Given the prevalence of social media and its rapid climb to the top of the communications ladder, it's only natural for those in the legal profession to start regarding these platforms with an eye to potential discovery. New cases related to vital data mined from social media are consistently popping up; eDiscovery is at the forefront of groundbreaking legal precedents.

A few important questions to ponder are:

- **What social media discovery best practices should be proactively used during litigation?**
- **How can vulnerabilities be revealed with eDiscovery that could potentially win your case?**

Seattle
San Francisco
Silicon Valley
San Diego
Phoenix
Austin
Dallas

TERIS.com

888.99.TERIS (83747)

NO DATA LEFT UNMINED

Social networking sites aren't just for socializing anymore. With their increased prevalence as powerful business tools, sites like Facebook, Twitter, and LinkedIn have all seen their user numbers soar. People interact with each other both professionally and casually across these sites.

Even businesses that are not active on social networks often feature social networking ads and/or widgets on their website which enable visitors to like, share, or otherwise disseminate their content to a visitor's contacts.

The sheer breadth of these fledgling online communities offers a virtual data goldmine. It would be absurd not to take advantage of these resources – where it makes sense – for legal disputes or litigation. However, this is not to say that all of the information available is actually relevant. So how can you separate the kernels of significant data from the acres of insignificant "data chaff"?

DATA PRESERVATION POLICIES

Only recently, courts have sketched out the basics of a company's duty to preserve electronic documentation, and are just beginning to address discovery with respect to social media sites — and with good reason, too, since social media sites don't preserve data in the same way a company stores private emails or documents on its hard drive or server. Normally, social media data is scattered across several sites and stored in the cloud. It also changes frequently and can be updated or deleted just as quickly as it first appeared. Effective discovery must use software that is able to track these changes and access their history.

The data retention policy of a business typically does not include its social media pages. This does not, however, exclude a business from its duty to preserve its social media information that could be relevant if litigation is anticipated. The best option for businesses is to adjust their internal policies in anticipation of the changing times, and develop a procedure for social media data preservation.

Employees will need training in order to follow the internal policies and will also need to be educated regarding the potential risks of using social media. Just as the advent of hard drives changed the definition of a company's data preservation responsibilities, the introduction of social media changes those definitions again.

The data retention policy of a business typically does not include its social media pages. This does not, however, exclude a business from its duty to preserve its social media information that may be relevant if litigation is anticipated.

TERIS
Sophisticated Litigation Support

DATA COLLECTION CHALLENGES

Without the proper tools, trying to eke information out of social media sites can be a challenge. Very few companies have adopted new data preservation procedures and most have not even begun to address social media discovery.

Every company maintains its data differently and could utilize a variety of programs with different retention qualities. While software exists that can aid in social media data preservation, companies are understandably reluctant to close the data-deletion loophole. Since any deleted information may be relevant later on, invoking the help of an experienced third party in the case of litigation is crucial.

Even if the hurdle of data collection is surmounted, it by no means ensures admissibility. The authentication of electronic data is fraught with complications; social media data particularly is left vulnerable to hackers, viruses, spam, and other forms of corruption, manipulation, or outright fraud. For this reason, courts are practicing caution when considering the admissibility of social media data.

In *Treat v. Tom Kelley Buick Pontiac GMC, Inc.*, the court allowed printed copies of the data with time stamps to be entered as evidence. In the case of *Lorraine v. Markel Am. Insur. Co.*, metadata and hash tags associated with the data's creation were accepted in order to determine authenticity. In *Barnes v. CUS Nashville, LLC*, the presiding judge "friended" one of the parties on Facebook in order to personally verify photos, postings, and other data.

Admissibility is one area that comprehensive eDiscovery software is able to address. Timestamps, metadata, and other efforts are made to authenticate collected electronic data from social media sites and ensure a greater likelihood of admissibility.

PROCEDURAL LIMITATIONS

Businesses, individuals and legal professionals alike must understand that the **Federal Rules of Civil Procedure** ("FRCP") recognize the vital role that electronic documentation may play in the discovery process. However, this does not give either party carte blanche for indiscriminate data mining. According to the FRCP Rule 26 (a)(2)(B)- *Specific Limitations on Electronically Stored Information*:

"A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery."

While the courts may consider any data stored on social media sites to be discoverable, it is essential that a cost-effective and streamlined procedure be utilized during the process, particularly since the phrase "undue burden" is subject to the court's discretion.

The framework of obligations and limitations regarding eDiscovery has not yet expanded to fully encompass social networking sites; procedural revisions are outpaced by technology almost every time. However, individual court cases are paving the way to more consistent and inclusive discovery procedures that specifically address social media.

TERIS
Sophisticated Litigation Support

RECENT COURT DECISIONS

Understanding the new climate surrounding social media discovery is integral to developing best practices, and studying recent court decisions is the only way to stay current with the latest changes. This is not to imply that the decisions are all consistent with each other, but rather to gauge the shifting climate surrounding social media discovery.

Offenback v. L.M. Bowman

In Offenback v. L.M. Bowman, the plaintiff claimed that damages from a car accident resulted in physical and psychological trauma. The parties asked the court "to determine whether certain information contained within Plaintiff's [social media] accounts is properly subject to discovery." The court used the plaintiff's login information to access their Facebook account, which indeed revealed evidence refuting the plaintiff's claim. The court stated that "public information contained in Plaintiff's account is properly subject to limited discovery in this case" and added that [relevant] "information is clearly discoverable under recent case law." However, the court also stated that "it would have been substantially more efficient for Plaintiff to have conducted this initial review and then, if he deemed it warranted, to object to disclosure of some or all of the potentially responsive information" and concluded with concerns regarding eDiscovery, stating "the challenge is to define appropriately broad limits … on the discoverability of social communications."

Mackelprang v. Fidelity National Title Agency of Nevada, Inc.

During Mackelprang v. Fidelity National Title Agency of Nevada, Inc., a sexual harassment case, the defense sought all MySpace records (including private messages) in the hopes of revealing that the plaintiff was having an extramarital affair. The motion in its original scope was denied by the court, stating that "private e-mail messages between Plaintiff and third persons regarding allegedly sexually explicit or promiscuous emails not related to Plaintiff's employment with Fidelity" were not relevant to the case. However, the court did allow the defense to present more admissible data through the use of data-specific discovery requests.

EEOC v. Simply Storage Mgmt., LLC

In EEOC v. Simply Storage Mgmt., LLC, another sexual harassment case, the defendant requested release of relevant content from the plaintiff's social media sites. The plaintiff argued that conceding to this motion was a privacy infringement. However, the court ruled that the content be produced, stating that "a person's expectation and intent that her [social media] communications be maintained as private is not a legitimate basis for shielding those communications from discovery" and that the request was simply an "application of basic discovery principles in a novel context."

Crispin v. Christian Audigier, Inc.

In direct contrast to the above case, the court's ruling of Crispin v. Christian Audigier, Inc. disallowed subpoenas requesting discovery from the plaintiff's MySpace and Facebook pages, among other sites. The court felt that these communications were protected under the Stored Communications Act, being electronic communication services (ECS) as defined by the Act. The plaintiff's private messaging, stated the court, was not subject to standard discovery process. Regardless of those messages occurring on a public social media platform, the interactions took place under a privacy setting, and so were protected.

BEST PRACTICES GOING FORWARD

The handful of cases listed above represent the widely varying opinions regarding discovery of social media. Although some judges are allowing the evidence, others continue citing the ***Stored Communications Act***. The emerging trend is that of courts allowing publicly-accessible information. Or, as the ***Federal Rules of Civil Procedure*** state, "any non-privileged matter that is relevant to any party's claim or defense" remains discoverable, whether through traditional discovery or eDiscovery.

What does this mean? For businesses, adopting new policies which address potential social media discovery regarding data preservation and collection is a must. For legal professionals, it means advising clients that any online action taken on their part may be subject to standard discovery process, including eDiscovery. In short, although the delivery method may have become more technological, the best practices surrounding social media discovery are the same as preparing for any other potential litigation: study the rapidly-evolving case history, take sensible precautions, and be prepared.

If you would like to learn more about how TERIS uses Best Practices for Social Discovery with its clients, please contact us.

TERIS.com | 888.99.TERIS (83747)
TERIS
Sophisticated Litigation Support