Courts are not prone to granting broad searches of email accounts in the hopes of accidental discovery. In AUSTIN OBODAI (d/b/a Heptad) v. INDEED, INC., Dist. Court, (2013) heard in the US District Court for Northern California, a Plaintiff’s Motion to Quash was granted in part, and a subpoena modified because the court found that the subpoenaed time period was overly-broad relevant to the case.

Spoliation: Watch Your Ps and Qs

Spoliation is defined in simple terms as significant alteration or destruction of evidence. Courts frown on spoliation and motions for sanctions against the party committing spoliation are not taken lightly. Remedies include fines, including attorney’s fees, and specific jury instructions with regard to evidence tainted by spoliation, even suit dismissal. In respect to email, spoliation includes editing emails after transmission, or, outright deleting email from sender accounts, receiver accounts, and/or servers to prevent discovery or alter the significance of the evidence.

On December 1, 2015, amendments to Rule 37(e) of the Federal Rules of Civil Procedure regarding electronically stored information, including but not limited to email, went into effect. By January 2016, Judge Francis of the US District Court for the Southern District of New York was already hearing a Motion for Sanctions. In *CAT3, LLC., vs BLACK LINEAGE, INC.,* the defendants claimed that the plaintiffs intentionally altered emails produced earlier in discovery. The spoliation was testified to by the defendants’ forensic discovery experts. While the plaintiffs denied the spoliation was their doing, they could not provide an explanation as to how the alterations happened to evidence in their possession.

The amended Rule 37(e) reads:
(e) Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
> (2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:
>
> > (A) presume that the lost information was unfavorable to the party;
> > (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
> > (C) dismiss the action or enter a default judgment.

Courts interpret the alteration of electronically stored information as part of failure to preserve, as the original information has been lost in the act of altering. Returning to the tangible document analogy, information in a document is covered with correction fluid, or redacted with heavy ink, the information may be lost. Even if the document is otherwise intact, the document may be rendered useless for evidentiary purposes.

In *Cat3 v Black,* the court found that despite the discovery of the original, unaltered emails, the plaintiffs committed spoliation under amended Rule 37(e). Plaintiffs were barred from using their version of the emails in the litigation, and, attorney’s fees and costs relative to the discovery of

the spoliation and the pursuit of sanctions were awarded to the defendants. While dismissal of the lawsuit was a remedy Judge Francis could have imposed, he chose to limit the sanctions to those above.

The amendments to Rule 37(e) don't require preserving all electronically stored information in perpetuity. The American Bar Association writes that new rule applies when "litigation is reasonably foreseeable and is based upon a longstanding common law duty." If you think you have an issue, proceed with caution. A reliable electronic discovery and computer forensics firm such as Digital Mountain can help preserve or restore evidence.

Transient Messaging: Here Today, Gone Tomorrow

Transient messaging, communication that is deleted after a specified action or period, may qualify as the technology least envisioned by the Fourth Amendment authors. Whereas email is roughly analogous to a tangible document, transient messaging is harder to concretize. More durable than speech, transient messaging may last only as long as the time required for recipients to view the message. Once gone, there are few recovery options, complicating legal discovery via the service provider.

Wickr Messenger is an example of a transient messaging application known for its security, dual-end encryption, and user control of message life. The service posts legal process guidelines on their website detailing how their transient messaging system works, and what the service can or will provide. In simple terms, Wickr will provide metadata in response to a subpoena, order, or warrant. With regard to preserving metadata, Wickr will preserve information for ninety days prior to legal service. As for content data, Wickr states that content sent through their server is encrypted in a manner that renders it unreadable by Wickr, and is deleted according to user settings. In short, even if Wickr has the communication on their server, only a ciphertext copy can be produced. Clearly, Wickr is serious when it comes to user privacy.

What does this mean for legal discovery? First, time is of the essence. There's no doubt that if a subpoena needs to be served, it needs to be served as soon as possible. With each day that passes, information disappears. Consider the applicability of an Order to Preserve. Secondly, forensic tools employed in e-discovery can often retrieve data from a user's mobile device or cloud storage. Not all is necessarily lost if the service provider encrypts or purges data.

With email and transient messaging firmly entrenched as communication technology, there's no doubt courts will continue to hear arguments over what is and is not subject to discovery. Knowing from where to seek the information and how quickly the information needs to be sought is vital. You've got mail. You've got transient messaging. You don't need a discovery issue.

UPCOMING INDUSTRY EVENTS

June 2016
LegalTech West Coast, San Francisco: June 13-14

July 2016
The Masters Conference, Managing the E-Discovery and Social Media Minefield,
New York: July 19

August 2016
HTCIA 2016 International Conference & Training Expo,
Las Vegas: August 28-31

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: