E-Discovery: Social Media Counts

Courts have made it clear that social media may be subject to pre-trial discovery. But judges aren't inclined to grant blanket access to social medial accounts just so litigants can engage in a fishing expedition. Instead they require proof that a site is likely to contain relevant material. This article discusses the e-discovery rules and how social media presents unique challenges.

Data stored on social media platforms may be fair game in pre-trial discovery — even if the user limits access to personal posts.

Increasingly, courts are deciding that private isn't necessarily the same as not public and they're granting discovery requests to obtain relevant social media evidence in civil cases.

Discovery Basics

In every lawsuit, there's a period when each party is allowed to obtain and examine the other party's information, documents and pre-trial testimony. The rules involved in this process are strict. Each party must adhere to them, or be subject to sanctions. Lawyers gather evidence by taking testimony from witnesses and examining physical evidence and relevant documents.

In the past, documents were primarily paper. But today, they're just as likely to be electronic — texts, emails, website pages and social media posts.

People generally use social media to communicate with friends and family. Businesses also use it as a low-cost marketing tool. But what's posted — including Tweets, blog posts, pictures, timelines and comments — may come back to haunt users in a lawsuit. Consider these examples:

A warehouse employee files a workers' compensation lawsuit against his employer for a back injury allegedly incurred while stocking shelves. A coworker tells the warehouse manager that the plaintiff's Facebook profile lists dirt bike racing and snowboarding as his personal interests. The company asks the court for access to his profile and any pictures of the plaintiff posted six months before and after the injury for evidence that he engaged in high-risk activities that might have caused or aggravated his injury.

A receivables clerk files a sexual harassment claim against her former boss (the company's CEO and co-owner) and requests access to his social media accounts during discovery. She specifically believes that the plaintiff shared inappropriate photos of her with his contacts — including another co-owner — on Facebook and Instagram following the company's holiday party and summer baseball outing.

A company's chief financial officer (CFO) is accused of stealing from the firm's retirement funds. The company requests access to her Twitter and Facebook account to search for evidence that she was living beyond her means and suffered from gambling and drug addictions. The plaintiff specifically requests access to posts made while the CFO was on an extravagant tour of Europe. She allegedly bragged about siphoning cash from the company's "slush fund" to pay for her "cocaine and blackjack binges."

E-Discovery Rules

The common denominator in these examples is that the party seeking access to the data is requesting specific information that could reasonably lead to the discovery of relevant, admissible evidence.

E-discovery deals with electronically stored information (ESI). This includes data stored on computers, mobile devices, networks, backup systems or other storage media. The Federal Rules of Civil Procedure specifically address ESI and provide protocols for how each party must produce documents. The rules allow for sanctions if parties are uncooperative and also consider ESI subject to subpoenas.

There may be safe harbors when electronic evidence is lost and unrecoverable as a matter of regular business processes. If data loss doesn't occur in the normal course of business, however, the party could be subject to sanctions.

Unique Challenges

Social media presents special legal challenges in discovery. Suppose a company allows its workers to access social media accounts on company computers during their lunch breaks. If an employee saves his or her username and password on a company-owned device, does the employer have the legal authority or practical ability to access the employee's social media data? What about data stored on personal devices that are subject to the company's bring-your-own-device policy? Who legally controls company data housed on the device?

Many people mistakenly believe that social media posts are private. But Facebook's homepage says that the site helps users "connect with friends and the world around you." Even if all of an individual's posts are private — that is, accessible only to approved contacts — the person is still sharing the posted information with outsiders. As a result, it may be discoverable.

Although courts may not buy the right-to-privacy argument, they generally don't honor blanket requests to access an entire social media account either. The party requesting access to social media content generally must prove a legitimate basis for needing the specific data.

Playing by the Rules

Social media content is typically fair game in discovery, but relevance is the name of the game. Attorneys who request specific social media posts are more likely to be granted access by the courts than those who file broad, nonspecific requests. However, as with any form of ESI, everyone must play by federal and state rules of procedure..

Gryphon Valuation Consultants is a full-service professional business appraisal firm offering a broad range of valuation and litigation consulting services. If we can serve your valuation needs, or if you have a question about our services, please contact us at 702-870-8258 or visit us on the web at www.BizVals.com. Gryphon is an independent member of the American Business Appraisers National Network.